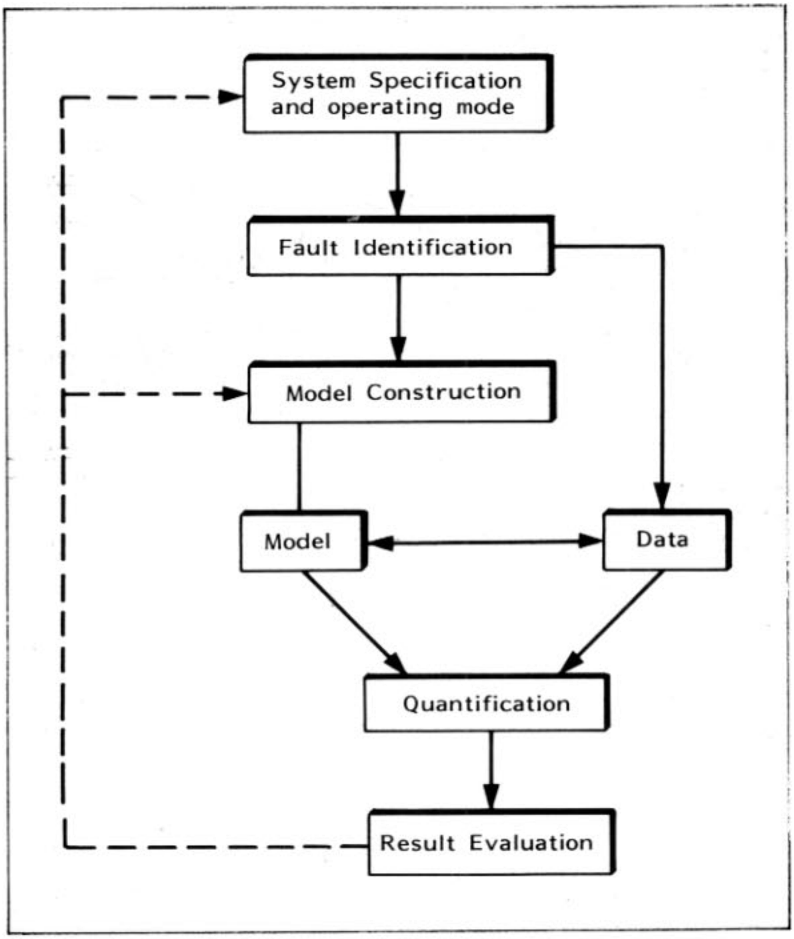
NORD
June 1985

PRA USES AND TECHNIQUES
A NORDIC PERSPECTIVE



nka
Nordic
liaison committee for
atomic energy

nka

Nordisk
kontaktorgan for
atomenergispørgsmål

Nordiska
kontaktorganet för
atomenergifrågor

Pohjoismainen
atomienergia-
yhdyselin

Nordic
liaison committee for
atomic energy

Säkerhetsprojekten

PRA USES AND TECHNIQUES
A NORDIC PERSPECTIVE

Summary report of the NKA project SÄK-1

Edited by
Stephen Dinsmore
Studsvik Energiteknik AB
Sweden

June 1985

THE SÄK STEERING COMMITTEE

T Eurola, STUK
C Gräslund, SKI*
E Hellstrand, STUDSVIK
D Malnes, IFE
T Mankamo, VTT
F Marcus, NKA
B Micheelsen, RISØ
A Olsen, RISØ
E Sokolowski, RKS
S Vuori, VTT
M Trolle, SKI

LIST OF PARTICIPANTS IN THE SÄK-1 PROJECT

ASEA-ATOM Aktiebolaget ASEA-ATOM	Göran Ericsson Stefan Hirschberg Kari Laakso
IFE Institute for Energy Technology	Gustav Dahll Nils Førdestrømmen
RISØ Risø National Laboratory	Per Becher Hans Kongsø Kurt Lauridsen Dan Nielsen Erik Nonbol Kurt Petersen Ole Platz Lene Schepper Niels Vestergaard
STUDSVIK Studsvik Energiteknik AB	Stephen Dinsmore Nils Kjellbert Kurt Pörn Ove Åkerlund
VTT Technical Research Centre of Finland	Pekka Aaltonen Iris Karvonen Tuomas Mankamo** Urho Pulkkinen Juhani Vanhala
STUK Finnish Centre for Radiation and Nuclear Safety	Kalevi Haule Osmo Viitasaari Reino Virolainen
SKI Swedish Nuclear Power Inspectorate	Lennart Carlsson Bo Liwång

* Chairman
** Project Leader

ABSTRACT

Techniques for probabilistic risk analysis (PRA) are analyzed with special emphasis on their application in nuclear power plants. Methods and codes currently available for PRA analysis in the Nordic countries are evaluated and compared. Additionaly, the ability to generate unique failure parameters from available plant data bases and generic data sources is examined. The subsequent application of PRA techniques as an aid in the licensing and regulatory process is discussed.

Key words

Block Diagram - Cause Consequence Diagram - Common Cause Failure - Comparative Evaluations -Denmark-Dependent Failure - Event Tree - Fault Identification-Fault Tree - Finland - Human Errors - Norway Nuclear Power Plants - Nuclear Power Regulation-Probabilistic Risk Assessment - Reliability Analysis-Reliability Computer Codes - Reliability Data Bases Sequence Modelling - System Modelling - Sweden Uncertainty Analysis

This report is part of the safety programme sponsored by NKA, the Nordic Liaison for Atomic Energy, 1981-85. The project has been financed by the Nordic Council of Ministers and the national institutions and regulatory bodies.

SUMMARY

Probabilistic risk analysis (PRA) techniques are increasingly being used at industrial plants to identify specific areas where safety and reliability can be improved in a cost effective manner. In the Nordic countries, PRA techniques are currently employed as a tool during the evaluation of the safety of chemical plants, off-shore platforms, nuclear power plants, and other complex industrial systems. In the nuclear field these techniques are used extensively for system evaluation in Finland and in the Swedish As-operated Safety Analysis Reports (ASAR's) which are periodic reviews of the operating nuclear power plants.

In principle, PRA methodology provides a comprehensive framework which leads to a well documented analysis of a plant and its functions. In order to take full advantage of PRA, techniques must be available which are systematic enough for general use and easily documented yet sufficiently accurate to resolve the issues in question. Currently, many alternative techniques exist which can benefit from comparisons and verification and some of which can be improved.

In the present project, some of the established PRA techniques were compared while other techniques were further developed. The work was essentially limited to functional modelling and subsequent probabilistic evaluation of accident sequences at nuclear power plants (the so called level 1 PRA). Other, non-nuclear, uses of these techniques are described in a separate report titled, "Risk Analysis Uses and Techniques in the Non-Nuclear Field - A Nordic Perspective".

In order to provide a practical framework for comparison work, two "Benchmark" studies were performed. In each Benchmark study, the same object was analyzed independently by each of three study groups in the Nordic countries. Comparisons were made between modelling methods, data sources, and computer codes.

The Benchmark 1 study was concerned with a high pressure injection system typical of PWR plants. Each group independently compiled the required reliability parameters for a common system model using data handbooks and other generic sources. The highest and the lowest selected values for identical parameters often differed by a factor of 3 or 4.

In the same study, each group quantified the system model using each data set in turn and their own computer code. The calculated results included the mean unavailability, the contribution of repair unavailability, and the impact of alternative test intervals. Generally, the results were quite consistent for any single data set irrespective of which code was used. Consequently, the source of the data is much more important than the quantification program, even when selecting from standard data sources.

In the Benchmark 2 study three plant response models for a loss of feedwater transient in a BWR plant were independently developed and then compared. The emphasis here was in the comparison between different modelling methods such as cause-consequence diagrams compared with event trees, and reliability block diagrams compared with fault trees. This study indicated that the choice of an appropriate method depends, to a large extent, on the complexity of the system to be analyzed and on the objectives of the analysis. Furthermore, the need for careful review and close contact with persons intimately familiar with the system, such as plant operators, was found to be at least as important as the choice of techniques.

Systematic search methods - both computerized and manual - were developed to identify potential common cause failures. These methods were subsequently tested in the context of the Swedish ASAR studies. Intensive work was also done to improve the dependent failure models necessary to quantify the identified dependencies. The new models were required in order to consistently take into account the high level of redundancy typical for nuclear power plants in the Nordic countries.

Statistical methods were developed for the treatment of field data collected from the power plants. Particular emphasis was placed on the estimation of the uncertainty in the calculated parameters. The methods are adapted for use in Nordic PRA studies and were used during the compilation of the second version of the Swedish Reliability Data Handbook (T-boken).

The available PRA techniques are useful tools which can help the licensing authorities evaluate the safety of nuclear power plants. The numerical result from such evaluations provide a means for referencing existing functions to a common scale allowing comparisons which otherwise would be impossible. When used with proper regard for the current limitations, these results can also be used to identify weak points and help the licensing authorities evaluate proposed changes and select between alternatives.

SAMMANFATTNING

Metoder för sannolikhetsbaserad riskanalys (Probabilistic Risk Analysis, PRA) används i ökande utsträckning vid industriella anläggningar för att identifiera områden där säkerhet och tillförlitlighet kan förbättras på ett kostnadseffektivt sätt. I de nordiska länderna används för närvarande PRA-teknik som ett verktyg för utvärdering av säkerheten i kemiska fabriker, havsbaserade plattformar, kärnkraftanläggningar och andra komplexa industriella system. På kärnkraftområdet används PRA i stor utsträckning i Finland för systemspecifika analyser och i de svenska ASAR-studierna som redovisar återkommande säkerhetsgranskning av driftsatta kärnkraftanläggningar.

PRA-metodiken kan sägas utgöra en grundstomme, som möjliggör väl dokumenterade analyser av anläggningar och deras funktion. För att till fullo utnyttja PRA måste metoder finnas som är tillräckligt systematiska för att kunna användas generellt och är lätta att dokumentera men ändå tillräckligt detaljerade för att kunna analysera de aktuella problemen. Det finns för närvarande många alternativa metoder som med fördel kan jämföras och verifieras och av vilka vissa kan förbättras.

I detta projekt har några etablerade PRA-metoder jämförts och några metoder vidareutvecklats. Arbetet begränsades väsentligen till modellering av systemfunktioner och efterföljande probabilistisk utvärdering av haverisekvenser i kärnkraftanläggningar (s k PRA nivå 1). Andra, icke-nukleära, tillämpningar av dessa metoder beskrivs i en separat rapport med titeln "Risk Analysis Uses and Techniques in the Non-Nuclear Field - A Nordic Perspective" (Riskanalytiska tillämpningar och metoder inom det icke-nukleära området - Ett nordiskt perspektiv).

Jämförande analys har gjorts i form av två referensstudier. I vardera studien analyserades samma system av tre arbetsgrupper i de nordiska länderna oberoende av varandera. Jämförelser gjordes av modelleringsmetoder, datakällor och beräkningsprogram.

Referensstudie 1 behandlade ett högtrycksinsprutningssystem typiskt för en tryckvattenreaktor. Varje grupp sammanställde erforderliga tillförlitlighetsdata för en gemensam systemmodell med hjälp av datahandböcker och andra generiska källor. Högsta och lägsta valda värden på identiska parametrar visade sig ofta skilja med en faktor 3 eller 4.

I samma studie kvantifierade varje grupp den gemensamma systemmodellen med hjälp av varje dataserie i tur och ordning och med gruppens eget datorprogram. Beräkningsresultaten omfattade den genomsnittliga systemotillängligheten, bidraget från otillgängligheten på grund av reparation samt inverkan av olika testintervall. I allmänhet var resultaten rätt samstämmiga för en given datauppsättning oberoende av vilket datorprogram som användes. Följaktligen är datakällan mycket viktigare än kvantifieringsprogrammet, även om man väljer data från en standardkälla.

I Referensstudie 2 undersöktes en transient med matarvattenförlust i en kokvattenreaktor. Tre oberoende svarsmodeller utvecklades och jämfördes. Tonvikten lades här på att jämföra de olika modellerna, t ex orsaks-konsekvensdiagram jämfört med händelseträd och tillförlitlighets - blockdiagram jämfört med felträd. Studien visade att valet av lämplig modell i stor utsträckning beror på komplexiteten hos det system som skall analyseras samt på analysens syfte. Dessutom befanns behovet av omsorgsfull granskning och kontakt med personer med god kännedom om systemet vara minst lika viktigt som valet av modell.

Systematiska sökmetoder - både datoriserade och manuella - utvecklades för att finna eventuella fel med gemensam orsak. Dessa metoder prövades senare i samband med de svenska ASAR-studierna. Intensivt arbete ägnades också åt att förbättra de modeller för beroende fel som behövdes för att kvantifiera de identifierade beroendena. De nya modellerna erfordrades för att på ett konsistent sätt kunna ta hänsyn till den högre nivå av redundans som kännetecknar kärnkraftanläggningar i de nordiska länderna.

Statistiska metoder utvecklades för behandling av erfarenhetsdata insamlade från anläggningarna. Speciell tonvikt lades på att uppskatta osäkerheten i de beräknade parametrarna. Metoderna är anpassade för tillämpning i nordiska PRA-studier och användes vid sammanställningen av den andra versionen av den svenska handboken över tillförlitlighetsdata (T-boken).

Tillgängliga PRA-metoder är användbara verktyg som kan hjälpa tillsynsmyndigheten att utvärdera kärnkraftanläggningars säkerhet. De numeriska resultaten av sådana utvärderingar ger ett sätt att referera existerande systemfunktioner till en gemensam skala vilket medger jämförelser som annars vore omöjliga. Om resultaten används med vederbörlig hänsyn till aktuella begränsningar kan de också användas för att identifiera svaga punkter och hjälpa myndigheter att värdera föreslagna åtgärder och välja mellan dem.

LIST OF CONTENTS

LIST OF CONTENTS con'd

1. INTRODUCTION

The Nordic project NKA/SÄK-1, Probabilistic Risk Assessement (PRA) and Licensing, has been carried out within the research program of the Nordic Liaison Committee for Atomic Energy (NKA) in the period 1981-84. This report is a summary of the work done during the project but also includes broader findings arising from general work in the field by the participating organizations. Technical support for most of the topics discussed in the study can be found in the references.

1.1 Basics of PRA

The probabilistic analysis process for a nuclear power plant can be divided into several major tasks as shown in Figure 1.1. This division is convenient since, although each level builds upon the previous level, each level involves different modelling techniques, methods, and tools. In brief these levels include the following:

Level 1 involves estimation of the types and frequencies of initiating events, evaluation of the available response or mitigating systems, and calculation of the failure probabilities of these systems. This process leads to an estimate of the expected frequency of various potential accident sequences which may result in degradation of the reactor core.

Level 2 involves evaluation of the containment protection features, estimation of the magnitude of the radionuclide release to the containment in the sequences identified above, and calculation of the magnitude and frequency of the release of various radionuclides to the environment.

Level 3 concerns the evaluation of radionuclide transport through the environment, calculation of

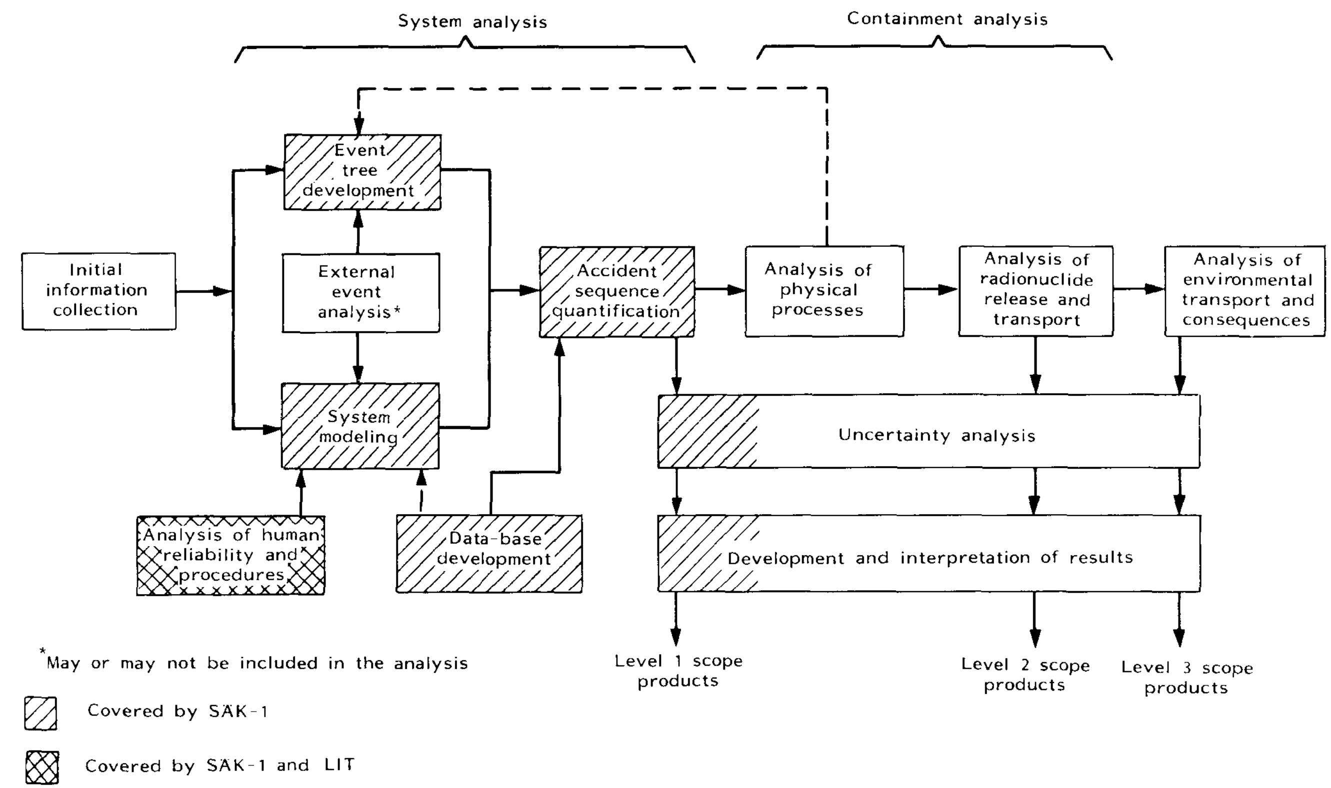


Figure 1.1.1 Risk Analysis Tasks [1 - 1].

potential radiation doses to the population around the site, and conversion of these doses to health risks.

Many of the methods used in PRA, particularly those discussed in this report, are not specific to nuclear power plant applications. They can be used for any electrical or process system or group of systems such as an offshore drilling facility, a chemical process plant, an electrical supply network, etc. These methods are, however, most useful for systems or groups of systems for which direct data of the failure frequency do not exist and for which the effects of a failure can lead to large economic or safety losses. In one recent project [1-2], some of the methods discussed in this report were applied to many different types of systems and reference [1-3] discusses the application of the method described in this report to non-nuclear plants.

1.2 Objectives and scope of the SÄK-1 project

The work was undertaken as a joint Nordic venture because of the multi-disciplinary nature of PRA itself, and the desire to combine the relatively limited national resources in this field.

The project was initiated with the following objectives:

- verification of risk analysis methods concerning the completeness of the models and the accuracy of quantitative predictions
- improvements in the data base for the reliability of components
- presentation of guidelines for the application of probabilistic methods in regulatory work including an evaluation of the benefits and limitations.

The scope was limited to procedures and methods of hazard identification, accident sequence modelling and the reliability analysis of safety systems. The project was thus concerned with level 1 PRA. Level 1 PRA was stressed in order to address the practical needs of the Nordic community which currently is primarily concerned with level 1 PRAs. The SÄK-1 project also addressed, to a limited extent, human errors in the context of quantitative reliability analysis. Another Nordic project, the LIT project [1-4], qualitatively addresses some specific aspects of human-system interactions.

Comparison and verification of the analysis methods has been based mainly on two Benchmark studies concerned with

- reliability analysis of a typical high pressure injection system for a PWR plant and
- modelling and quantification of disturbance sequences resulting in the loss of feedwater in a BWR plant.

The Benchmark studies have for the most part been carried out independently by different institutes. The results and experience provide insight about the completeness of system modelling and the uncertainties inherent in the method and data choices.

Work in the reliability data base was connected with the compilation of the Swedish Data Reliability Handbook [1-5]. The main emphasis was on the statistical methods for the treatment of field data; especially for the estimation of uncertainty limits. Insight on the applicability of different data sources has also been obtained in the two Benchmark studies.

In order to consider implementation of PRA in regulatory work, the developments in the US and other countries were reviewed with consideration being given to the local circumstances in the Nordic countries. During this review, emphasis was placed on how PRA is used as a decision aid while considering design changes and procedure development and during the assessment of operating experience from nuclear power plants.

1.3 Organization of the project

The project has been carried out as a joint effort by:

- Risø National Laboratory, Denmark
- Technical Research Centre of Finland
- Institute for Energy Technology, Norway
- Studsvik Energiteknik AB and ASEA ATOM, Sweden.

The project schedule is presented in Table 1.2.1. The work has been directed by a Project Group composed of one or two project members from each participating institute and of experts from the Swedish Nuclear Power Inspectorate, Finnish Centre for Radiation Protection and Nuclear Safety, and the Nuclear Safety Board of the Swedish Utilities.

Table 1.2.1

Project task and timetable

	Task	Person years	TIMETABLE 1981	1982	1983	1984
1	Method development and verification	7				
2	Data base improvement	5				
3	Sensitivity and uncertainty analyses	2				
4	Trial studies					
	Benchmark 1	1				
	Benchmark 2	3				
5	Implementation of PRA in regulatory work	4				
6	Joint activities	2				
	- Project seminars		1st	2nd	3rd	
	- Data workshop			x		
	- Dependent failure workshop				x	
	- Licensing workshop					x
	- Expert workshop					x
	Person years total	Σ 24				

REFERENCES

1-1 PRA Procedures Guide.
NUREG/CR-2300, January 1983.

1-2 "Sikkerhetsanalyse som beslutningsunderlag", Vol I: Teori og metoder, Vol II: Praktiske eksempler.
Slutrapport från SCRATCH-programmet.
Nordforsk, RISØ juni 1982.

1-3 PETERSEN, K E
"Risk Analysis Uses and Techniques in the Non-Nuclear Field-A Nordic Perspective".
To be published Sept 85, available from RISØ

1-4 ANDERSSON, H
"Human Errors in Test and Maintenance of Nuclear Power Plants", NKA/LIT-1(85), to be published 1985.

1-5 T-boken, tillförlitlighetsdata för komponenter i svenska kokvattenreaktorer, RKS 85-05, May 1985.

2. OUTLINE OF THE BENCHMARK STUDIES

This chapter briefly describes the Benchmark studies as a background for the methods and data discussions in subsequent chapters.

2.1 Benchmark 1 on reliability parameters

The first Benchmark study was concerned with the generation and propagation of reliability parameters. A sample high pressure injection system (HPIS) shown in Figure 2.1.1 was prepared by VTT on the basis of structures that are typical of high pressure emergency core cooling systems in pressurized water reactors. A system model was developed for this system and three study groups at Risø, VTT and Studsvik were asked to quantify the model.

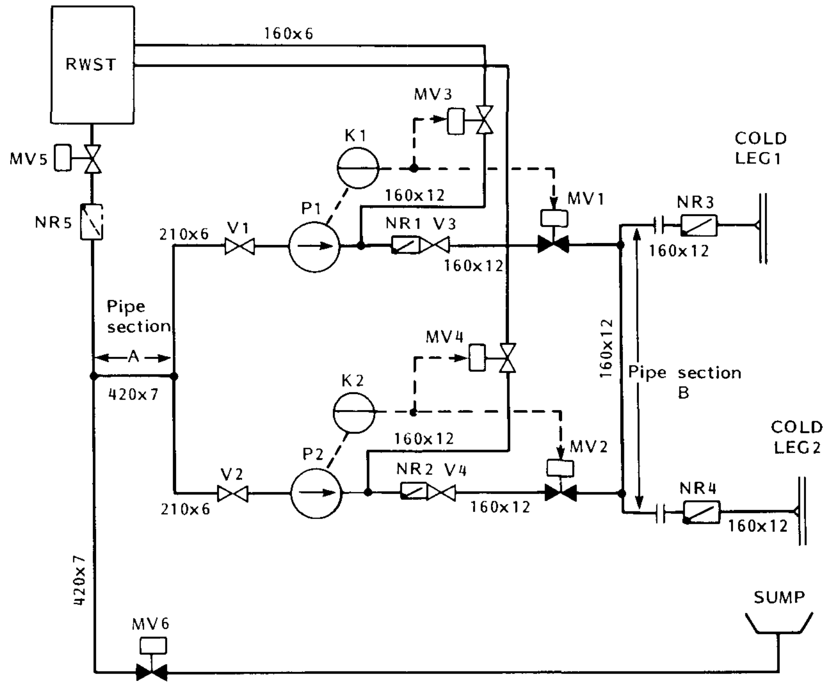


Figure 2.1.1 High Pressure Injection System PWR Process Diagram.

2.1.1 Comparison of data choices

The three study groups compiled reliability parameters for the components in the example system using data handbooks and other sources of generic data. The final values selected for the different data requirements are presented in Figure 2.1.2.

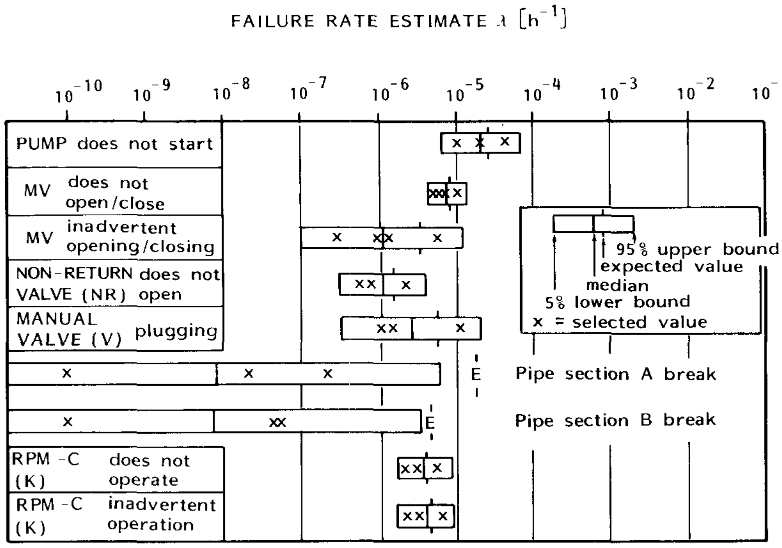


Figure 2.1.2 Calculated Failure Parameters.

The 90 % confidence bounds were calculated assuming a log-normal distribution. Note that the mean value (E) for the pipe breaks are above the 95 % limit.

The largest deviation (not presented in Figure 2.1.2) occurred for pumps due to the choice of the erroneously calculated average value from NPRDS data handbook 1978. This figure was allowed to be corrected as it was considered likely that the failure rate would have been observed to be too high during the quantitative analysis.

Uncertainty intervals were calculated by assuming that the selected values are samples from a log-normal distribution. These are also presented in Figure 2.1.2. As expected, reliability data of pipe sections have the largest deviation. In the other data, the variation was moderate or small.

2.1.2 Comparison of the results with different codes

The system reliability quantification was done independently by the study groups using the three different data sets (I, II or III), identical system models, and each institute's own computer code. Risø used the MOCARE code which is a Monte Carlo simulation code. VTT used the REPINT code based on analytic expressions for the unavailability of stand-by systems. Studsvik used the FRANTIC

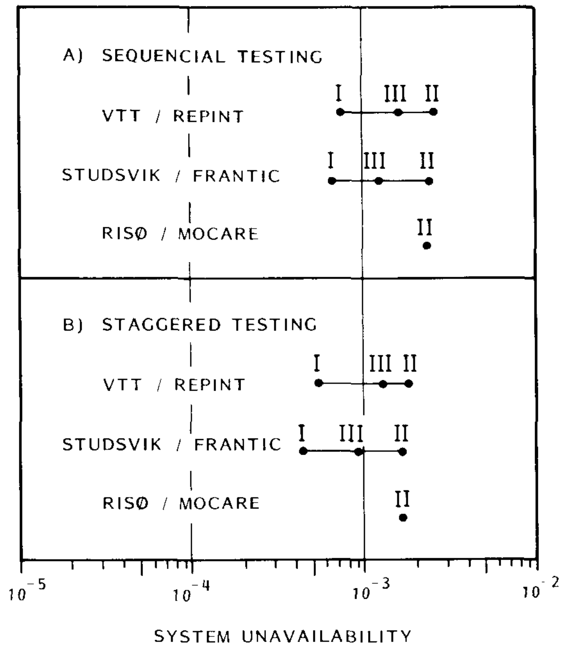


Figure 2.1.3 Benchmark 1 Study Results.
The numbers I-III refer to the results of the calculations using the different data sets.

code originating in the USA and based on the analytic calculation of the instantaneous unavailability of stand-by systems.

As shown in Figure 2.1.3 the results obtained by different codes using the same data set are generally in good agreement. The minor numerical differences seem to be caused by the specific features of the computing methods. These differences were considered too laborious to be tracked in more detail. In addition, the differences between the codes are small compared with the differences dependent on the choice of data sets.

The analytic method used by VTT proved to be more flexible in performing sensitivity studies and in obtaining intermediate results and detailed information on the contribution of different components and model parameters. In principle the same results could be obtained from the MOCARE and FRANTIC codes, but only with occasional reprogramming and more computer time. The reliability structure to be quantified was, however, quite small and extensive conclusions should not be drawn on the basis of this single trial.

2.1.3 General experience

One of the main findings of the first Benchmark study was the difficulty in specifying the work at the reliability model level. Construction of the models involves simplifications and assumptions that are not always explicitly specified and written down and different groups have developed their own practices. Once again it became apparent that the modelling phase is the most critical in reliability analysis. Investigation of the modelling uncertainties was set as the main task in the second Benchmark study.

The large uncertainty found in the case of compiling pipe failure rates resulted in anomalies when using the log-normal distribution model. In particular, when a few "samples" differ by a factor greater then 1 000, the mean of the distribution is greater than the 95 % confidence bound.

Detailed results of the Benchmark 1 study were presented at the 1982 Project Seminar and published in the seminar proceedings [2-1].

2.2 Benchmark 2 on system modelling

The second Benchmark study emphasized system modelling as opposed to model quantification. The general task selected was the analysis of transients in which feedwater is lost in a BWR plant, resulting in the need to depressurize the primary system to enable the use of the low pressure injection systems.

Background material for the study was delivered by Sydkraft Power Company for the Barsebäck Nuclear Power Plant, and by ASEA ATOM. The process diagram of the feedwater systems is presented in Figure 2.2.1. The AC electric power supply backed up by diesel generators and on site gas turbines were included in the analysis.

The original aims in Benchmark 2 were:

- Comparison of the different approaches in the systematic identification of potential failures, errors, and other hazards and evaluation of the completeness of the identification.
- Comparison of alternative methods for the modelling of complex event sequences.
- Independent quantification and comparison of computer codes.

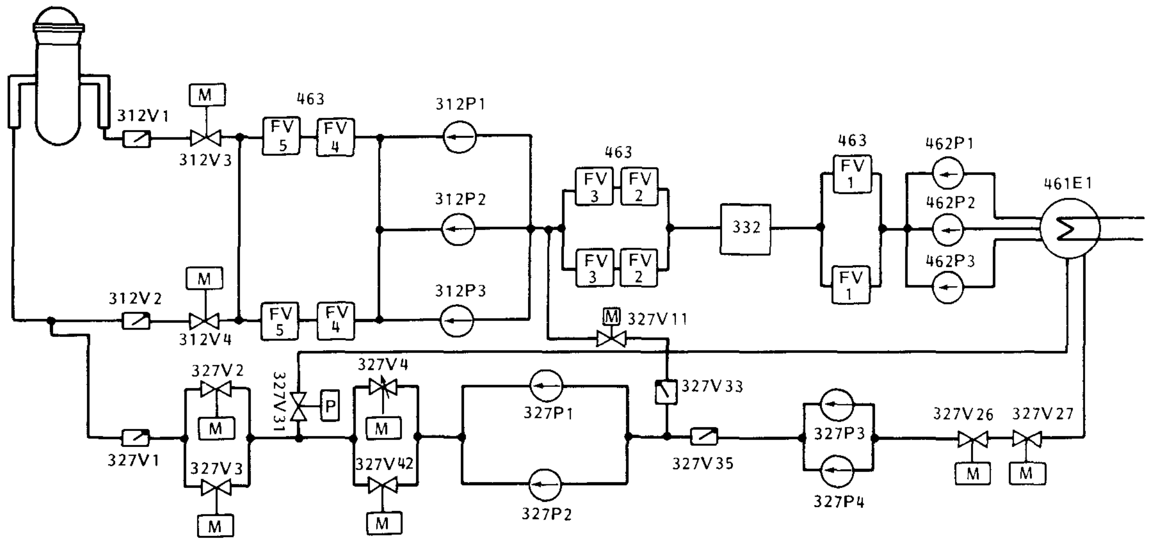


Figure 2.2.1 Barsebäck 1 Main (312 and 462) and Auxilliary (327) Feedwater Systems (BWR).

During the study the scope was limited to some representative transients. The transients were

- spurious or inadvertent A-isolation, i.e. trip of the main feedwater system (MFWS) with the possibility to restart it,
- loss of external grid.

A-isolation was selected because it is the most frequent initiator to loss of feedwater transients. Loss of external grid, on the other hand, is relatively unlikely but important from the safety point of view.

2.2.1 Identification of the initiating events

The scope of this task had to be significantly reduced because it was quickly realized that close co-operation with plant operators and designers was necessary if the task was to be completed with a reasonable effort. From a practical standpoint it was, however, impossible to arrange such support for all three research groups.

This task was thus limited to the analysis of the operating experience at the Barsebäck plant. The question of completeness in the identification of initiating and contributing events remained unresolved.

2.2.2 Modelling of the event sequences

All three research groups chose the conventional modelling approach where, at the plant response level, the event sequences are described principally by event trees or cause-consequence diagrams. At the second level, the events related to the failure or success of the front line safety systems are modelled down to equipment failure and operator error level by using fault trees or block diagrams.

For the first level models, the event sequences, the following modelling techniques were chosen.

VTT: event tree; the main argument behind the choice was to keep the models as simple as possible.

Studsvik: cause-consequence diagram; the ambition was to model recovery actions more in detail already at this level (in the quantification the dominant sequences were simplified into an event tree).

Risø: cause-consequence event tree (a computer-aided diagram combining several features of the above two); here also an attempt was made to model the recovery actions in detail.

At various times throughout the study the different models were compared. Both the techniques used and the experience and insight obtained from this comparison are discussed in more detail in Section 3.2.1.

During the course of the modelling work it was found necessary to fix many assumptions and boundaries for the analysis in order to prevent the models from diverging too much and to facilitate useful comparisons. Some of the main assumptions are listed in Table 2.2.1. This point should be strongly emphasized because in the course of a system analysis the analyst is always making simplifications, truncations, approximations and other types of assumptions which are often not documented.

Table 2.2.1

Assumptions and Boundaries for Benchmark 2

Assumption/boundary	Remarks
1. No high pressure make-up systems other than MFWS and AFWS are included.	Capacity of the other systems is relatively small and their use could only prolong the sequences slightly.
2. Reactor shutdown is sucess-ful.	Sequences with non-sucessful shutdown are quite different (and unlikely).
3. Island operation is not considered.	Not relevant for Benchmark 2.
4. Restoration possibility of the lost external grid is included in the models.	Restoration is quite likely and interesting from the modelling point of view.
5. Onsite gas turbines are included.	This is a likely way to restore the external power.
6. Successful operation of DC power supply to instrumen-tation is assumed.	DC power supply is backed up by batteries and highly reliable during the short interval of interest (20 min).
7. Water content in the turbine condenser is sufficient.	Loss of condenser inventory is relatively unlikely and not of special interest for Benchmark 2 purposes.
8. Plant protection system was not explicitly included in the models except local equipment protection and the interface relays for A-isolation.	Usually the logic systems do not contribute significantly; the Benchmark 2 resources did not allow a systematic checking of this assumption (although it is a very central one).
9. Operator actions are modelled in a functional way, i.e. only omission errors in the recov-ery actions are accounted for (control room actions only).	Benchmark 2 resources did not allow a deeper treatment of operator actions.
10. Maintenance errors are con-sidered.	Special emphasis on potential common cause failures.

2.2.3 Front line safety systems modelling

The second level models of the main and auxiliary feedwater systems and the electric supply system up to the boundaries agreed upon were modelled using

- fault trees by Risø and Studsvik groups,
- block diagrams by VTT group.

Very detailed fault trees were developed which covered about 100 pages. The block diagrams, on the other hand, were developed to the main equipment level with only principal system and equipment interactions included and took only 2 pages. The two approaches are quite different and are compared in more detail in Section 3.2.2.

2.2.4 Quantification

During the initial stage of the quantification each group compiled data for the basic events in their models. Thereafter, a common data list was agreed on for all the basic events that were common to all the models. Variations in data were smaller than in the Benchmark 1 study because all three groups used the Swedish Reliability Data Handbook as the primary source.

Although the quantitative results differed from each other, this difference was slight when taking into account differences in the modelling detail, treatment of operator errors, and common cause failures. In order to carry out a more objective comparison of the computer codes a model fault tree was developed on the basis of the Benchmark 2 study models and run with the same data. Results of this comparison are discussed in Section 3.5.

2.2.5 Experience from the analysis of operator errors

As a supplementary task in Benchmark 2, a selection of analyzed sequences were performed on a training simulator [2-3]. The simulations were performed in order to obtain a more illustrative picture of what is happening in the control room during the transients, what information is available to the operators, and how they identify the situation and recover the plant operations. To this end the simulator excercise proved very useful, especially for system analysts who did not have much practical experience with operator error analysis.

The information and insight obtained from the simulations were taken into account in the final checking of Benchmark 2 study models.

2.2.6 Completeness

The system models were compared prior to any thorough review process. Six significant differences were identified and are listed in Table 2.2.2. Two of them were omissions of hardware, while the rest involved incorrect modelling of the functional logic. It is interesting to note that only one of these differences had a significant impact on the quantitative results.

The number of differences observed here can not be used as an estimate of the error frequency in PRA work in general because the differences were discovered at an early stage in the modelling. It is likely that they would all have been identified and corrected during the review process which is typically performed during a PRA. However, the experience from Benchmark 2 once again highlights the need for a well organised review of a system analysis.

Table 2.2.2

Differences and incompletenesses found in Benchmark 2 models

Item	Sensitivity factor[1]
1. Check valve causing a single failure of MFWS (462V30)	0.7
2. Connection line from the condensate pumps to AFWS	1.1
3. Reverse flow in pump lines	0.9
4. Loss and recovery of the external power source	0.9 - 1.1
5. Automatic start signals	1.0
6. Operation mode switch of the MFWS pumps (running/stand-by selector)	14

[1] The following definition has been used:

$$\text{Sensitivity factor} = \frac{\text{Erroneous result}}{\text{Correct result}}$$

2.3 Summary of experience

The two Benchmark studies provided an excellent framework for applying different methods, data sources, and computer codes to practical problems and comparing the results. Thus they were of central importance in the NKA/SÄK-1 project.

During the Benchmark 1 study the sensitivity of derived failure parameters to available data was demonstrated. It is apparent that judgement plays an important role in calculating the parameters through the selection of data or even data handbooks. Once the data were selected, however, the various calculational techniques produce similar results.

In the Benchmark 2 study experience was obtained about the advantages and limitations of different modelling methods and approaches. Although the final models were similar with respect to the major contributors to system failure, they differed considerably in most other respects. Many of the differences, however, can be attributed to the lack of continuous communication with the plant, utility, or vendor. Hence, although scoping models may be possible from the documentation alone, detailed models should not be attempted without this communication.

Regarding the modelling techniques themselves, it appears that familiarity with the technique is the most important factor for ease of model construction and review. Block diagrams appear to be easier to work with for simple systems but can become logically quite complex for more complicated systems. Similarly, cause-consequence diagrams allow a more compact evaluation of the many possible event sequences but can also become very difficult to manage for complex systems.

It is interesting to note that the group using the success oriented model (block diagrams) included a success path not included in the fault trees. Conversely, the groups using the failure oriented model (fault trees) included a failure path not included in the block diagram model. Hence, although both techniques are capable of modelling the same events, it appears that the strategy behind the techniques may influence what events are included.

The large system models provided good test cases for the comparison of various computer codes. In fact, during the course of the study, the computer codes were continuously improved in order to handle large models more efficiently by, for example, the use of modularization. As an alternative, support states were used to split the large models into smaller ones which could then be managed by the existing computer codes in a reasonable time.

REFERENCES

2-1 "Probabilistic Risk Assessment and Licensing", Proceedings of project seminar 2, Helsingør, Risø National Laboratory-M-2363, 29-31 March 1982.

2-2 MANKAMO, T
"Summary Report of Benchmark 2 of NKA/SÄK-1". Technical Research Centre of Finland, Report NKA/SÄK-1-F(84)1, Feb 85.

2-3 DINSMORE, S C
"NKA/SÄK-1 Simulator Exercise and Results". STUDSVIK/NR-84/355, SÄK-1-S(84)1, April 85.

3. COMPARISON OF METHODS

A reliability analysis of large technological process systems such as nuclear power plants is a complex process. Experience in performing such analyses throughout the world has lead to the definition of several analysis areas and resulted in the generation of alternative techniques to address each area. In general, methods do exist to address all problems although some require approximations and/or simplifications. In practice, the choice of a specific method is often a matter of preference and familiarity.

3.1 Fault identification

The construction of system models, illustrated in Figure 3.1.1, allows the systematic identification of causes of failure for complex systems. To construct a model, both the operational requirements and the possible failure modes (or faults) of the components are required. Thus the identification of which basic fault events (component failure modes, human actions, etc) should be included in the system models is a basic part of any analysis. One very important class of faults, common cause initiators, is discussed in detail in Section 3.3.10.

Several different methods, manual as well as computer aided, are available to help with the identification of faults. Selection of which method to use should be made with due consideration of the circumstances of each problem. Often the use of several different methods in combination is necessary.

It should be emphasized that even the most advanced methods can not guarantee the completeness of the results. Good documentation, including a clear

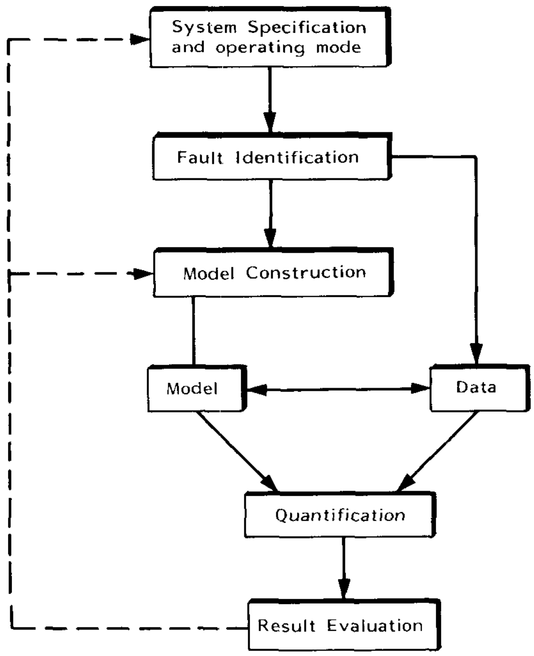


FIGURE 3.1.1 System Analysis Flow-chart
The solid lines indicate the initial construction process and the dashed lines the checking process.

specification of the failure search strategies applied, in addition to a careful independent review can, however, ensure the quality of the work.

3.1.1 Search methods

The methods used for fault identification and those used for system modelling should not be stringently separated. The latter methods support the former ones in many cases by highlighting some, but not all, areas which need closer investigation.

3.1.1.1 Failure mode and effects analysis

Failure mode and effects analysis [3-1] is always used during analysis of a system; either explicitly using tables and forms [3-2] or implicitly using experience.

The principle of the method is to examine every component in the system and ask the questions:

How can this component fail?
What will happen if this component fails?

As an aid in documenting and completing the analysis, results can be recorded in a tabular format.

Application of tabular formats is recommended since a systematic recording of all failure modes analysed is a valuable part of the documentation, particularly when addressing completeness. An example of such a format is presented in Table 3.1.1.

3.1.1.2 Hazards and operability study

The hazards and operability analysis method [3-1, 3-3, 3-4] is a procedure currently in wide use throughout the chemical industry. It should be noted, however, that the term hazards and operability study is used in design, construction, and operation of plants and not just for disturbance analysis.

As in a failure mode and effects analysis, each component in a system is considered in turn. However, instead of considering only equipment faults, a systematic search procedure is used to identify potential deviations in each process variable (flow, pressure, temperature, etc), using prescribed tabular formats and check lists.

COMPONENT IDENTIFICATION	STATES FUNCTIONS	FAILURE MODES	FAILURE CAUSES	TEST AND MAINTENANCE FREQUENCY	FAILURE EFFECTS ON ASG	EFFECT ON OTHER SYSTEMS (optional)	FAILURE DETECTION POSSIBILITY	OPERATOR ACTIONS	NOTES
No. xxx Globe Check-valve	Prevention of reverse flow	Fails to open	Mechanical blockage	Annually	Loss of one pump line	None	Low flow alarm	None possible	To be included in the fault tree
		Fails to close	" - "		Reverse flow if pump in the same line fails to op.	" - "	Low flow alarm + low pressure on meter	" - "	" - "
		Disruption of globe	Corrosion Water hammer		The globe may be moved to the T-joint blocking the common pipeline of the system	" - "	" - "	" - "	Possible effects should be investigated further.
		External leakage	Wear of Seal		Minor	" - "			Not to be included in the f.t.
			Disruption of housing		Loss of system function	" - "	" - "	" - "	Probability too low to be included in the f.t.

Table 3.1.1. Example on the application of the Failure mode and effect analysis format.

The deviations are recorded using a cause-consequence-cure format. The analysis is documented in detail, which is an important aspect in ensuring an adequate analysis. An organizational technique using action sheets to ensure that areas of doubt are investigated has been found to be particularly useful when several people are involved in an analysis.

The hazards and operability analysis method was used extensively in the SCRATCH project and the experience obtained reported in [3-3].

3.1.1.3 Check lists

Check lists can be used as an aid in the identification of failures. Check lists are available for various categories of failures such as the circumstances for occurrence of a fire or the failure modes for failure of pressure boundaries in components. A danger in the use of check lists is, however, that the analyst may restrict the search to those items in the check list [3-1]. One alternative which avoids this problem is to use check lists during the review, instead of during the initial analysis.

3.1.1.4 MORT

The management oversight and risk tree (MORT) is a logic tree for organizing administrative strengths and/or weaknesses to allow specific recommendations to improve management control [3-5]. The method is applied by using checklists which address management control over various tasks.

3.1.2 Operating experience

Utilizing operating experience related to the system under analysis is highly recommended in order to make the analysis as realistic as possible. This experience is available to a limited extent through failure reports. However, interviews of operating personnel or reviews by the operating personnel of the documentation of an analysis are generally much more useful.

It should be noted that operating experience for the entire system can be used only as a supplement to an analysis. It can only stand alone in exceptional cases where the operating experience is sufficient for calculation of statistical failure data for the system. Care should be taken to ensure that the operating experience utilized concerns either the same system/component as the one analyzed or a similar system/component operated under similar conditions with respect to operating procedures, maintenance, testing, and environment.

3.1.3 Onsite inspection

Experience shows that it is impossible to identify all potential failure and hazard causes from drawings and flow sheets alone. Methods have been developed for systematic onsite inspection such as walk through and inspection check lists [3-1]. In particular, onsite inspection is useful for identification of certain types of dependent and common cause failures occurring in components which are located near each other.

3.1.4 Computer aided methods

Automatic and computer aided methods are useful for identification of failures and ensure a consistent level of resolution throughout the analysis. Although manpower requirements for an analysis are similar, the quality of the result using computer codes is less dependent on the experience of the analyst.

One example of automatic fault tree construction is the RIKKE program [3-6]. A system flow sheet is constructed interactively on a graphic terminal by selecting from a library of component modules and defining their input and output relationships. The program then draws from a library of failure modes to construct a fault tree. It can analyze mechanical and electrical systems and operating procedures.

3.2 Sequence and system modelling

Modelling methods currently used in PRA studies fall into two main categories:

1. Methods for the description of event propagation:
   - event tree (ET)
   - cause-consequence diagram (CCD)

2) Reliability models of systems:
   - fault tree (FT)
   - block diagram (BD)
   - GO-chart (GO)

An additional method, the state model, can not be included in either group. The state method is an auxiliary method which is used in connection with system reliability models. It can be useful in the quantification of complex minimal cut sets but increases the complexity of the calculations.

Event and fault tree formats are the most common but the best point to end one format and begin the other can not be exactly specified. The description of event propagation and plant response is done using both types of methods in combination and they can be used in different proportions to each other (Figure 3.2.1). In fact, this is the key problem in modelling: what should be included in event sequences and from where to begin detailed system modelling.

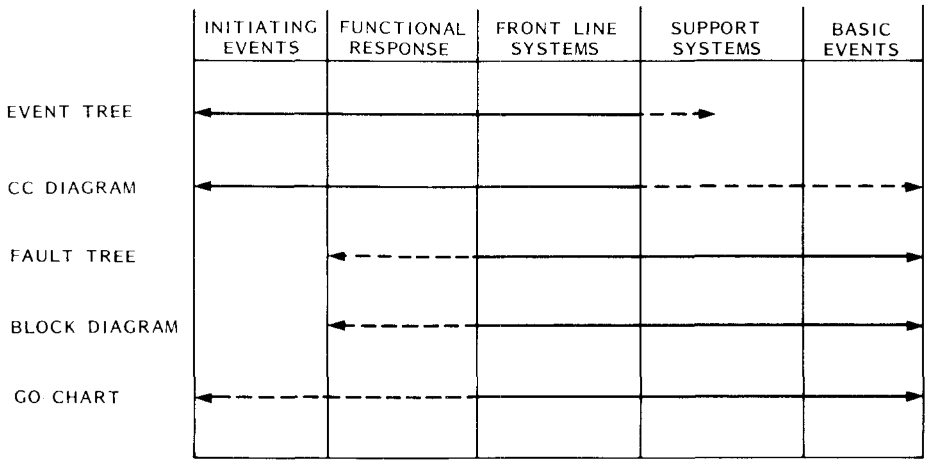


FIGURE 3.2.1 Nominal Ranges for Modelling Techniques. Solid lines commonly used, dashed lines potentially used.

Different approaches to modelling and the benefits and limitations of available methods will be illustrated by examples based on the Benchmark 2 Study. In the examples, a configuration of the main feedwater system (MFWS) and auxiliary feedwater system (AFWS) are considered together with the electric supply system (ESS).

In Sweden, fault trees and event trees have been used in all PRA's. A standard fault tree format has been selected (see Figure 3.2.5) and several similar component/failure mode naming schemes have been developed and incorporated in the data base manipulation codes [3 - 45].

3.2.1 Event sequence modelling

In the traditional modelling approach, originating in the Reactor Safety Study [3-7], event trees and fault trees are used in combination. An event tree used to describe the functional response of the plant in the Benchmark 2 Study is presented in Figure 3.2.2.

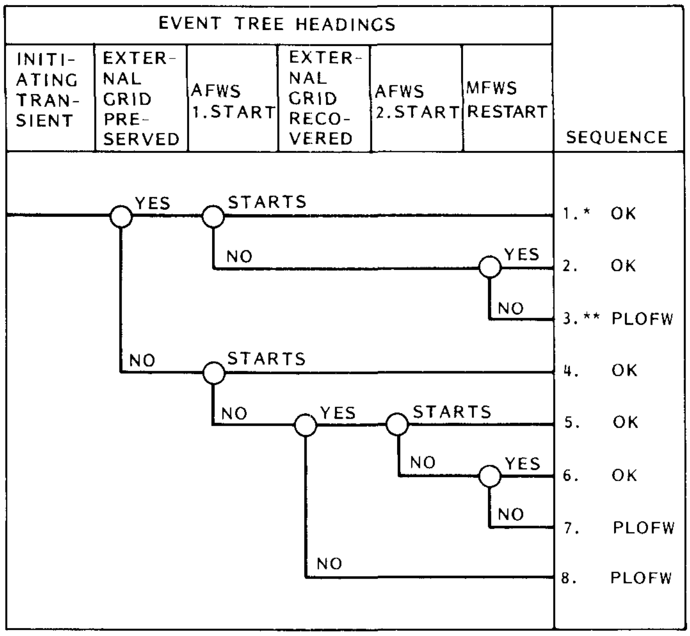


Figure 3.2.2 Sample Event Tree.
The initiating event includes trip of the reactor, turbine and MFWS.
* High Pressure Feedwater available
** Prevaling Loss of Feedwater (Depressurization required).

The event tree headings are arranged either in chronological or causal order. Headings can be systems' status, basic events, or operator actions. Systems' status are usually developed down to the component and action level in fault trees, basic events are quantified from data, and operator actions are developed with human reliability techniques. Note that fault trees are composed of essentially the same items and this contributes to the difficulty of deciding what should be included in the fault trees versus the event trees.

In Figure 3.2.3 a CCD corresponding to the event tree in 3.2.2 is drawn with the operator actions modelled in more detail. In a more complicated case, CCD usually results in more compact models because parallel branches can be grouped together by logical gates and treated as a single entity. However, ET is the most simple model because there is only one logical operator: YES/NO-branching.

The compactness of CCD compared with ET also has its drawbacks. Grouping of the branches makes sequence by sequence review difficult and may cause some dependences to be overlooked. During quantification the CCD must be restructured into alternative, mutually exclusive branches (i.e. to an ET effectively) in order to account for the dependences. Thus the use of CCD is typically reduced to qualitative use only, or as an intermediate modelling stage.

There are several intrinsic problems in ET construction. No universal solutions can be presented and the optimum approach varies from case to case. The main problems and some recommendations on how to address them are discussed below.

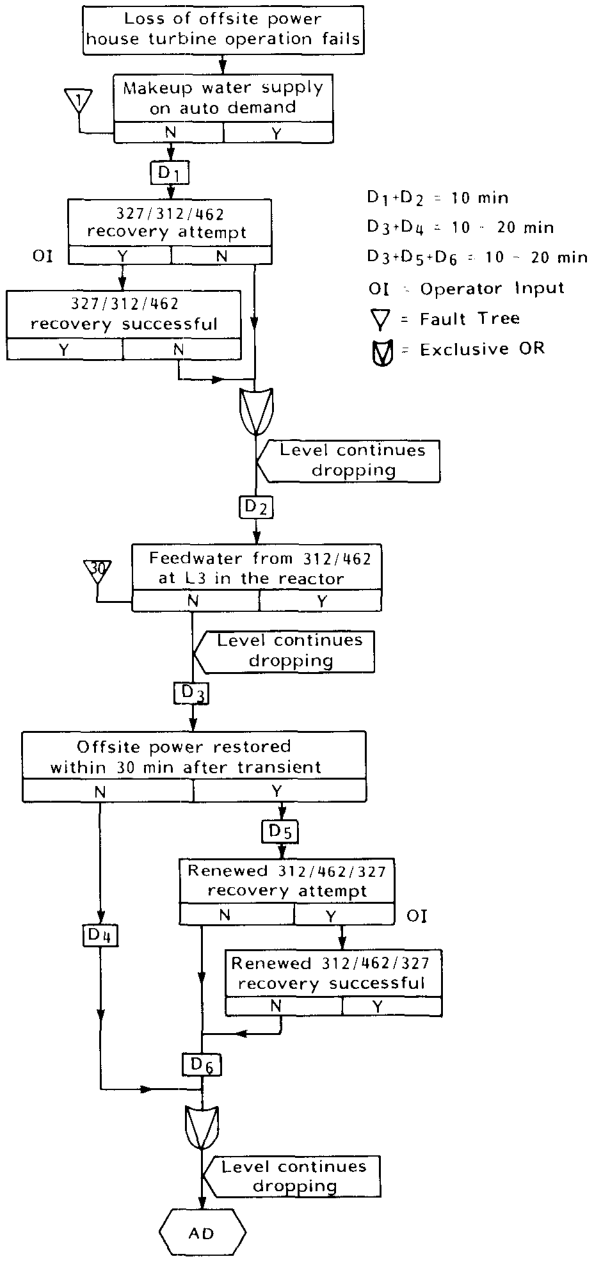


Figure 3.2.3 Sample Cause-Consequence Diagram. Time delays and recovery events included.

AD = Automatic Depressurization

ET branches are related to the success/non success of the events represented by the headings. The success criteria for a specific ET heading may depend on the events placed earlier. This is not usually indicated explicitly in ET but should not be overlooked in quantification. Principally, the success criteria are defined for each single sequence individually and can thus be handled correctly.

Another problem is how to correctly treat shared equipment and other system interactions. In the Benchmark 2 study problem, for example, one sequence cut set included the failure of one train of MFW, one train of AFW, and loss of an electric bus which supplied the other trains in each system. In this case none of the individual systems has completely failed but the combination of partial failures leads to the failure of the required function. This means that ET should be interpreted as a functional model only and that reduction and quantification in the general case must be done for entire sequences.

The shared equipment and system interactions are treated in the traditional approach in such a way that

1) most important interactions are included as ET headings,

2) other dependences, such as low level shared equipment, are included in the fault trees. In the quantification, the fault trees involved are joined by an AND gate and the large fault tree is handled by a computer program in order to obtain the correct cut sets.

An alternative has been used in some recent PRA studies:

3) dependences between several safety systems are described by support states: a typical example is the availability of the electric power at different buses.

In the third approach the fault trees for ET headings - in some case even the event trees -are drawn conditionally for each support state. This may easily result in very tedious work. For example, the number of main electric buses ranges typically from 6 for two train systems to 12 for four train systems: if they are treated by using support states then 2^6 to 2^{12} states need to be defined. Although there is a certain degree of symmetry between the states, the number of different states to be treated becomes several tens at least. This results in laborious matrix arithmetics during quantification, which tends to obscure the engineering insight that could be gained from event trees.

On the other hand, the problem can not be solved by incorporating all dependences in ET headings because system interactions are usually present at the subsystem level and often at the equipment level. Event trees could easily become very long and difficult to manage.

In event sequence modelling a proper balance should be found between the detail and compactness of event trees. This means that ET headings should include at least the response of the front line safety systems and (only) the most important shared equipment at support system level.

3.2.2 System reliability modelling

In order to aid in the discussion of system models, a section of the AFW in Figure 2.2.1 is expanded and reproduced in Figure 3.2.4. A fault tree for this section is presented in Figure 3.2.5. As an alternative to fault trees, block diagrams (BD) can be used for detailed modelling. A block diagram corresponding to 3.2.5 is shown in Figure 3.2.6.

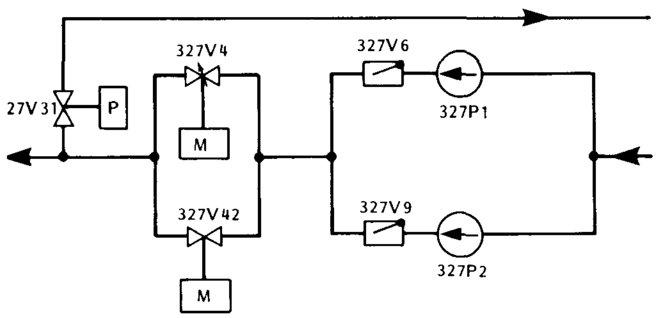


Figure 3.2.4 High Pressure Section of AFWS (BWR). Expanded section of Figure 2.2.1 used to demonstrate modelling techniques.

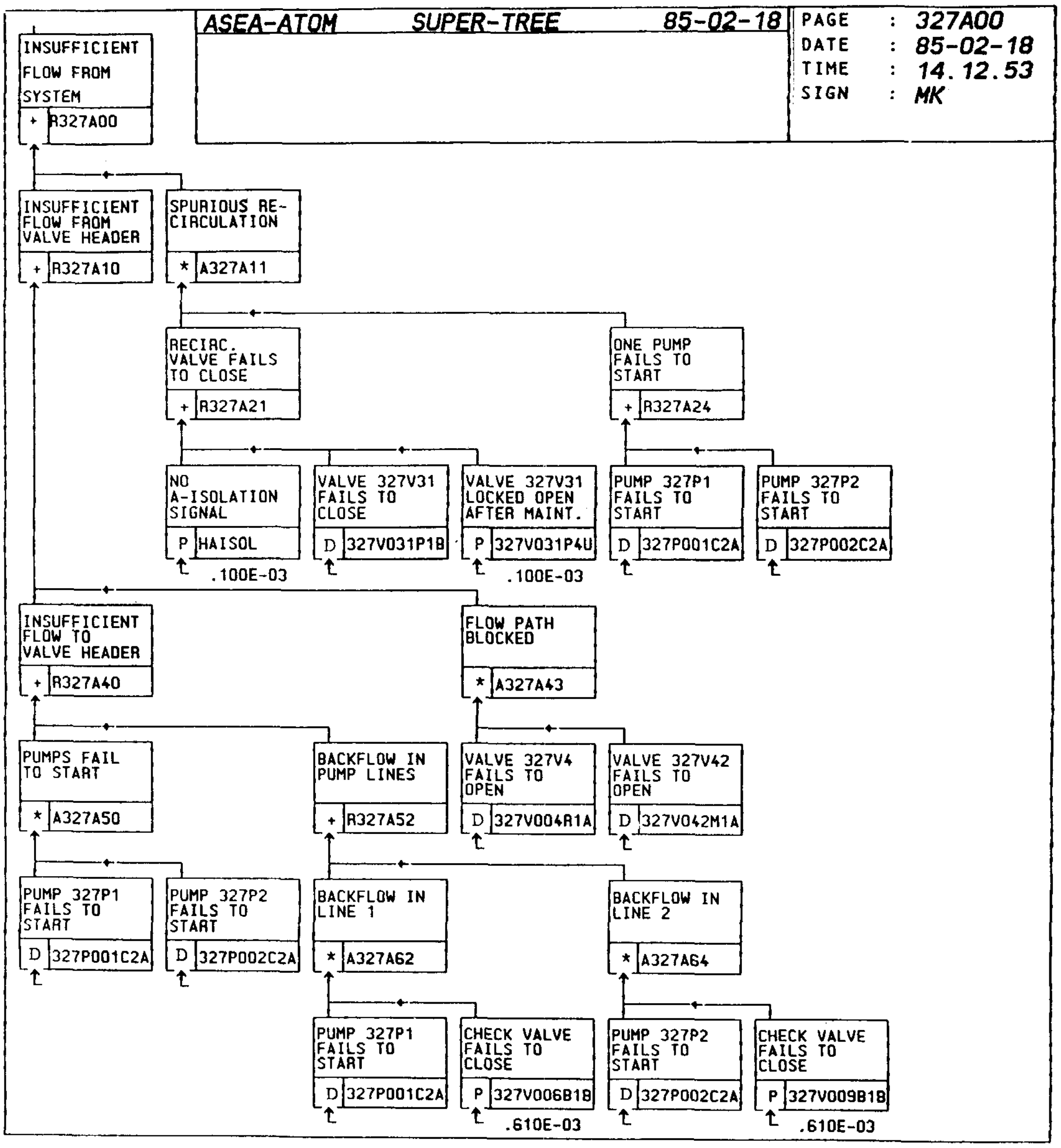
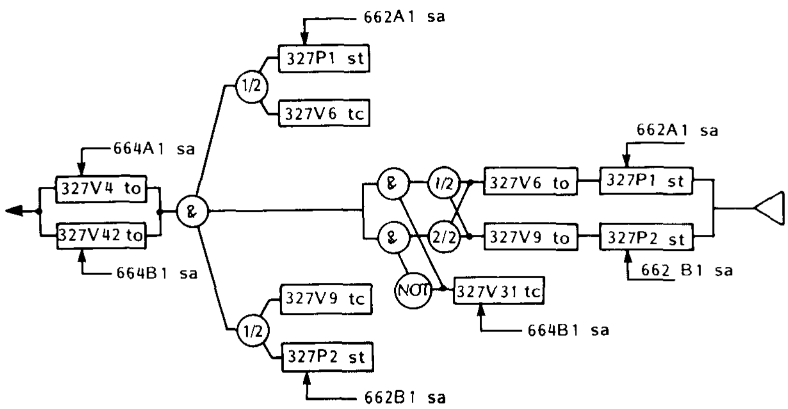


Figure 3.2.5 Fault Tree for Figure 3.2.4

D = Transfer
P = Primary event
+ = OR gate
* = AND gate



SUCCESS MODE LEGEND

st = starts
to = transfers open
tc = transfers closed
sa = supply available

Figure 3.2 6 Reliability Block Diagram
The diagram includes the section of the AFWS in Figure 3.2.4. The necessary power inputs are represented by arrows into the sides of the block. The diagram is drawn from right to left to enhance comparison with the process diagram.

The reliability BD is typically more compact than the fault tree. This is achieved at the cost that component failure modes (or other events in the model) are not explicitly written down in the BD. This has its drawbacks because important assumptions which might be apparent from the text could be missed.

The BD may follow the physical structure of the systems closely. This makes a BD easier to understand and check against system drawings. In complex structures, however, the physical structure can not be strictly followed: typical examples are back-flow possibilities in pump lines which are included in the examples given.

Thus it seems that the BD is a preferable model for systems with relatively straightforward functional logic. However, the deductive construction philosophy of fault trees makes them recommendable in cases of complex functional logics.

3.2.3 GO method

The GO method [3-8] is a success diagram which is much more general than a BD. There are 17 GO-operators available as diagram elements in the GO computer program compared with 5 for a BD.

GO charts can also be used to model the event propagation. The example event tree of Figure 3.2.2 is translated into a GO-chart in Figure 3.2.7. For convenience the success definition is written under each operator. The GO-chart is not very illustrative. When used for event sequence modelling GO-charts become quite similar to fault trees: plenty of AND- and OR-operators are used.

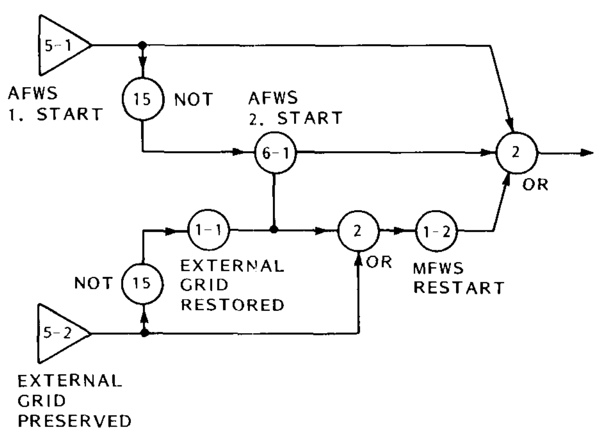


Figure 3.2.7 GO Event Sequence Model.

The use of GO as a system reliability model is illustrated in Figure 3.2.8. In this case the repetition of the same basic event is avoided by using complicated logical structure to model the back flow cut sets. Another alternative would be a structure similar to that of a BD, Figure 3.2.6.

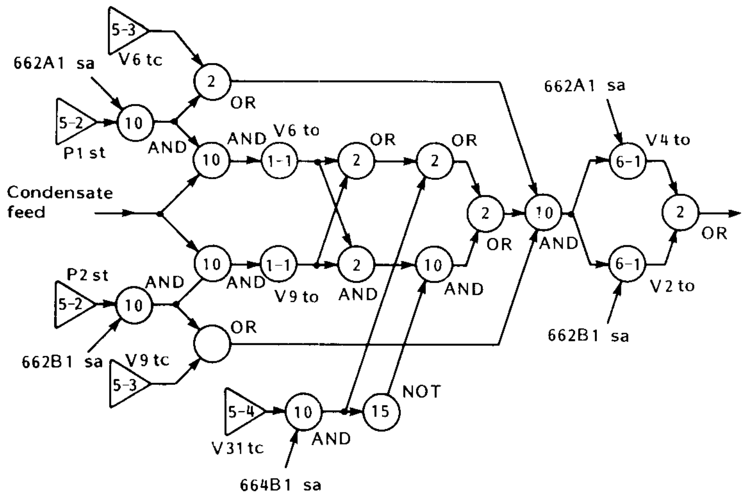


Figure 3.2.8 Go-Chart.
The diagram includes the section of the AFWS in Figure 3.2.4. The legend for the abbreviations is given in Figure 3.2.6. The diagram is drawn in the conventional direction from left to right.

3.3 Dependent failure analysis

The use of redundant and diverse systems to provide reactor safety functions has effectively reduced the probability of independent failures leading to reactor accidents. The complexity of the design, however, creates a potential for dependencies between and within the systems which may have a decisive influence on the reliability. Design defficiencies, external phenomena (including events like earthquakes, fires, etc), functional deficiencies and human factors (e.g. installation, manufacturing, testing, maintenance and operator errors) are typical causes of dependent failures.

The importance of multiple failures has already been demonstrated by reactor operating experience, and dominating accident sequences frequently involve multiple failures. Dependencies tend to increase the frequency of multiple concurrent failures; therefore, treatment of dependencies should constitute a crucial part of any PRA study. A general assumption of independence between systems (components) is non-conservative and usually leads to excessively optimistic results.

A comprehensive discussion of difficulties encountered in the practical analysis of dependencies may be found in [3-9]. In addition, several specific recommendations concerning different problem areas have been given.

3.3.1 Definition

Problems associated with the choice of terminology and definitions have sometimes led to confusion. Several types of dependent failures exist, namely: common cause failures (CCF's), common mode failures (CMF's), cascade failures, shared equipment dependencies.

Common cause failures have attracted much attention since special methods are required for their treatment. According to a general definition, common cause failures are multiple failures at the same time (occur simultaneously or in a short time interval) which are attributable to a common cause. Such a rather inclusive definition seems adequate for the performance of PRA studies, where all potentially significant CCF's are to be identified. A more exclusive definition may be necessary for identification of CCF's in the available data bases in order to reduce the potential for different interpretations of the same material. Although it is not absolutely necessary to have a unique and precise definition, each analyst should specify which definition he is actually using. This applies to reviews of the data bases as well as to the PRA studies.

A clear distinction should be made between common cause failures and common mode failures. The latter group of failures is a subset of CCF's, which only strikes identical redundant components or systems. In thorough studies of dependencies the term "common cause" should be used, since the aim of such analyses is to identify dependencies among all components and not just similar components.

Cascade failures are a sequence of two or more failures in which each failure results from the preceding one. Shared equipment dependencies occur when the same equipment is shared by more than one system. These failures can be successfully handled by independent failure models which explicitly incorporate fault propagation paths. Nevertheless they are sometimes classified as CCF's. The differences in classifications are of little importance as long as all types of failures are treated consistently treated.

3.3.2 Classification

Dependent failures are usually subdivided into several categories in order to facilitate performance of the analysis. The set of classes of CCF's proposed by the CSNI Task Force on Rare Events [3-10] is based on different mechanisms constituting the cause of dependency. The classification of the PRA Procedures Guide [3-11], made with consideration given to the available methods for analysis, concerns general dependent failures which include all types of system interaction. The system in the PRA Procedures Guide is more helpful for structuring the problem and identifying the main risk contributors than for making a proper classification.

3.3.3 Methods for qualitative analysis

Available methods for qualitative common cause failure analysis (CCFA), i.e. methods primarily used to identify CCF's, may roughly be divided into three groups:

- "think-through" and "walk-through" analyses
- modified fault trees [3-7]
- generic cause approach [3-12].

"Think-through" and "walk-through" analyses represent an engineering approach to the problem and rely heavily on detailed knowledge of the process or plant to be analysed (including operating experience). The main advantages of these two methods are that they are fairly simple to apply and do not normally require large resources of manpower and computer codes. Even if completeness can not be guaranteed, the level of confidence may be considerably increased by application of systematic procedures based on extensive use of check lists, questionnaires, etc. Figure 3.3.1 illustrates one such check list [3-13]. The method is purely qualitative and requires incorporation of dominant CCF contributors into the original fault trees in a fashion similar to what is done in the modified fault tree method. Extensive use of systematic "think-through" and "walk-through" analyses is strongly recommended.

DATE:83-05-04
SYSTEM: 327
SIGN: SH

CHECK LIST ATTACHMENT 1

DEPENDENCY / REDUNDANCY	PROXIMITY	SEPARATION	NORMAL EXTERNAL ENVIRONMENT: GRIT	NORMAL EXTERNAL ENVIRONMENT: HUMIDITY	NORMAL EXTERNAL ENVIRONMENT: CHEMICAL REACTIONS	NORMAL EXTERNAL ENVIRONMENT: VIBRATION	NORMAL EXTERNAL ENVIRONMENT: TEMPERATURE	NORMAL EXTERNAL ENVIRONMENT: RADIATION	FACILITY-RELATED EXTERNAL PHENOMENA: FIRE	FACILITY-RELATED EXTERNAL PHENOMENA: IMPACT	FACILITY-RELATED EXTERNAL PHENOMENA: ELECTRICAL INTERFERENCE	FACILITY-RELATED EXTERNAL PHENOMENA: LEAKAGE	HUMAN ERROR: MANUFACTURE INSTALLATION	HUMAN ERROR: TEST MAINTENANCE REPAIR	COMMENT
Auxiliary feedwater pumps P1,P2	X	non-exist.							X 4	X 2	X 3	X 4	X 2	X 3	Short circuit, may influence surveillance equipment Leakage; drain connected to system 345
Auxiliary condensate pumps P3,P4	X	non-exist.				X 2			X 2				X 2	X 2	The pumps have never been subject to maintenance or repair
V2,V3	X	non-exist.								X 3			X 2	X 3	
V4,V42	X	non-exist.							X 4	X 2	X 3	X 4	X 2	X 3	Same environment as P1 and P2
V28,V29	X	non-exist.				X 2			X 2				X 2	X 2	Same environment as P3 and P4
V26,V27	X	non-exist.				X 2			X 2				X 2	X 2	Same environment as P3 and P4
K105,K106	X	non-exist.							X 4	X 4	X 4	X 2	X 2	X 3	Impact - missiles from pumps; exposed location
V6,V9	X	non-exist.							X 2	X 3			X 2	X 2	
V15,V17	X	non-exist.				X 2			X 2	X 2			X 2	X 2	
K113,K114	X	non-exist.							X 4	X 3	X 4	X 2	X 2	X 3	

Figure 3.3.1 Identification of potential dependencies [3-13]. A six degree scale extending from 1 (insignificant) to 6 (large significance) has been used for assignment of ranks.

The modified fault tree method incorporates dependencies into the logical model through modification of the original fault tree. Since the decision of which dependencies to model must be made by an analyst and the modification may depend on the tree structure, it may be difficult to ensure a systematic approach in the application of the method. In addition, analysis of the resulting large fault trees can be costly and time consuming. However, if this method is used to identify CCF-contributors, it may also be used for quantification since the CCF's have already been incorporated into the fault trees.

The generic cause approach is based on analysis of dependencies within minimal cut sets. Therefore, no insertion of potential CCFs into the logic model is necessary. Computer codes may be used to automate the analysis to a large extent, as discussed in Section 3.3.6. This approach can easily be extended to include quantification. The technique is extremely systematic, which creates a potential danger that the analyst is systematically missing some important items. Therefore, "think-through" and "walk-through" analyses should be performed in parallel.

A combination of available methods for qualitative CCFA seems to be the optimal approach to the problem, since each technique has some special drawbacks and merits. A reasonable methodology may involve systematic "think-through" and "walk-through" analyses supplemented with a limited scope generic cause approach.

3.3.4 Screening

Independently of which qualitative method is chosen for CCFA, great importance must be given to the screening procedures for elimination of insignificant dependencies. Otherwise the problem becomes impossible to handle. The necessary sorting can make use of the physical location of the components, the existing barriers, etc. Great care must be taken when screening procedures are applied. The risk of excluding significant contributions is considerable.

3.3.5 Human error as a cause of CCF

Human errors connected with testing, maintenance and operator actions constitute one of the dominating causes of dependency. There is an enormous number of failure modes which may be caused by the human factor and a very wide spectrum of hypothetical unusual situations. Techniques for qualitative and quantitative analysis of simple human errors are available, but these techniques are not very useful for addressing errors which can lead to common cause failures.

3.3.6 Computer codes for CCFA

A number of computer programs based on fault tree techniques have been developed to aid in the explicit modelling of multiple failures using the generic cause approach. The SETS code seems to be most widely used among the programs having CCF options. The principles and capacity of other codes (BACFIRE, COMCAN) used for dependent failure analysis are similar to those of SETS. The positive features of SETS include generality, flexibility, capability of handling large and complex fault trees, and screening ability [3-43].

The key disadvantage is that all the codes produce vast amounts of qualitative information about the potential for CCF's which is extremely difficult to prioritize and use. Therefore, the computerized CCFA should be performed with caution and interact with the manual work [3-44].

3.3.7 Methods for quantitative analysis

Among different quantitative methods used for absolute prediction of CCF contributions the following have been frequently used:

- square root method [3-7]
- beta-factor method [3-14]
- Marshall-Olkin specialization [3-15]
- common load model [3-16]
- Markov models [3-17].

The square root method, which only requires independent failure probabilities, has been criticized for its arbitrariness. The other techniques have different merits and disadvantages. Concerning the choice of the optimal quantitative method, the availability of data is a decisive factor which usually does not justify using sophisticated models. Thus, if possible, methods utilizing only few parameters (e.g. the beta-factor model), should be used. As noted in [3-9], the beta-factor method was developed for systems with only two trains. Consequently, direct application of the method to systems with higher redundancy leads to excessively conservative predictions. It is extremely important that the analysts are aware of the weaknesses and limitations of the models applied.

Recently, higher order models, namely the Multiple Greek Letter Method [3-18], Multiple Dependent-Failure-Fraction Method [3-19], and Additive Dependence models [3-20] have been developed. These models, when applied to systems characterized by a high level of redundancy, provide more realistic estimates of system failure probabilities than traditional one-parameter methods [3-21]. A recent workshop was dedicated to a thorough study of methods for quantitative CCF analysis [3-20].

Since lack of data constitutes the most serious limitation, common to all parametric methods, sensitivity analysis is strongly recommended. It allows the analyst to get a better feeling for uncertainties and weak points, and to try different models, data sets and assumptions. Usually, the results obtained by means of sensitivity analysis can be easily interpreted and decisions may be made regarding the necessity of further investigation. In some cases it may be more practical to introduce system modifications or apply defensive measures than to attempt an absolute failure prediction.

3.3.8 Data sources

Limitations of available data sources stand out as the weakest link in the current state of CCF quantification. Definitely most information is available on diesel generators [3-22] which are particularly suitable objects for the study of dependent failures. Some compilations also deal with pumps, valves, instrumentation and control assemblies. There are considerable discrepancies between the reported probabilities of multiple failures. Also the range of obtained values of CCF parameters (e.g. beta-factor) is very broad. Several sources of uncertainty have been identified: use of different CCF definitions and different classification schemes, ambiguity in the event description, differences in sample sizes, plant-to-plant variation, use of different models for CCF estimation.

The urgent need for reliable generic component parameters, cause related data, and component-specific models and data is apparent.

3.3.9 External events

There is a wide spectrum of external events which should be considered as potential causes of dependent failures. These include earthquakes, fires, flooding, tornados, hurricanes, lightning, airplane crashes and exploding gas clouds. Experience from safety analyses of many plants shows that facility- and site-related external phenomena may constitute the dominant contributors to the total risk.

The methods for treatment of external events in risk studies have been thoroughly described in PRA Procedures Guide [3-11]. Most of the external events are modelled by developing hazard curves (relating severity of the event to its frequency of occurrence) and fragility distributions for structures, systems and/or components (relating the probability of failure to the severity of the hazard). For each potential accident sequence, the hazard curves are combined by mathematical convolution to estimate the frequency of the accident sequence due to the considered external event.

The sophisticated approach to analysis of external events, based on computerized techniques, is not always needed. "Think-through" and "walk-through" analyses may lead to very qualified work.

The treatment of external events having large magnitudes entails a certain degree of subjectivity, since data on the occurrence of such low probability events are scarce. However, the use of a probabilistic approach for the analysis of external phenomena is in many cases better supported by data than the corresponding analysis of familiar internal events (e.g. large LOCAs).

It should be kept in mind that defensive measures (physical separation in particular) provide a very effective protection against most of the external events.

3.3.10 Common cause initiators

In PRA the identification of events which may initiate accident sequences is of central importance. In addition to conventional LOCA and transient initiators there exist disturbances and failure combinations which are much more difficult to discover and which directly affect several safety systems and thus contribute significantly to the core melt probability. Of particular interest are the so called common cause initiating events which require function of a safety system yet at the same time cause unavailability of this system. Latent design errors may contribute to the occurrence of common cause initiators.

3.4 Human error analysis

Human errors at power plants include maintenance or repetitive errors and operational or non repetitive errors. Maintenance errors of commission and errors of omission are usually included. However, operational errors of commission and recovery actions have recently been addressed [3-23, 3-24].

There are many different ways of addressing human error [3-11, 3-25]. Selection of the most detailed method to address all errors would require a prohibitive expenditure of manpower. However, the exclusive use of the simplest method may not accuratly reflect the expected frequency of the errors. A mix of the various techniques, depending on the impact of the errors, is suggested.

3.4.1 Identification of important human errors

In the same way as basic failure event identification, human error identification can be simplified with the use of tables and checklists. An example of a checklist to evaluate operator actions and hence illustrate typical errors and the underlying factors contributing to the errors are given in Figure 3.4.1 [3-26].

Since maintenance errors are associated with components they are usually included in the fault trees. Systematic maintenance errors, due either to management policy or similar task dependence, should be considered. However, if sufficient plant specific information is available, maintenance dependencies may already be included in component common cause failure events. If a simple and conservative estimate of maintenance error probability is made first, additional analysis can be performed on any errors which contribute greatly to the system unavailability.

Operational errors are usually included at the event or function tree level but, in some cases, may be placed in the fault trees. If included in a fault tree, their importance can be assessed in the same way as maintenance errors. If included in the event or function tree, however, it may be necessary to estimate the importance of the error before quantification. Unlike system analysis, accident sequence analysis can be so complex that it is impractical to repeat the analysis.

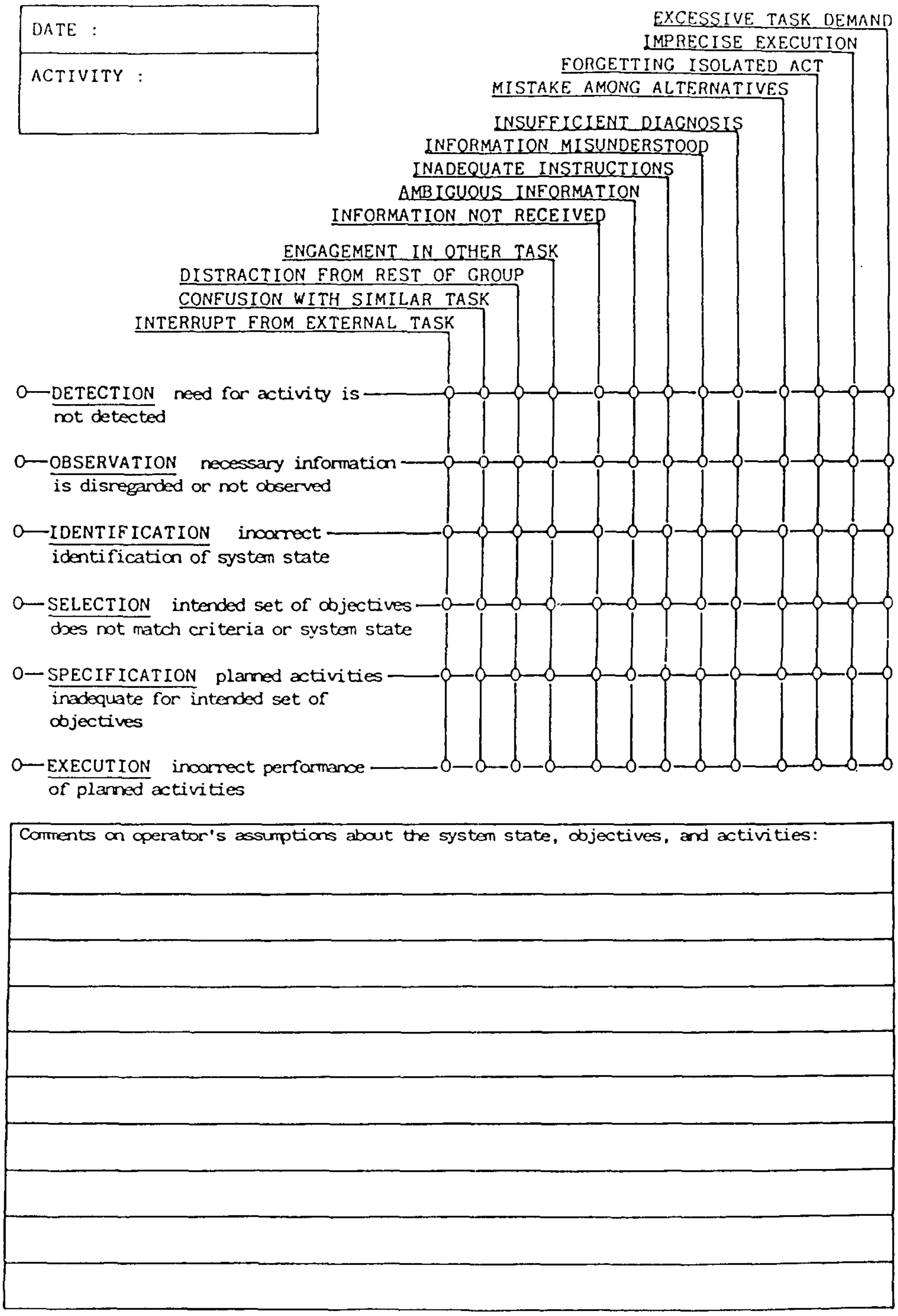


Figure 3.4.1 Checklist to evalulate operator performance (3-26)

3.4.2 Quantification of human errors

The most direct method for quantifying human error probabilities is to assemble a panel of experts to directly judge the probabilities [3 - 42]. A more systematic, and perhaps the most used, method is given by Swain [3-27, 3-28]. Swain gives basic human error rates for specific actions and guidance on adaption of the supplied rates to specific situations. Maintenance and repetitive task errors are quantified independently of the specific sequences, in much the same way as components.

Recently, the importance of available time has been recognized for non repetitive or sequence dependent operator actions. This time dependence is expressed as the cumulative frequency of not completing an action within a given time (Figure 3.4.2). This time-reliability curve is used with a time supplied from the systems analysis. The resulting probability is occasionally modified by situation factors or coupled with repetitive task errors. Here

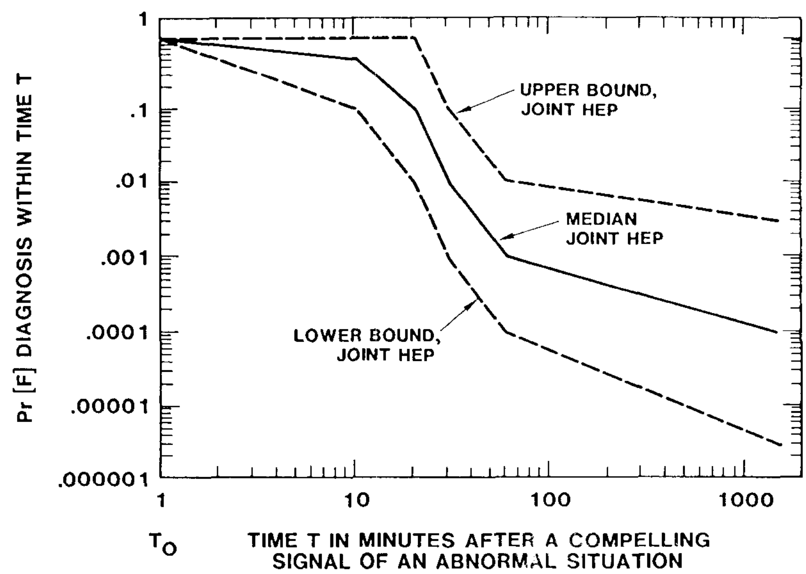


Figure 3.4.2. Operator Time-Reliability Curve(3-27).

again Swain provides both quantitative and qualitative guidance. An alternative method is presented in [3-29] where the reader is referred to Swain or another time-reliability curve [3-30] for quantification.

It should be noted that, if applied in detail, all the methods are complex and time consuming and the results still quite uncertain. Thus, particularly at first, the supplied basic rates from Swain's handbook are often used. This simple use may contribute to the fact that many qualitative human factor experts strongly disagree with the available techniques without, however, suggesting practical alternatives. In summary, current operator error probabilities are more appropriate for comparison purposes than as absolute error rates.

3.4.3 Simulation of failure

The necessary and extensive use of judgement in the evaluation of human errors requires that the analyst have some familiarity with the general methods used by operators in a control room. Since many situations which must normally be evaluated involve post accident conditions not observable by visits to an operating plant's control room, simulation of accident sequences can provide useful insight [3-31].

However, the use of a simulator to study specific sequences developed in a PRA analysis may often be subject to modelling constraints imposed because not all components are included in the simulator's model. For example, the failure of one check valve to close may have to be modelled by the failure to open of two parallel, motor operated, isolation valves. In this case, the valve position indicators assist the operators in verifying the nature of the problem.

3.5 Computer codes

The use of computer aided methods in reliability analysis in general is steadily increasing. A coarse grouping of the computer codes used in this area can be made according to the main capabilities of the codes. These capabilities are:

- identification of failures and construction of models (fault trees, reliability block diagrams)
- search for minimal cut or path sets
- calculation of various probabilistic quantities (reliability, unavailability etc)
- analysis of dependent failures
- analysis of sensitivity and uncertainty propagation
- plotting of analysis models (fault trees, block diagrams).

A good summary of the most common codes, based on a search of available literature, is given in [3-11]. Therefore it is sufficient here to concentrate on the codes which are used in the Scandinavian countries. These codes are summarized in Tables 3.5.1 - 3.5.4 with the same headings as in [3-11]. A performance comparison between some of these codes is reported in [3-32].

Concerning computer codes in the first group, the GO method has already been discussed in 3.2 and the RIKKE code has been treated in 3.1.4. RELVEC [3-33] is an interactive code primarily developed for the analysis of large control systems. The unique physical structure and the varying control tasks are easily modelled by the use of "connections".

3.5.1 Computer codes for MCS determination

This group of codes finds the minimal cut and/or path sets of a fault tree. A minimal cut set (MCS) is a smallest combination of failures that must occur simultaneously for the system to fail. The MCS may be considered as unique system failure modes. Their number, which is often very large, is in a strong and intrinsic way dependent on the number of basic events and gates of the fault tree. A minimal path set is a dual and complementary concept: a smallest set of components that simultaneously must operate successfully for the system to function.

All of the codes in this group, which are summarized in Table 3.5.1, use a deterministic method. WAMCUT uses a bottom-up Boolean substitation, while FAUNET and RISA search for the MCS's by a top-down substitution (Mocus-algorithm, [3-34, 3-35]). The latter method is also used by SETS but in a more free, user-specified way.

The MCS's themselves yield much useful information about the system being analysed. Furthermore, MCS's are used by some codes to calculate reliability characteristics for the top event, to perform sensitivity analysis and importance calculations, and to search for common cause candidates.

Table 3.5.1

Computer codes for minimum cut set determination

Code	Input	Limit on number of gates or events	Types of gates	Limit on number or size of cut sets	Method of generating cut sets	Other outputs	Fault-tree truncation	Other features	Type of computer, language, and availability
FAUNET	Fault-tree description in *numeric form*	1000 primary and complex *events, and* 1000 gates for the PDP-11 version	AND, OR NOT *K-of-N*	None	Top-down Boolean *substitution*	Pivotally decomposed *minimal* cut or path sets	Yes, based on cut-set *order*	Contains algorithms for modularization *and pivotal decompo-*siton. Contains algorithms for converting network into fault trees	PDP-11/VAX-11 FORTRAN IV *Available from* Risö National Laboratory
FTAP	8-character alpha numeric names	None	AND, OR NOT, NOR NAND K-of-N	Up to 16 components in minimal cut sets	Modular subtree Down, Modular Subtree Up Nelson Method	Probability of minimal cut sets, probability of minimal path sets	Yes, based on both cut set order and probability	Minimal cut sets of intermediate gates	IBM, CDC7600 Fortran Berkeley, University of California
RELVEC	10-char alphanumeric names, control system, control tasks, fault tree, block dia*gram, numerical* data	3000	AND, OR K/N, CONDITIONAL, PARENTHSIS	Number ~ 0.5 Mil size ≤ 9	*Path net*	*Reliability* availability, importances, sensitivity analysis, re*pair need*	Yes, based on cut set order	*Automatic path net* construction for control tasks. There can be several control tasks in one system. *Interactive, CCF*	*CYBER 173* VAX 11/750 Pascal Available from VTT
RISA	*10-character alpha* numeric names, control information, fault tree description, failure data	*2000 gates* and 2000 events	*AND, OR* K-of-N	*None*	Top-down Boolean substitution; Monte Carlo method	*Probability of* minimal cut sets and top event	Yes, based on probability (absolute and relative)	*Plot option*, restar option, elimination of rare and certain events, direct or weighted simulation	*CDC 7600* Fortran IV Available at Control Data AB
SETS	16 character alphanumeric names, user's program, failure data, fault-tree description	8000 events (gates and primary events together)	AND, OR INHIBIT PRIORITY Exclusive or special	None	Top-down Boolean substitution, but *user's program* can be designed for any other method	Prime implicants and common cause *candidates*	Yes, based on cut-set order	Processing in stages or independent subtrees can be used to *simplify cut-set gen-*eration	Cyber 170-835 Fortran IV Available at *Studsvik* Energiteknik AB
WAMCUT, CUTMOD	10 character alphanumeric names, control infor*mation, failure* data, fault-tree description	1500 primary events and 1500 gates *For CUTMOD* these limits apply to the modularized tree	AND, OR NOT, NOR NAND, ANOT ONOT K-of-N	Up to 1500 minimal cut sets of any order can be generated	Bottom-up Boolean substitution, *CUTMOD* modularizes the fault tree before cut set generation	Probabilities and moments of minimal cut sets and top event, unavailability polynominal	Yes, based on both cut-set order *and prob*ability	Can generate minimal cut sets of intermediate gates. CUTMOD calculates Fussel-Vesely importance measures for basic events	Cyber 170-835 Extended Fortran IV Available at Studsvik Energiteknik AB

3.5.2 Computer codes for quantitative analysis

Many of the codes in this group are used to compute point estimates of the system or subsystem probability (FAUNET, RELVEC, RISA, WAMBAM). Some codes are able to compute time-dependent unavailabilities. However, there are codes specifically aimed at a detailed time-dependent analysis of system unavailability (FRANTIC, MOCARE, TESVEC version of RELVEC).

Some codes also provide importance measures for primary events and modules of the tree (IMPORTANCE, RELVEC). Codes for uncertainty analysis are treated in the next section.

As regards the methods used, the codes can be grouped into deterministic or Monte Carlo codes; minimal cut set or direct-evaluation codes. Which group each code belongs to is displayed in Table 3.5.2.

3.5.3 Computer codes for uncertainty analysis

Because of the statistical uncertainty in the input failure and event frequency data it is very important to include uncertainty analysis in PRA. Various computer codes have been developed for this purpose, most of which apply Monte Carlo simulation to determine the distribution of a system probability. The uncertainty in the primary event probabilities is described by suitable probability distributions. Three codes in this group (CONFSI, RISA, SPASM) are summarized in Table 3.5.3.

Table 3.5.2

Computer codes for quantitative analysis

Code	Input	Quantitative calculations	Importance calculation	Other features	Type of computer and availability
FAUNET	Minimal cut or minimal path sets. Pivotally decomposed minimal cut or path sets. Primary-event failure data	Time-dependent as well as independent calculations of availability and reliability for systems with nonrepairable, repairable and periodically tested components	No		PDP-11/Vax-11 Abailable from Risö National Laboratory
FRANTIC,	Reduced system equation or minimal cut sets, primary-event failure data	Time-dependent calculation; nonrepairable, monitored, and periodically tested primary events are handled	No	Can model human-error and dependent-failure contributions	Cyber 170-835 Available at Studsvik Energiteknik AB
FTAP	*Fault tree description,* primary-event failure data	*Point unavailability* for top event and intermediate gates, no time-dependent analysis possible	*Output from* FTAP may be made compatible with the IMPORTANCE code	*Error checking,* probability truncation of fault tree	*IBM, CDC7600* Fortran Berkeley University of California
IMPORT-ANCE	Minimal cut sets, primary-event failure data	Top-event point-estimate probability or unavailability	Can calculate the following: Birnbaum, criticality, up-grading function, Fussel-Vesely, *Barlow-Proschan, steady-*state Barlow-Proschan, sequential contributory	Can rank cut sets and primary events on basis of each importance measure	Cyber 170-835 Available at Studsvik Energiteknik AB
MOCARE	Logical model: cut sets or tie sets generated by FAUNET; primary event data directly or via FAUNET-file	Reliability in the time interval o-t max. Unavailability, average and at t max. Average number of system failures/period and outage-time/system failure	The cut sets generated can be listed in order of importance	Extraordinary flexibility in modelling. All conditions for occurrence of component and subsystem failures can be specified *by means of subsystem-*models. Plot option	Burroughs B7800. Can easily be converted to an IBM 3033. Available from Risö National Laboratory
TESVEC	Physical control system, block diagram, fault tree, numerical data	Time-dependent calculation (nonrepairable, monitored and periodically tested components), reliability, availability	The cut sets are listed in order of importance; Fussel-Vessaly importance measures are calculated for components and listed in order of importance	Interactive; sensitivity analysis for 5 parameters, CCF	CYBER 173 VAX 11/750 Available from VTT

Table 3.5.2 con't

Computer codes for quantitative analysis

Code	Input	Quantitative calculations	Importance calculation	Other features	Type of computer and availability
RISA	Fault tree description, primary event failure data	Prob. of min cut sets and top event (incl neglected cut sets), time-dependent calculation of min cut sets, periodically inspected components, uncertainty analysis	Time dependent calculation of components marginal, fractional, competitive, sequention contributive and diagnostical importance	Extensive error checking, prob. truncation of fault trees, sensitivity analysis possible, Monte Carlo simulation	CDC7600 Fortran IV Available at Control Data AB
WAM-BAM BAMMOD	Fault-tree description, primary-event failure data	Point unavailability for top event and intermediate gates, no time-dependent analysis possible. Modularization of the fault tree is used in BAMMOD.	No	Extensive error checking possible through WAM, probability truncation of fault tree, sensitivity analysis possble by using WAM-TAP preprocessor instead of WAM	Cyber 170-835 Available at Studsvik Energiteknik AB

Table 3.5.3

Computer codes for uncertainty analysis

Code	Input	Method of uncertainty analysis	Type of statistical distribution	Other features	Type of computer and availability
CONSFI	Multiparameter function	Monte Carlo simulation	Log-normal Discrete empirical	Simulation threshold, Statistically dependent parameters optional	CYBER 170 (Simula) Available from VTT
RISA	Fault tree, failure rates, repair data, failure probabilities	Monte Carlo procedure	Gaussian, log normal, equal, uniexponential beta, gamma	Extension to other distribution types is possible without any substantial increase in the work involved	CDC7600 FORTRAN Available at Control Data AB
SPASM	Fault tree or reduced system equation, *component-failure data*	Monte Carlo simulation of average unavailability *for each* component	Normal, lognormal, uniform, beta, gamma, inverted *beta*, X^2-*and t*-distrib, empirical	Works in conjunction with WAMCUT	Cyber 170-835 Available at Studsvik *Energi*teknik AB

3.5.4 Computer codes for dependent failure analysis

It has become quite obvious that dependent failures can often dominate random hardware failures. Codes developed to deal with dependent failures are primarily aimed at solving the problem of identifying the system failure modes (common-cause candidates) that may be caused by a single common event or condition. Two codes of this kind (RIKKE, SETS) are summarized in Table 3.5.4.

The supply of computer codes for a quantitative evaluation of fault trees with dependent events is very limited. WAMBAM and RELVEC (Table 3.5.2) are, to a certain extent, able to handle probability evaluation of dependent events [3-36].

3.6 Uncertainty analysis

A probabilistic risk analysis produces estimates of undesirable events. However, various assumptions and limitations are made and engineering judgement is used in order to produce tractable models. In addition, the final estimates of the accident sequence frequencies rely largely on scarce data obtained from similar failures but from different environments. Thus, an uncertainty analysis should be an integral part of any risk assessment regardless of the scope of the study.

Table 3.5.4

Computer codes for dependent-failure analysis

Code	Input	Method of common-cause analysis	Other features	Type of computer and availability
RIKKE	Flowsheet or piping and instrumentation diagram	Adds generic causes, catastrophic causes, common supply and control dependencies to fault tree. Uses FAUNET to establish identity of repeated events	Allows fully automatic or interactive fault tree construction based on plant diagram alone. Can provide a large amount of detail	DEC PDP/11 and VAX. Available Risö National-laboratory
SETS	Fault tree	Adds generic causes and links to fault tree, cut sets that include one or more generic causes are obtained and identified as common-cause candidates	Can handle large fault trees and can identify partial dependency in cut sets, attractive features of SETS as cut-set generator justify use for dependent-failure analysis	Cyber 170-835 Available at Studsvik Energiteknik AB

3.6.1 Sources of uncertainty

There are many sources of uncertainty in a PRA, both in the construction of the models and in their subsequent quantification. The major identified sources of uncertainty inherent in current PRA practice are:

1. Model uncertainties

- Limitations in the modelling technique's ability to represent the real system.
- Incomplete or incorrect application of a modelling technique such as missing initiating and/or failure events.
- Limitations in the ability to model dependent failures, human errors, and other complex system interactions.

2. Assumptions

- Bounding conditions imposed to limit the depth or scope of the analysis such as the assignment of a binary failed or successful status for all components.
- Incomplete system information leading to possibly incorrect assumptions on the system operation.
- Simplified specification or imperfect knowledge of the success criteria.

3. Data uncertainties

- Unknown component failure distributions which must be specified to extract failure parameters from limited data.
- Simplified or improper treatment of time dependent failures.
- Limitations in, or the complete lack of, data for component failure.
- Questions of the relevance of the available data.

3.6.2 Treatment of uncertainties

Uncertainties can be included either indirectly by performing a sensitivity analysis or directly by numerical or analytic propagation of basic event uncertainties. Model and assumption uncertainties must usually be addressed by sensitivity analysis while data uncertainties can be propagated through the models or assessed by using statistical methods. Whatever methods are used, it is important to assess the magnitude of the uncertainty in order to evaluate the credibility that should be attached to the estimate.

While model and assumption uncertainties are very study dependent and thus difficult to address in general, techniques do exist to aid in the evaluation of data uncertainties' contributions to the system failure uncertainty. Note that the data uncertainties (whose calculation is discussed in Section 4) are almost certainly overshadowed by the model and assumption uncertainties when discussing absolute risk predictions.

The traditional procedure, initiated by WASH-1400 [3-7], uses a Bayesian type of approach for propagating uncertainties in the probabilities of basic events through a fault tree to obtain the uncertainty of the probability of the top event. The numerical inputs to the model (the failure and repair parameters) are treated as random variables with specified probability distributions. The distribution of the system failure probability - the top-event - is generated by using analytical methods or Monte Carlo simulation.

An alternative technique, which does not require the specification of the input probability distributions, can be used if sufficient failure data are available [3-37]. In this technique, the observed data are assumed to be random samples from an incompletely specified distribution, and confidence intervals of the parameters of the distribution are calculated. Unfortunately, there currently exists no exact method for obtaining confidence intervals for a top-event given confidence intervals for the input parameters. However, a few approximate methods are available [3-38, 3-39] as well as a nonparametric method [3-40].

A clear distinction should be made between the Bayesian techniques and those based on classical statistics such as those discussed above. In particular, the Bayesian technique includes the use of intermediate event probability distributions whose parameters are estimated using whatever data are available and engineering judgement when necessary. Because these methods allow limitations in the basic data to be bypassed, they are the most practical - and currently the only - methods for general use.

There is, however, disagreement as to whether this bypassing of data limitations produces valid results. The majority of the authors of this report, and presumably the majority of PRA practitioners, believe that the resulting distributions are accurate enough to characterize the uncertainty and can be used while classical statistical methods and the required data bases are developed.

3.7 Advanced techniques for special purposes

PRA studies are usually conducted with rather simple reliability tools. Typically, components are modelled by on-off failure models with a single constant reliability parameter such as failure rate or demand failure probability. Repairs and recovery options are either not taken into account, or modelled using an exponentially distributed recovery time. Finally, systems are assumed to be static reliability structures, i.e. the impact of component failures depends only on the presence or non-presence of the failed states, not on the order or time between failures.

The use of simple theory is necessary in order to be able to quantify the large models found in even a level 1 PRA-study. In fact, the simplifications do not essentially contradict the primary objectives of a PRA study: ranking of the accident sequences and significant contributors. But in more dedicated applications, the conventional PRA techniques are far too limited.

An important area of application requiring a more advanced theoretical basis is re-evaluation of the technical specifications or limiting conditions for operations. For example, stand-by equipment testing strategies and the maximum repair time allowed for components or subsystems before the reactor must be shut down need to be addressed with advanced techniques.

Extensive research and development has been conducted in this area in the Nordic countries, primarily by VTT and partially within the SÄK-1 project. This work has identified the following areas as those where improvements are needed.

- Classification of the failure modes of stand-by components into different types depending on the impact the failure state has on system function.
- Component unavailability (failure probability on demand) as a function of test procedure and time in stand-by state.
- Statistical dependence between the failure probabilities of redundant components with correlation on the time scale.

Correct expression of the system unavailability (failure probability on demand) as the conditional probability given the knowledge of the current status and past history of the system and its components.

Description of repair policy including prioritization of repairs, potentially imperfect detection of common faults, and true distributions for time to recovery.

Although only small practical applications have been conducted thus far [3-41], the experience motivates continued effort. Uncertainties, which are mainly caused by the lack of relevant data, can be addressed with sensitivity analyses, and the validity of the conclusions verified. Typically, most of the conclusions are rather insensitive with respect to uncertainties, as illustrated in Figure 3.7.1.

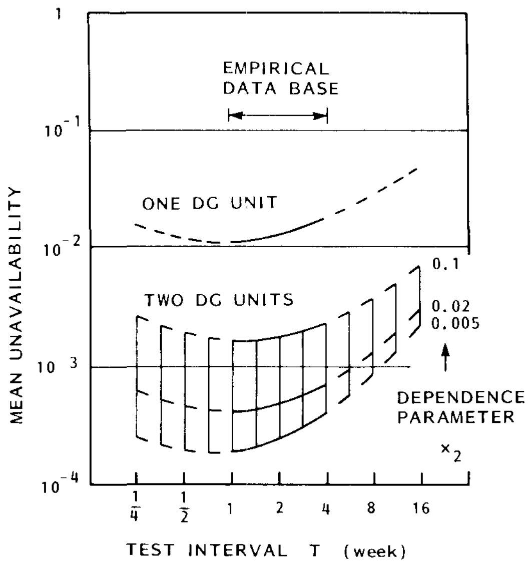


Figure 3.7.1 Calculated mean unavailability of one and two diesel generators with staggered testing [3-41]. The optimum with respect to the test interval is rather insensitive as the function of statistical dependence parameter x_2.

Further development of the methods for the optimization of technical specifications will be subject to a new Nordic project which will be carried out in the NKA program in 1985-88.

REFERENCES

3-1 TAYLOR, J R
A Background to Risk Analysis.
Vol 1-4, Risø National Laboratory 1979.

3-2 "The European Reliability Benchmark Exercise (RBE) Summary Report", Joint Research Centre, ISPRA Establishment, ISPRA Italy (to be published in 1985).

3-3 "Metoder för Risk- och säkerhetsanalys", Slutrapport från SCRATCH-programmet, Nordforsk, Juni 1982.

3-4 A Guide to Hazard and Operability Studies, Chemical Industry Safety and Health Council of the Chemical Industries Association, London, 1977.

3-5 JOHNSON, W G
"MORT. The Management Oversight and Risk Tree". SAN 821-1, 1971.

3-6 TAYLOR, J R
"Automatic Fault Tree Construction with RIKKE - A Compendium of Examples".
Vol 1-2, Risø-M-2311, 1981.

3-7 Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400, NUREG-75/014, October 1975.

3-8 GO-Methodology.
Vol 1-3, EPRI NP-3123-CCM, prepared by Energy Incorporated, 1983.

3-9 HIRSCHBERG, S
"Workshop on Dependent Failure Analysis, Västerås, 27-28 April 1983.
Summary Report: Conclusions and Recommendations for Future Work", ASEA-ATOM, 1983.

3-10 "Report from Task Force on Problems of Rare Events in the Reliability Analysis of Nuclear Power Plants".
CSNI Group of Experts on Common Mode Failure Analysis.
DECO/NEA, SINDOC (78) 41A, June 1978.

3-11 PRA Procedures Guide, Nuclear Regulatory Commission, NRC Report NUREG/CR-2300 January 1983.

3-12 FUSSELL, J B et al
"A Collection of Methods for Reliability and Safety Engineering", ANCR-1273, April 1976.

3-13 ERICSSON, G and HIRSCHBERG, S
"Treatment of Common Cause Failures in the Barsebäck 1 Safety Study".
5th International Meeting on Thermal Nuclear Reactor Safety, Karlsruhe, Germany, September 1984.

3-14 FLEMING, K N et al
"HTGR Accident Initiation and Progression Analysis Status Report". Vol II, General Atomic Report GA-13617, October 1975.

3-15 VESELY, W E
"Estimating Common Cause Failure Probabilities in Reliability and Risk Analysis: Marshall-Olkin Specializations".
International Conference on Nuclear Systems Reliability Engineering and Risk Assessment, Gatlinburg, Tennessee, June 20-24, 1977.

3-16 MANKAMO, T
"Common Load Model. A Tool for Common Cause Failure Analysis", Technical Research Centre of Finland, Electrical Engineering Laboratory, Report 31, December 1977.

3-17 PLATZ, O
"A Review of Selected Methods for Quantitative Analysis of Dependencies in Reliability Models".
Workshop on Dependent Failure Analysis, Västerås, 27-28 April 1983.

3-18 FLEMING, K N and KALINOWSKI, A M
"An Extension of the Beta Factor Method for Systems with High Levels of Redundancy",
PLG-0289, August 1983.

3-19 STAMATELATOS, M G
"Improved Method for Evaluating Common-Cause Failure Probabilities",
Trans Am Nucl Soc, Vol 43, pp 474-475 (1982).

3-20 MANKAMO, T et al
"Proceedings of the CCF-Workshop, Lepolampi, Espoo", 10-11 May 1984.
VTT Symposium Series.

3-21 HIRSCHBERG, S
"Comparison of Methods for Quantitative Analysis of Common Cause Failures - a Case Study", Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, 24 Feb - 1 May 1985.

3-22 HIRSCHBERG, S and PULKKINEN, U
"Common Cause Failure Data: Experience from Diesel Generator Studies", Nuclear Safety Vol 26, No 3, May - June 1985.

3-23 APOSTOLAKIS, G, CHU T L
"Time-dependent Accident Sequences Including Human Actions".
Nuclear Technology, Vol 64, Feb 1984.

3-24 LYDELL, B O Y et al
"Human Reliability Analysis in Contemporary Probabilistic Risk Assessment Studies".
PLG-0349, prepared for Swedish Nuclear Power Inspectorate, Draft report March 1984.

3-25 RASMUSSEN, J and ROUSE, WB (Eds)
"Human Detection and Diagnosis".
A NATO symposium, Roskilde, Denmark (1980), published by Plenum Press (1981).

3-26 HOLLNAGEL, E
"Report from the IEOP Pilot Study of Training Simulator Analysis Method".
NKA-LIT 3.2(82)114, Risø 1982.

3-27 SWAIN, A D and GUTTMANN, H E
"Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications".
NUREG/CR-1278, 1983.

3-28 BELL, B J and SWAIN, A D
"A Procedure for Conducting a Human-Reliability Analysis for Nuclear Power Plants".
NUREG/CR-2254, May 1983.

3-29 HANNAMAN, G W
"Systematic Human Action Reliability Procedure (SHARP)".
EPRI NP-3583, Interim Report, June 1984.

3-30 HALL, R E et al
"Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation".
NUREG/CR-3010, Nov 1982.

3-31 DINSMORE, S D
"NKA/SÄK-1 Simulator Exercise and Results".
STUDSVIK/NR-84/355, March 1984.

3-32 PULKKINEN, U
"A comparison between selected Computer Codes for Fault Tree Evaluation", NKA/SÄK-1-S(84)3, Technical Research Centre of Finland, to be published February 1985.

3-33 HOSSI, H J and NIEMELÄ, Z M
"RELVEC - A Tool for Control System Reliability Analysis".
Technical Research Centre of Finland (VTT), Electrical Engineering Laboratory, ESPOO, Finland.

3-34 BARLOW, R E and PROSCHAN, F
Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, Inc, New York.

3-35 FUSSELL, J B and VESELY, W E
"A New Methodology for Obtaining Cut Sets For Fault Trees".
Trans Am Nucl Soc 15, 1972.

3-36 PÖRN, K
"About Two Computer Codes for the Analysis of Dependent Failures".
STUDSVIK/SD-83/14, 1983.

3-37 EASTERLING, R G
"Methods for Statistical Uncertainty Analysis in PRAs".
SAND-82-2832C, CONF-830304-13, 1982.

3-38 SPENCER, F W and EASTERLING, R G
"Lower Confidence Bounds on System Reliability using Component Data".
SAND-84-1199C, CONF 8406135-1, 1984.

3-39 LLOYD, D K and LIPOW, M
Reliability in Management, Methods and Mathematics, Prentice Hall, New Jersey 1962.

3-40 EFRON, B A
"Bootstrap Methods: Another look at the Jackknife".
Annuals of Statistics, V 19. 1-16 (1979).

3-41 MANKAMO, T et al
"Experiences from the use of PRA methods in the re-evaluation of technical specifications".
International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, 24 - 28 February 1985, San Francisco.

3-42 EMBREY, D E et al
"SLIM-Maud: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement" NUREG/CR-3518, Vol 1, March 1984.

3-43 STENQUIST, C
"Identification of Common Cause Candidates in the Residual Heat Removal System in Ringhals I".
STUDSVIK/NR-82/95. SÄK-1-S(82)1.

3-44 HELLSTRÖM, P
"CCF-Analysis of Residual Heat Removal System at Ringhals I".
STUDSVIK/NR-84/465. SÄK-1-S(84)3.

3-45 ERICSSON, G, KNOCHENHAUER, M, MILLS, R
"Efficient Fault Tree Handling, The ASEA-ATOM Approach" Presented at the International ANS/ENS Probabilistic Safety Methods and Applications Topical Meeting, San Francisco, February 24-28, 1985.

4. RELIABILITY DATA

Reliability data are defined here to mean numerical information on reliability parameters (and eventually their distributions) that are specific to generic types of components. Examples are

- failure rate for operating components
- demand failure probability or stand-by failure rate of stand-by components
- repair and maintenance down-time.

Other input data are also needed in a quantitative PRA: frequency and contributing causes of plant transients, fires, external disturbances, probability of operator errors, parameters for dependent failure models, etc. Data in this wider meaning are not considered here. Recently compiled information on Nordic plant transients is available in [4-1].

4.1 Generic data sources

Generic data comprise average information for classes of components. These include the so called generic components like centrifugal pumps, motor operated valves, non-return valves, temperature measurements, etc.

Generic data are obtained through combining information from several plants and other sources. In this process averaging and weighting based on engineering judgement is used.

In the generic data detailed information is neglected, i.e. information that is specific to details of equipment design, materials, operating environment, maintenance policy, etc.

Owing to the non-specific nature, there is always an inherent, rather broad uncertainty band when generic data are used. Thus the use of generic data is basically limited to rough quantification such as, for example, the comparison of design alternatives at an early design stage.

If the quantification of an operating system is based on the use of generic data, it is particularly important to evaluate the impact of uncertainties and how they might effect the conclusions.

A selection of primary sources of generic data is listed in Table 4.1.1. In addition to these, there are many secondary sources such as current PRA reports which may often be quite useful.

The three last sources in Table 4.1.1 are data banks. These can also offer plant and component specific information. There is, however, often the problem that the user does not possess sufficient information to be able to evaluate the quality and validity of the information for application to a specific situation.

Table 4.1.1

Selection of generic data sources

Source	Year of last edition	Content	Origin	Comments
WASH-1400	1975	Mechanical and electrical components	Nuclear and process industry	Still quite useful source. Some data may be optimistic, specially because medians of log-normal distributions are used instead of mean values.
GRS	1980	Mechanical and electrical components	Nuclear	Improved with respect to WASH-1400. Uncertainty bands well treated.
IEEE-500	1984	Electrical, electronic and sensing components	Power plants	Data synthesized from experience and opinions of a number of experts.
NUREG/CR-1205 NUREG/CR-1362 NUREG/CR-1363 NUREG/CR-1331 NUREG/CR-1730 NUREG/CR-1740		Pumps Diesel gen Valves Control rods Containment penetrations Instrument	Nuclear Nuclear Nuclear Nuclear Nuclear Nuclear	These reports present the summaries of the Licensee Event Reports at U S nuclear power plants. LER reports are available and may be used as background information (laborious interpretation required).
T-bok	1984	Mechanical and electrical components	Nuclear (Swedish)	Represents component averages for each plant
MIL-HDBK-217D	1983	Electronic	Military	Represents models for accounting environmental and load factors.
NPRDS	1982	Mechanical and electrical components	Nuclear (U S)	Quality suffers from irregularities in participant reporting. Annual reports available.
ATV data bank	1983	Mechanical and electrical components	Nuclear (Swedish) (Finnish)	Additional work usually required to check the failure interpretation. Annual reports available.
SRS Syrel data bank	1983	Various	Various	Commerical all-purpose data bank. Information available to associate members in form of annual summaries and directly via computer terminal entry.

4.2 Collection and treatment of field data

Field data are defined here as the numerical, coded, and plain-language information about the populations, operating status, and failures of safety- and process-related components. This kind of information may be collected ad hoc for special analysis, but more important is the information that is systematically collected in data banks. An example of the latter type, the Swedish ATV system, will be considered here with respect to its purpose, contents, and collection methods.

4.2.1 Purpose and scope of ATV

The ATV data bank was initiated in 1974 by the nuclear power utilities in Sweden [4-2]. Later the Finnish TVO power company joined the collection system for operating safety data. The main purpose of the system is to provide the power industry with different kinds of operating safety data and failure statistics. After an initial phase of development, the system attained its production status in 1980, at which time the first calculated safety parameters were presented. The information in ATV is available to the utilities, vendors, authorities, research institutes, etc. The operation and management of the system is located at the Swedish State Power Board.

The system can be used to generate different kinds of summarizing tables: selected, sorted, or merged according to various parameters such as type, manufacturer, material, size, etc. However, much of the information is in coded format which makes its interpretation difficult. Component specific reliability characteristics, e.g. failure rates and mean repair times, can be calculated. Such an analysis, updated every year, might give valuable information about possible trends in component behaviour.

The system is extensively used in on-going safety or risk analyses. In order to facilitate this type of application, a reliability data handbook [4-3] with plant specific and generic failure rates or failure probabilities has been compiled from the ATV system supplemented with Swedish and Finnish licences' event reports.

The ATV system can not be used for a detailed analysis of failure causes [4-4] because the system is not planned for that purpose. The system contains information about all individual components; however, the follow-up of the component history is truncated if the component is stored after repair.

4.2.2 Contents of ATV

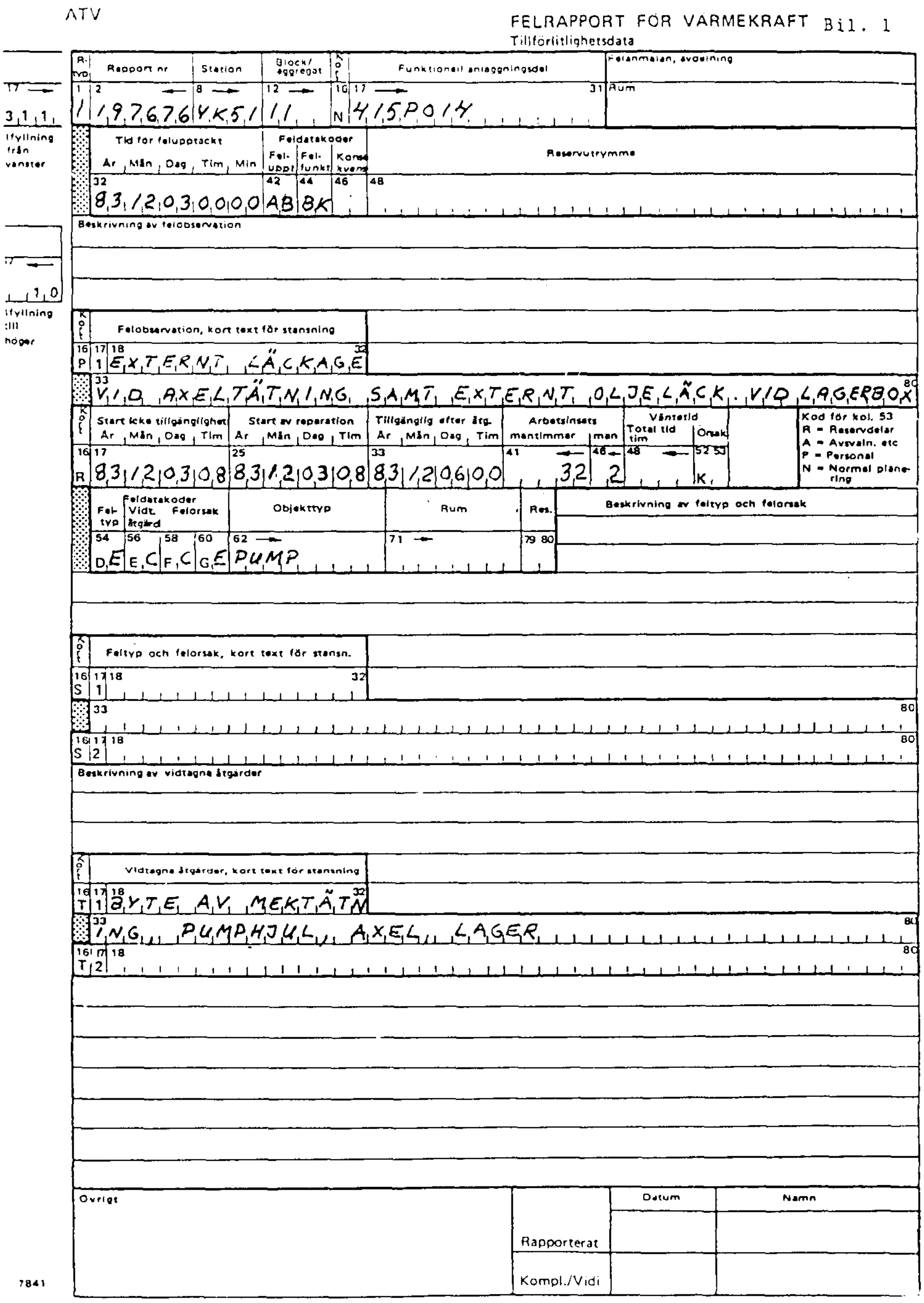
To be able to calculate component reliability characteristics the data bank must include information about the component itself, about any failures which have occurred, and about the operating profile of the component. Technical data concerning the components (type, size, manufacturer, etc) are stored only once. The operating profile is stored componentwise only for a limited number of components. Generally, the operating profiles of the components are derived from the operating profile of the whole plant, which is defined through a number of discrete operating states according to the Technical Specifications. The operating profile statistics are obtained from the parallel availability system TGV.

The maintenance staff at the utilities are responsible for the monthly reporting of failures which have occurred in safety- and process-related components. In addition, failures which are detected or repaired during the annual shutdowns are reported. The form used and the different items that are reported are shown in Figure 4.2.1. Due to the awareness of coding difficulties the coded information is supplemented with plain-language information.

The ATV-system contains on average 18 000 recorded components per power block. In January 1983, ATV included about 41 000 failure reports. This amount increases annually by about 1 000 failure reports per block. The quality of the ATV system has been investigated in special studies [4-6, 4-7]. The coverage of occurred component failures was not greater than about 50 % during the development phase (1974 - 1978). However, the trend seemed to be upward, so the coverage increased to 75 - 80 % during the period 1979 - 1980.

4.3 Estimation of uncertainty intervals

A major concern in a probabilistic risk assessment is the question of uncertainty in the various evaluations. As has been pointed out in Chapters 2 and 3, there are three main sources of uncertainties: model uncertainties, assumptions and the data uncertainties. This section is concerned primarily with the data uncertainties as reflected in the calculated parameters. An overall uncertainty analysis must also include the propagation of uncertainties from step to step throughout the risk assessment.



ATV

FELRAPPORT FÖR VARMEKRAFT Bil. 1

Tillförlitlighetsdata

R-typ | Rapport nr | Station | Block/aggregat | Kod | Funktionell anläggningsdel | Felanmälan, avdelning | Rum

1 | 1 9 7 6 7 6 | V K 5 1 | 1 1 | N | 4 1 5 P 0 1 4

Ifyllning från vänster

Tid för felupptäckt: År, Mån, Dag, Tim, Min — 8 3 1 2 0 3 0 0 0 0

Feldatakoder: Fel-uppt, Fel-funkt, Konsekvens — A B, B K

Reservutrymme

Beskrivning av felobservation

Ifyllning till höger

Felobservation, kort text för stansning

P 1 EXTERNT LÄCKAGE

VID AXELTÄTNING SAMT EXTERNT OLJELÄCK. VID LAGERBOX

Start icke tillgänglighet: År, Mån, Dag, Tim — 8 3 1 2 0 3 0 8

Start av reparation: År, Mån, Dag, Tim — 8 3 1 2 0 3 0 8

Tillgänglig efter åtg.: År, Mån, Dag, Tim — 8 3 1 2 0 6 0 0

Arbetsinsats: mantimmar 32, man 2

Väntetid: Total tid tim, Orsak — K

Kod för kol. 53: R = Reservdelar, A = Avvaktan. etc, P = Personal, N = Normal planering

R

Feldatakoder: Fel-typ, Vidt. åtgärd, Felorsak — D E, E C, F C, G E

Objekttyp: PUMP

Rum

Res.

Beskrivning av feltyp och felorsak

Feltyp och felorsak, kort text för stansn.

S 1

S 2

Beskrivning av vidtagna åtgärder

Vidtagna åtgärder, kort text för stansning

T 1 BYTE AV MEKTÄTN

ING, PUMPHJUL, AXEL, LAGER

T 2

Övrigt

Datum | Namn

Rapporterat

Kompl./Vidi

7841

<u>Figure 4.2.1</u> Form for Reporting Component Failures to the ATV System [4-5].

In order to be able to determine the uncertainty of the output values of the analysis, each estimate of a parameter value must be accompanied by an uncertainty measure. The term "uncertainty" is commonly used in the context of PRA to describe two different concepts [4-8]:

1 Random variability (or incomplete knowledge) of failure rate or demand failure probability.

2 Imprecision in the knowledge about the distribution models (and their parameters) that are used to describe this random variability.

Reference [4-8] also gives an illustrative example of predicting the failure rate of a specific valve, based on a model that has been developed from a valve-failure data base containing data from several plants. Then the prediction may be uncertain for two reasons:

1 The distribution is intended to describe a randomness that is due to plant-to-plant or component-to-component variations (population variability).

2 There are inadequacies in the variability model (modelling uncertainty) and its parameters have been estimated from a limited data base (sampling uncertainty).

There is an essential difference between these two concepts, that will be explained below, which affects the analyst's choice of model.

4.3.1 Population variability and sampling uncertainty

The example in [4-8] also illustrates a rather common PRA situation: probabilistic parameters are required for a specific component, but the component specific data are so scarce that the analyst must rely on a wider data base including data for similar components in several plants. Both of the uncertainty concepts above, population variability and sampling uncertainty, can be quantified by using the theory of distributions and the theory of statistics.

A basic difference between the two uncertainty concepts is that an expansion of the data base may improve the sampling precision (decrease sampling uncertainty) but cannot decrease the fundamental population variability. In other words, the determination of the population variability can be made more precise by the use of an expanded data base. However, consideration should always be given as to whether the data base is representative enough for the current problem.

Current practice generally does not distinguish between the two concepts in the uncertainty analysis. Thus, it is not possible to separate their contributions to the final uncertainty bounds. It is important, however, that both concepts are taken into account in the determination of the total uncertainty measures.

There are two main approaches to the treatment of uncertainty in PRAs: the frequentist, or classical, approach and the Bayesian approach. The Scandinavian countries have tried, as far as possible, an empirical Bayes approach [4-3].

4.3.2 Homogeneous or non-homogeneous failure model

The population variability (i.e. the variation of reliability characteristics of similar components) may be due to differing materials in fabrication, differing environmental conditions, and differing testing and maintenance procedures. In addition, if there are components with time or age dependent failure rates or failure probabilities, this may also appear as a variation between components in the data, which only count the number of failures during a certain operating time or number of demands.

Thus there are many reasons for assuming that the population of similar components is non-homogeneous. This means that the reliability parameter is assumed to vary from component to component within the population although it remains constant in time for any given component. In this compound model the distribution of failure rate or failure probability in a given class of components rather than a single value of the appropriate parameter is estimated. A second type of estimation is done for the homogeneous model, where all components of a given class are assumed to have the same reliability parameter.

Various statistical tests [4-9] are available that can aid the analyst in choosing between the two models. The non-homogeneous approach has the advantage that it explicitly defines the population variability while the homogeneous model ignores the existence of such a variation. In both cases the analyst has to choose a sampling model

$$f\ (x \mid \theta) \qquad \text{(Eq 4.1)}$$

where θ denotes the reliability characteristic being studied and x is the observable, random number of failures.

In the non-homogeneous model, θ is assumed to vary according to a distribution $g(\theta)$. In this case the observable number of failures follows the compound distribution

$$h(x) = \int f\ (x|\theta)\ g(\theta)\ d\theta \qquad \text{(Eq 4.2)}$$

The difference between these two models is illustrated by Figure 4.3.1 from [4-9], which shows the resulting uncertainty bounds for the failure probability of closing valves. The non-homogeneous probability interval, corresponding to the plotted density function, is much larger than the homogeneous confidence interval. For increasing sample size, the confidence interval decreases, while the probability interval changes only slightly.

So far both of these models are based on classical statistics and probability concepts. The non-homogeneous model becomes a Bayesian approach when it is applied in a component or plant specific analysis. Here $g\ (\theta)$ is used as a prior distribution. The combination of this distribution with component specific data results in a posterior distribution, which provides the new information about the particular object and can be summarized in terms of point estimates and probability intervals.

For the reliability data handbook [4-3], the non-homogeneous model has been used for all of the roughly 55 groups of components and 80 failure modes. In order to simplify both the analytical treatment in and the use of the handbook, the so called conjugate distributions were chosen to describe the

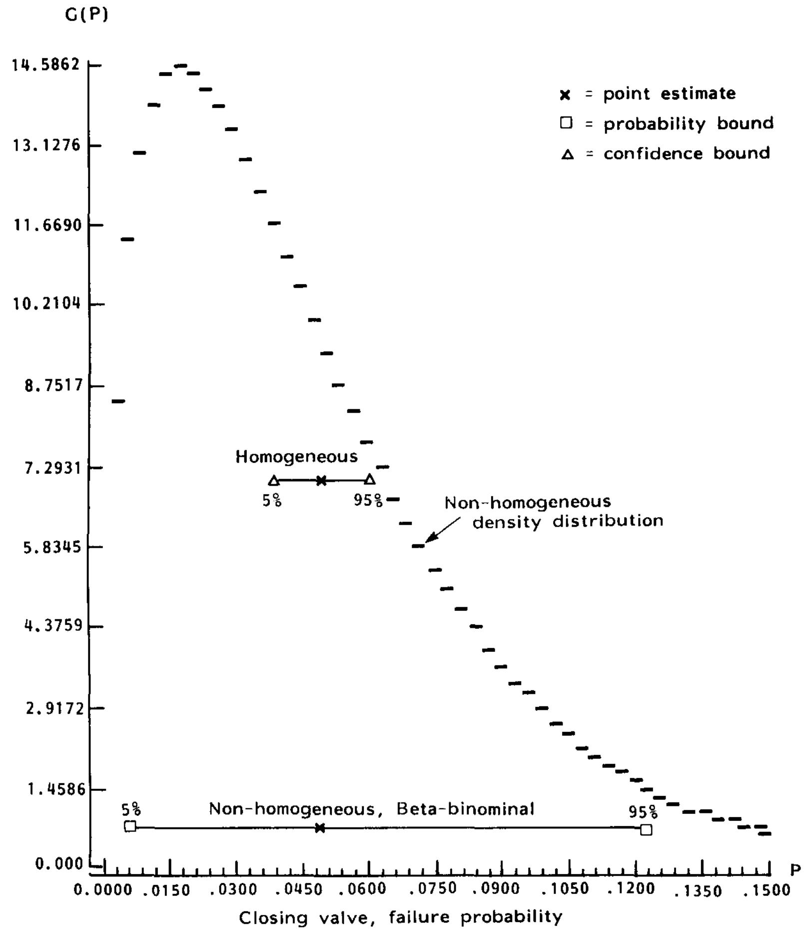


Figure 4.3.1 Point estimates of the failure probability for closing valves (Case 3, ref [4-9]) with associated probability or confidence bounds. The probability density function corresponds to the interval at the bottom.

population variability. Prior distributions are said to be conjugate when the posterior distributions have the same form. Thus, the gamma and beta distributions were chosen to describe the failure rate and failure probability respectively. The impact of the choice of conjugate priors on the resulting posterior estimates as compared to alternative distribution families is currently being studied [4-10].

REFERENCES

4-1 LAAKSO, K
"A systematic feedback of plant disturbance experience in Swedish nuclear power plants".
ASEA-ATOM Report KPA 84-351,
November 1984 (SÄK-1-S(84)4).

4-2 Vad är ATV?
Booklet issued by the ATV staff, Vattenfall Kärnkraft, 1983.

4-3 BENTO, J-P et al
T-boken. Tillförlitlighetsdata för komponenter i svenska kokvattenreaktorer.
RKS 82-07.

4-4 ROSEN, Y
"Samordning av drift- och störningsrapportering från svenska kärnkraftsverk, etapp 1".
Asea-Atom PM KSD 80-122, 1980.
(Section 5.2.5).

4-5 Användardokumentation för ATV-systemet.
Sammanställd av ATV-kansliet, Statens Vattenfallsverk, Aug 1980.

4-6 BENTO, J-P and VENDLER, E
"Quantitative and qualitative analysis of the ATV Data Base".
STUDSVIK/K2-81/479, 1981.

4-7 STENQUIST, C and KJELLBERT, N A
"Quantitative analysis of the ATV Data Base, Stage 2".
STUDSVIK Technical Report NR-81/69, 1981.

4-8 PRA Procedures Guide. A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.
NUREG/CR-2300, Jan 1983.

4-9 PÖRN, K
"NKA/SÄK-1. Reliability Data Workshop - Summary Report".
STUDSVIK/SD-83/13, /NR-83/250,
SÄK-1-S(83)3.

4-10 PÖRN, K and ÅKERLUND, O
"Estimation and Robustness of Prior Distributions for the analysis of Reliability Data".
STUDSVIK/NR-85/19
SÄK-1-S(85)1 (to be published).

5. PRA IN REGULATORY WORK

The rules and regulations governing the licensing and operation of nuclear power plants are continuously being modified. These modifications arise partly from operating experience and partly from advances in analysis techniques. There is currently a tentative but basic shift from very conservative deterministic based regulations towards more realistic regulations with an explicit probabilistic basis. This chapter briefly describes this shift and tries to clarify those areas where probabilistic methods can be and are used. Note that a definition of the three levels of PRA can be found in Section 1.1.

5.1 Historical background

The development of commercial nuclear power in the USA was based on experience obtained from the military program. Responsible bodies soon acknowledged the fact that nuclear power required special attention because of the potential for severe accidents. This, plus the fact that there are several vendors and many utilities, has resulted in a very formalized licensing procedure in the U.S.

The overall rules governing licensing in the U.S were laid down in the "General Design Criteria". These contain requirements and rules for the design of nuclear reactors such as the number of independent shutdown systems, number of emergency core cooling systems, etc. The criteria were further supplemented by Regulatory Guidelines issued by USNRC and by codes and standards issued by ANS, ASME, IEEE, etc. Finally, the USNRC issued Standard Review Plans, which specify in detail how the NRC reviews the licensees' applications.

Consequently licensing work in the USA is quite formal with all rules and requirements written down and little room for ad hoc decision and improvisation. An illustrative example is the rules governing the analysis of loss of coolant accident which specify the models to be used, the heat transfer coefficient, etc.

In the European countries the situation is different. Typically every country has one or two vendors and public utilities in which the government often takes part. In these countries, the general practice from the USA has been followed. In particular, the General Design Criteria and some codes and standards have been adapted and supplemented by national rules. However, the small number of parties involved in the regulatory and licensing work has resulted in an informal and much smoother process.

Accordingly, although formal contact certainly exists in Europe, much regulatory work is performed through close and informal contact between authorities, vendors, and utilities. The informal process, which places emphasis on problem solving and not simply fulfilling requirements, generally results in enchanced safety.

Although the process in the USA as well as in Europe has been deterministic in nature, the philosophical basis for many of the rules is probabilistic. For example, many regulations are based on the most probable accidents and not on a hypothetical maximum accident. In addition, recognition of the possibility of failures and the potential for common cause failures can be found in rules regarding "defence in depth", redundant and independent engineered safeguards, and diversity; to name a few.

5.2 Developments in recent years

In 1974 the USNRC issued the Reactor Safety Study, often referred to by the report's number, WASH 1400. This was the first level 3 probabilistic risk study performed for nuclear power plants. All the basic tools and methods of a probabilistic risk assessment were utilized. The final results were expressed as the expected number of early deaths, latent cancers, etc. Results of this form were required in order to enable the direct comparison of the risks from nuclear power plant operation with other societal risks, one of the major goals of the study.

In 1980 the Federal Republic of Germany conducted a "German Risk Study" which utilizes the methods, tools, and models from WASH 1400 transferred to German reactors using, as much as possible, German data.

These two studies were widely discussed and also criticized. Specifically, models for human behaviour, common mode/cause failures, system interactions, and component failure rates were criticized. These points raised the important question of the completeness and the accuracy of the results regarding both the probabilities and consequences.

The accident at Three Mile Island (TMI) in 1979 demonstrated that the licensing process in the USA, which allocated large resources based on conservative calculations, could be improved. Accordingly, many actions and revisions were made concerning research and development within the areas mentioned above and, more important, the licensing process in USA and Europe is being revised to incorporate probabilistic methods.

Both supporters and critics of PRA techniques used the TMI accident to present strong arguments supporting their positions. In any case, all parties agreed that the methodology of the WASH-1400 study provided a framework for detailed analysis and discussion of potential accidents. As a result a series of plant specific PRA studies were started. These have aided in the identification and removal of many design and procedural weaknesses.

Currently, the use of probabilistic techniques is being considered to assist in the cautious reduction of the conservative assumptions and models traditionally used in deterministic techniques. In particular, regulations and standards which are essentially deterministic in nature may be supplemented with a probalistic bound. A good example of this bounding approach concerns the loss of coolant calculations discussed earlier. Recently, the NRC has proposed that the calculation of maximum cladding temperatures could employ best estimate models and parameters to calculate a best estimate temperature and a more conservative 95 % upper bound [5-1]. The 95 % bound would, in this case, be the temperature of interest. Systematic techniques which allow the propagation of input uncertainties through complex models exist [5-2] and can be adapted for use in PRA.

5.3. Current status of PRA

PRA has gained increased attention and influence in the licensing process. Several surveys have been conducted [5-3, 5-4, 5-5] and the OECD has started an international working group (Principal working group no 5 - Risk assessment). This group is currently conducting a survey on how, and for what purpose, PRA methods have been used in regulatory work in the member countries.

In the USA several guides on the practical performance of PRA's have been issued. The first guide, the "ANS PRA Procedures Guide" [5-6], was made by a task force founded by ANS in 1982. It is a guide for engineers and scientists on how to conduct a probabilistic risk assessment for nuclear power plants. It describes and recommends available techniques and personal requirements for performing a PRA of all three levels and provides some discussion on how to include the so called external events such as earthquakes, flooding, and fire.

In addition to the ANS guide, the USNRC has issued two PRA guides [5-7, 5-8]. These guides, which essentially stop at level 1 and do not discuss external events, are more specific to ensure that the results of the studies are comparable. It should be noted, however, that these are all state of the art manuals which contain methods and techniques acceptable at the time when the manuals were written.

In general, Level 1 PRA's are used extensively in several countries to verify that sufficient independence and redundancy exist for a variety of initiating events and to evaluate proposed modifications. PRA techniques are also used during design although these studies are usually of limited scope and, of course, must use generic data. Some differences are, however, apparent between the different countries.

In the USA, extensive studies including full scale PRA's have been conducted. The studies have been used during licensing hearings and can be used for setting up site selection criteria and emergency planning. Economic factors have motivated many U.S. utilities to perform PRA's of all levels to address backfitting issues and to balance technical specifications.

Furthermore, research has been initiated concerning the items identified as a result of the criticism of the studies conducted (i.e. WASH 1400 and the German Risk Study) and lessons learned from the TMI accident.

The USNRC is studying the usefulness of quantitative probabilistic bounds (safety goals) for the design and siting of nuclear power plants [5-9, 5-10]. Since some of these goals are based on risk, full scale PRA's for granting of operating licenses for future nuclear power plants would presumably be required.

In France the licensing process has for some time been based on a cut off value of 10^{-6} per year for an accident with health effects for the environment, including human beings. In other words, if an accident is estimated to have a probability lower than the cut off value, it is disregarded. Accidents with a higher probability call for design modifications and/or special emergency procedures. As a consequence, PRA's have been used extensively at all stages in the licensing process.

In Germany PRA is regarded as a research item, i.e. as a means for evaluating important projects while no major role is foreseen for full scale PRA in the licensing process. Yet level 1 PRA's are used extensively by the authorities, vendors and utilities when selecting design alternatives and/or modifications.

In the UK PRA's on all levels, but mainly level 1, have been used in licensing of the gas cooled reactors. During the writing of this report, hearings were underway concerning a technological shift to the pressurized water reactor. As a basis for this decision, a level 3 PRA for a PWR sited at Sizewell was performed and is expected to be a major contributor to the decision process. The analysis was also used for design modification of the planned concept in order to enhance safety.

In Sweden the use of PRA in regulatory work is increasing. It should be remembered, however, that the Swedish nuclear power program is practically complete, which results in a situation where only operating or nearly completed nuclear power plants are dealt with. Yet SKI has requested a level 1 PRA for both the newest plants, scheduled to start up in 1985. Furthermore, PRA at level 1 is used in the assessment of operating experience and helps define what type of failure data are needed. Finally, PRA methods constitute a major part of the As Operated Safety Analysis Report (ASAR) which is requested for power plants which have been operated for 10 years.

In Finland the licensing process is based mainly on the deterministic approach, but reliability analysis has a role as a supporting tool. It appears, however, that probabilistic risk analysis will play an increasing role for any new plants, both in the licensing and regulatory processes. Furthermore, a level 2 PRA has been required for one operating PWR and one operating BWR. These studies are currently in a pre-study phase. They will be conducted by the utilities and reviewed by STUK. STUK sees these studies as a pilot study with strong educational purposes.

5.4 Areas of application

General experience seems to indicate that PRA will have an increasing role in regulatory work. Whether full scale PRA's will become mandatory is, however, uncertain. There are several reasons for this, among which the question of completeness and the accuracy of the absolute quantification are the most important. But when PRA is regarded as a tool and an aid in a continuous process involving authority, utility and vendor, its importance will increase.

5.4.1 Documentation, education and research priorities

PRA is the most comprehensive and systematic way of describing and documenting system behaviour and possible interactions. Furthermore, the very process of conducting an analysis is a very important aid in educating the utility and the authority in thinking in terms of probabilities and functional performance, rendering a more balanced discussion between authorities and utility possible. Finally, PRA can aid in setting priorities for research and development.

5.4.2 Human Interactions

PRA studies have helped highlight the importance of human actions, both during normal operation (such as maintenance and repair) and during plant transients. At present, the quantification of human error probabilities is difficult and very uncertain. However, the accident sequences in which the actions are embedded provide a systematic framework for both ranking the importance of the actions and providing information about the environment present when the action is required. When coupled to the complexity of these actions and the time constraints, this can be used for deciding if automation would be beneficial or if procedures need to be written, modified, or stressed during training.

For example, when a Swedish PRA study was reviewed, the lack of a "Feed and Bleed" procedure at the plant was noted. Steps have been taken to provide this procedure and the required training.

5.4.3 Common cause failures

Common cause failures constitute a very important problem when the redundancy and operability of the safety systems must be assured. PRA techniques can identify, in a systematic and qualitative way, areas within a system and/or across systems which are vulnerable to this type of failure.

A typical example of a common cause event which can also initiate an accident sequence (i.e. a common cause initiator) is given below. Note that the sequence of events ignores all possible operator recovery actions.

In the reactor protection system for a BWR, the signal for high reactor tank water level has a 2/3 logic structure. During an analysis, it was discovered that two of the channels were connected to the same electric bus. Thus the loss of the bus would cause inadvertent actuation of the two channels (fail safe principle), activation of the high level signal and, as a consequence, reactor scram and prevention of start of all coolant injection systems. The common cause initiator was subsequently removed by using three separate buses to power the three separate channels.

5.4.4 Operating experience

Operating experience can be assessed in a systematic way using the methods and tools of PRA. Trends and "near misses" can be identified and component failure rates evaluated and subsequently monitored on a plant specific and generic basis.

The Swedish program on the ASAR's is an example of utilization of PRA methods in assessing operating experience. A probabilistic analysis was not performed as part of the licensing of the older reactors in Sweden, but the ASAR's include level 1 PRA analysis for some of the important systems. Therefore, the checking of experience against expectation can subsequently be performed within a probabilistic framework.

5.4.5 Design modifications and backfits

PRA methods are being used extensively in decision making concerning design alternatives or modifications. This is a general trend in all countries and constitutes a balanced and systematic way of quantifying alternative system configurations.

For example [5-11], a moderately costly proposal was recently made to transfer the power supply for some large pumps from the diesel supported buses to the gas turbine supported buses. The primary motivation for this change was to prevent the - safety related - pumps from tripping in the event of loss of offsite power. However, when the change was evaluated in the plant's PRA, it increased the probability of an initially negligible sequence about 100 times so that it became the second largest contributor. After checking the reasons for this increase, the proposal was dropped.

Furthermore, PRA can help in applying codes and standards in a balanced way since it provides a means of checking that the level of safety is uniform. In particular, conservative overdimensioning can be avoided so that a more balanced allocation of resources can be used to improve safety in a efficient and economical way.

5.4.6 Technical specifications

The reliability and the safety of the plant is influenced directly by the specifications concerning testing and allowable down-time due to repair in safety systems during operation. Currently, most of these specifications are based primarily on engineering judgement. Application of the probabilistic analysis techniques in this field indicates that the current specifications are not well balanced.

For example, a reliability analysis was used to support the allowance of preventive maintenance during operation in a Finnish plant. Because of the high level of redundancy and separation, it was a relatively straightforward task to verify that moderately sized maintenance periods in one redundant train at a time will only marginally increase system unavailability even when common cause failures are taken into account. The marginal unavailability increase is expected to be more than compensated for by better maintenance quality because, during the operational period, the work can be done without the time pressure which can be a problem during busy refueling outages.

The optimum test interval of standby systems and components have recently been studied. The results have contributed to the relaxing of frequent test requirements for some systems as the system unavailability is only marginally affected by the change but test caused degradation is effectively reduced.

In addition, the application of PRA techniques has indicated that the process of shutting down a reactor is not completely risk-free because transients may be initiated due to the change of the plant state. This makes continued operation perferable in some situations where sub-system or component failures can be repaired within a reasonable time. This contrasts with the traditional approach which strongly favours shut-down and on which many current technical specifications are based.

In general, the most important advantage in the use of PRA and PRA techniques is that they provide a systematic basis on which utilities and regulatory bodies can objectively discuss the re-evaluation of technical specifications. It appears that periodic test intervals and allowable downtime for repair can be allocated in a better way, improving both safety and the balance between safety and economy.

5.5 Conclusions

In summary, it can be stated that PRA's are used extensively in regulatory work although they are, of course, one of many tools. It should be noted, however, that the techniques and models required to perform the analysis become more uncertain with each level. Level 2 uncertainties include, of course, uncertainties from level 1 as well as uncertainties associated with the modelling of such phenomena as core melt progression, fission product retention in the primary coolant, and hydrogen explosions. Level 3, in turn, requires estimates for evacuation times, weather models, and dose-effect relationships. Hence, it is not surprising that level 1 PRA's are most often used in regulatory work although valuable information can be obtained from current level 3 PRA's to assist in emergency planning and site selection criteria.

The performance of a PRA of any level is a complicated task. In order to be successful it calls for well organized work and close collaboration with persons experienced in plant operation and others intimately familiar with system details. As was noted during the SÄK-1 project, even the performance of a single system analysis requires adequate support from the plant staff to be successful.

A level 2 or 3 analysis requires resources which may often be prohibitive. Yet it should be emphasized that useful work can be performed with limited resources when concentrating on specific topics such as the contribution of repair down-time to the reliability of a specific system function.

The most important attribute of a PRA of any level is that it provides a framework within which the functional requirements and interactions of a plant are documented in an orderly manner. Although some areas of analysis rely perhaps too heavily upon assumptions and simplifications, these areas are recognized by the PRA community and are the subject of various research projects. It should be noted that the building block nature of a PRA makes it relatively easy to replace coarse models in the study with better models when they become available.

The scope of SÄK-1 was limited to level 1 analysis, corresponding to the current analysis trends in the Nordic countries. At this level, certain general comments and conclusions can be made.

Even with currently available techniques, the performance of a PRA can identify specific points in a plant which differ significantly from other plants or from basic design principles. The generated probabilities of, for example, core melt should be considered more of a tool than the result of a study. The results of a study are the following: the ranking of accident sequences, a measure of the relative importance of various events and the as built systems, and the model itself. Using this model, questions of various types can be addressed with model structure modifications or sensitivity studies. The quantitative impact of any changes can be used to provide guidance on the selection between alternatives or the importance of an issue.

Perhaps the greatest problem with current PRA's is that they are usually quite voluminous and hence difficult to review. Although part of this is the unavoidable result of the scope of the studies, part is attributable to the limitations in some of the models which require extensive documentation to describe and justify. This second source should decrease as better models become standardized and less justification is required. In addition the continued development of data base systems and analysis codes will make the models easier to construct, access, and use.

REFERENCES (Partially unquoted)

5-1 "Emergency Core Cooling System Analysis Methods", NRC Information Report, SEC4-83-472, November 1983.

5-2 COX, N D
"A Report on a Sensitivity Study of the Response Surface Method of Uncertainty Analysis of a PWR Model", EG & G RE-S-77-7, January 1977.

5-3 "A Review of Some Early Large-Scale Probabilistic Risk Assessments". Chapter 4, EPRI NP-3265, October 1983.

5-4 "Survey of Probabilistic Methods in Safety and Risk Assessment for Nuclear Power Plant Licensing" IAEA-TECDOC-308.

5-5 Von HERRMANN and WOOD
"Engineering Aspects of Probabilistic Risk Assessment", Progress in Nuclear Energy, Vol 14, No 1, pp 1-19, 1984.

5-6 PRA Procedures Guide, Nuclear Regulatory Commission, NRC Report NUREG/CR-2300, January 1983.

5-7 Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, January 1983.

5-8 Probabilistic Safety Analysis Procedures Guide, NUREG/CR-2815, January 1984.

5-9 "Safety Goals for Nuclear Power Plant Operation", NUREG-0880, (Draft) May 1983.

5-10 ERNST, M L
"Use of PRA and Safety Goals in Nuclear Power Plant Regulation", Nuclear Engineering and Design 75, 1982.

5-11 THURING, L
"Bvt - Gasturbinsäkrade 327-pumpar", ÅK 8409-69 Sydkraft, September 1984.

5-12 JOKSIMOVICH, V et al
"Some Insights Gained from Conducting an EPRI-Sponsored Review of Five PRA Studies", Presented at the 11th WRSR Information Meeting in Gaithensburg, Maryland, October 24-28, 1983.

5-13 LEVINE, S et al
"Probabilistic Risk Assessment in the U.S.", Reliability Engineering 6, 1983.

5-14 VIROLAINEN, R and THADANI, A
"On Licensing and Regulatory Practice in NRC", Available from the Finnish Centre for Radiation and Nuclear Safety, April 1984.

6. CONCLUDING PROJECT SUMMARY

This final chapter summarizes the main results of the SÄK-1 project. The degree to which the original objectives were reached and topics for continued work are also discussed.

6.1 Methodological progress

An advanced methodology and a preliminary data base for time-dependent availability analysis of stand-by safety systems have been developed. The methodology reaches beyond the conventional PRA methodology, and can be used, for example, in the context of the optimization of test and repair arrangements for safety systems. The modelling approaches and available computer codes were compared and tested in the Benchmark 1 study of the SÄK-1 project. The development in this area was partly conducted within the SÄK-1 project and partly on a national basis in parallel with other development projects.

Qualitative identification methods were developed primarily for common cause failure analysis (CCFA). Different approaches and computer codes have been compared and developed and tested in the Swedish PRA studies. In 1983 a workshop sponsored by SKI was held on CCFA. It was very successful and will be reported in an international journal. The work on this subject was conducted partly within the SÄK-1 project and partly by ASEA-ATOM and the Swedish utilities in connection with other practical work.

Substantial effort has been directed towards improving the quantification models of CCFA. Significant improvements were made which consistently take into account the high level of redundancy and diversity that are typical of the safety systems in the newer Nordic nuclear power plants. Due to the sparse data base of CCF's in four-train systems, special emphasis was placed on systematic sensitivity analyses which can be used to verify how much PRA results and conclusions are influenced by incompletely known CCF contributions. It should be noted that, during this work, inconsistencies and actual errors have been discovered in the CCF quantification models used in some PRA studies in the USA.

6.2 Data base improvements

Statistical techniques and computer programs have been developed for the handling of failure records and the estimation of reliability parameters. The main emphasis in this area was on the treatment of uncertainties. As a result, the uncertainties at the component data level can currently be satisfactorily managed. The principles and methods developed are adapted for use in the Nordic PRA studies and in the compilation of the Swedish Data Handbook (T-bok), and they will be implemented in the Swedish Data Bank (ATV system).

Work with practical data has included a pipe failure study (Risø) and a valve closing study (VTT). In the pipe failure study, the faults in the piping of the Nordic nuclear power plants were compiled and analyzed. The study resulted in recommendations for improvements in the explanatory part of failure cause reporting. The valve closing study verified the principles behind the time-dependent modelling and parameter estimation for stand-by components.

6.3 Model and code comparisons

The two Benchmark studies proved very useful in the comparison and evaluation of different modelling approaches. As a result, better insight has been obtained concerning the advantages and limitations of the cause-consequence diagram compared with the traditional event tree method, and the block diagram compared with the traditional fault tree approach. Our general recommendation is that the modelling should be done hierarchically starting from a simple model and adding detailed submodels as needed ("top down" principle). Often it is most efficient to use different modelling methods on different levels of the hierarchy.

The Benchmark exercises also proved productive with respect to the comparison of available fault tree codes and other related computer programs. The comparisons themselves stimulated further development of the codes. The best example is the implementation of the automatic modularization of series basic events, which reduces the time to search of minimal cut sets by a factor of 2 to 10 depending on the case.

6.4 Goals not achieved

Looking at the original objectives, there are two essential topics which were only partially achieved.

- Uncertainty analysis (quantitative treatment at the system and plant level).
- Implementation of PRA methods in the regulatory work (progressive hold).

The treatment of uncertainties was successfully considered at the component data and parameter estimation level. The Benchmark studies also resulted in useful qualitative insight into the lack of completeness and other types of uncertainty in connection with a full scale PRA study. Nevertheless, the overall management and quantitative estimation of uncertainties on the plant level remain an unresolved issue. The key problems are

- overall management of assumptions, simplifications and boundaries of an analysis, and the influence of these on the risk predictions,
- imperfect state of knowledge about the human contribution and different types of common cause failures, and the correlation between these and the dependence on the management quality and outside influence (regulatory hold, public opinion etc).

Improvements in this respect can be expected to occur gradually as more operating experience accumulates and comparisons can be made with respect to completed PRA studies.

The practical needs of the task concerning the implementation of PRA methods in regulatory work changed during the project. The final product constitutes merely a review of the current status and no progressive work was undertaken. Specifically, there is currently little interest in the Nordic countries concerning the possible implementation of quantitative safety goals. The results of PRA's and other reliability studies can be beneficially used on a relative and/or qualitative basis without depending upon absolute quantitative risk predictions. This type of use avoids the complex problems related to the defination of acceptable risk levels and specifying the absolute uncertainties in the quantitative predictions, which are associated with quantitative safety goals.
In addition, further experience should be obtained in performing and using PRA's before further steps are planned.

6.5 Work left

As indicated above, there remains important research wcrk still to be done. The principal needs will be covered by the following two PRA-related projects in the next NKA program in 1985-88:

- Risk Analysis: The objective is the continued work with uncertainty treatment, completeness question, CCF analysis, and human error analysis. A more challenging Benchmark study is planned which includes human error analysis and gives greater attention to the completeness question.
- Optimization of Technical Specifications: This is a practically oriented project with the aim of applying PRA methods for the balancing of test and repair arrangements in the safety systems.

The ongoing and planned Nordic PRA studies and other practical work will certainly also contribute in the further development of PRA techniques.

6.6 Concluding remarks

The SÄK-1 project has contributed to the development of PRA methodology and the improvement of data bases and computer programs and increased the level of expertise in the Nordic countries. It has also provided an important communications channel for research people, experts working at the regulatory bodies, and utilities and consultants who are relatively small in number in each country separately. In this way, people actively engaged in the development work have received wide support (including constructive criticism) which has certainly had a very productive influence on the practical implementation of available methods and the development of new methods where required.

7. SÄK-1 PUBLICATIONS AND REPORTS

GENERAL REPORTS

1. Proceedings of Project Seminar 1, Helsinki, 8 - 9 April 1981. Technical Research Centre of Finland. Symposium 15/81

2. Proceedings of Project Seminar 2, Helsingør 29 - 31 March 1982. Risø National Laboratory, Risø-M-2363

3. Proceedings of the Workshop on Dependent Failure Analysis, Västerås, 27 - 28 April 1983. Swedish Nuclear Power Inspectorate & ASEA ATOM.

4. Proceedings of the CCF Workshop, Lepolaupi, Espoo, 10 - 11 May 1984. Technical Research Centre of Finland, Symposium Series, 1985.

5. Notes on Worskhop on PRA on Licensing, Lidingö, Decmber 1984. Risø National Laboratory, SÄK-1-0(84)3.

6. MANKAMO, T, PETERSEN, K-E, PÖRN, K & ERICSSON, G, "Experiences from the Nordic Benchmark Analyses". International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, 24 February-- 1 March 1985, San Francisco. Proceedings.

ASEA-ATOM REPORTS

HIRSCHBERG, S and PULKKINEN, U
"Common Cause Failure Data: Experience from Diesel Generator Studies", Nuclear Safety, Vol 26, No 3, May - June, 1985.

HIRSCHBERG, S
"Comparison of Methods for Quantitative Analysis of Common Cause Failures - a Case Study". Proceedings of the International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, 24 Feb - 1 May 1985.

RISØ REPORTS

<u>1981</u>

SÄK-1-D(81)1	Analysis of pipe failures in light water reactors, K E Petersen & P E Becher (SRE-4-81)

<u>1982</u>

SÄK-1-D(82)1	Bounds for the probability of a union - fault tree applications, O Platz (Risø-M-2340)
SÄK-1-D(82)2	Influence of test intervals and repair period limitations for standby systems. H E Kongsø & L Schepper (SPA-1-82)
SÄK-1-D(82)3	SÄK-1 Trial study 1, Danish contribution, H E Kongsø, L Schepper & K Lauridsen (SPA-3-82)
SÄK-1-D(82)5	The use of cause-consequence analysis in defining failure criteria, D S Nielsen & E Nonbøl
SÄK-1-D(82)8	Analysis of pipe failures in Swedish nuclear power plants, K E Petersen (SPA-8-82)
SÄK-1-D(82)10	Data workshop, Danish contribution, K E Petersen & O Platz (SPA-12-82)

<u>1983</u>

SÄK-1-D(83)2	Review of feedwater transients in BWRs, P E Becher (SPA-2-83)

<u>1984</u>

SÄK-1-D(84)1	Benchmark study 2 - Final report, H E Kongsø & K E Petersen
SÄK-1-D(84)2	Computer code comparison - Final report, H E Kongsø & K E Petersen
SÄK-1-D(84)4	Note on interactive fault tree analysis, K E Petersen & N K Vestergaard

STUDSVIK REPORTS

SÄK-1-S(81)1	Pörn K, Implementation and use of FRANTIC for time dependent unavailability analysis STUDSVIK/SD-81/82
SÄK-1-S(82)1	Stenquist C, Identification of common cause candidates in the residual heat removal system in Ringhals 1 STUDSVIK/NR-82/95
SÄK-1-S(82)2	Pörn K, Some comments regarding the use of FRANTIC STUDSVIK/SD-82/108/NR-82/111
SÄK-1-S(82)4	Pörn K, Stenquist C, Benchmark Study of a HPIS Example System Studsvik Technical Report SD-82/112/NR-82/119
SÄK-1-S(83)1	Pörn K, Methods used and results obtained by Studsvik on some NKA/SÄK-1 Data Workshop exercises. STUDSVIK/SD-83/3, /NR-83/229
SÄK-1-S(83)5	Pörn K, About two computer codes for the analysis of dependent failures. STUDSVIK/SD-83/14
SÄK-1-S(83)2	Kjellbert N A, Tuxen-Meyer H, Johansson K-M, Pörn K, Tillförlitlighetsdata för elektriska komponenter i svenska kokvattenreaktorers prefererade/favoriserade hjälpkraftsystem. STUDSVIK/NR-82/217
SÄK-1-S(83)3	Pörn K, NKA/SÄK-1 Reliability Data Workshop - Summary Report. STUDSVIK/SD-83/13/NR-83/250
SÄK-1-S(83)6	Dinsmore S, Kjellbert N A, Pörn K, Åkerlund O, NKA/SÄK-1 Benchmark Study of Loss-of-feedwater. Transients in a BWR, Volume I & II. STUDSVIK/NR-83/279
SÄK-1-S(84)1	Dinsmore S, Simulator Exercise and Results. STUDSVIK/NR-84/355

SÄK-1-S(84)2	Dinsmore S, Operator Time Reliability Curves: A Simulator Data Based Model. STUDSVIK/NR-84/435
SÄK-1-S(84)3	Hellström P*, CCF-analysis of RHRS at Ringhals 1. STUDSVIK/NR-84/465.
SÄK-1-S(85)1	Pörn K, Åkerlund O, Estimation and Robustness of Prior Distributions for the Analysis of Reliability Data. STUDSVIK/NR-85/19

* Royal Institute of Technology, Stockholm

VTT REPORTS

SÄK-1-F(81)1	Aaltonen, P, CONFSI, "A computer Code for Estimating Confidence Limits". Research Report SÄH 34/81, 19.10.1981.
SÄK-1-F(82)3	Mankamo, T, "Importance Measures and Reliability Criteria for Components". Research Report SÄH 13/81, June 1982.
SÄK-1-F(83)2	Lehtinen, E, Mankamo, T & Pulkkinen, U, "Optimum test Interval of Closing Valves". Presented in IAEA Symposim on Reliability of Reactor Pressure Components, Stuttgart, 21 - 25 March 1983.
SÄK-1-F(83)7	Mankamo, T & Pulkkinen, U, "Test Interval Optimization of Standby Equipment". VTT, November 1983.
SÄK-1-F(84)1	Mankamo, T, "Experiences from the Benchmark 2 Study of NKA/SÄK-1". Manuscript December 1984.
SÄK-1-F(84)4	Pulkkinen, U, "A comparison Between Selected Computer Codes for Fault Tree Evaluation". Manuscript December 1984.
SÄK-1-F(82)5	LEHTINEN, E, MANKAMO, T & PULKKINEN, U, "Contribution to Data Worskhop", 15-16 December 1982.

8.0 GLOSSARY OF ABBREVIATIONS

AC	Alternating Current
AD	Automatic Depressurization
AFWS	Auxiliary Feedwater System
ANS	American Nuclear Society
ASAR	As-operated Safety Analysis Report
ASME	American Society of Mechanical Engineers
ATV	Arbetsgruppen för Tillförlitlighet för Värmekraft
BD	Block Diagram
BWR	Boiling Water Reactor
CCD	Cause Consequence Diagram
CCF	Common Cause Failure
CCFA	Common Cause Failure Analysis
CMF	Common Mode Failure
DC	Direct Current
DG	Diesel Generator
ET	Event Tree
ESS	Electric Supply System
FT	Fault Tree
FV	Förvärmare (Pre-heater)
GRS	Gesellschaft für Reaktor Sicherheit
HEP	Human Error Probability
HPIS	High Pressure Injection System
IEEE	Institute of Electrical and Electronics Engineers
KØØ1	Instrument number ØØ1
LIT	Mänsklig Tillförlitlighet - The Nordic project on human reliability

LOCA	Loss of Coolant Accident
MCS	Minimum Cut Sets
MORT	Management Oversight and Risk Tree
MOVØØ1	Motor operated Valve number ØØ1
MØØ1	Motor ØØ1
NKA	Nordic Liaison Committee for Atomic Energy
NPRDS	Nuclear Plant Reliability Data System
NRØØ1	Non Return Valve number ØØ1
OECD	Organisation for Economic Co-operation and Development
OI	Operator Input
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
PØØ1	Pump number ØØ1
RPM-C	Revolution per Minute - Control
RSS	Reactor Safety Study
RWST	Reactor Water Storage Tank
SKI	Swedish Nuclear Power Inspectorate
SRS	System Reliability Services
STUK	Finnish Center for Radiation and Nuclear Safety
SÄK-1	Säkerhetsprojekt-1 - The Nordic project on reliability techniques
TGV	Tillgänglighet Värmekraft
TMI	Three Mile Island nuclear power plant (Unit 2)
USNRC	United States nuclear regulatory commission
VTT	Technical Research Centre of Finland
VØØ1	Valve number ØØ1

Copies of this report can be ordered from

Studsvik Energiteknik AB
Reactor Technology
Safety Analysis
S-611 82 Nyköping
Sweden

The other participating organizations are

Danmark

Risø National Laboratory (Risø)
Dk-4000 Roskilde

Finland

Finnish Centre for Radiation and Nuclear Safety (STUK)
Pl 268
SF-00101 Helsinki 10

Technical Research Centre of Finland (VTT)
Electrical Engineering Laboratory
Otakaan 7B
SF-02150 ESPOO

Norway

Institute for Energy Technology (IFE)
Box 173
N-1751 Halden

Sweden

ASEA-ATOM AB (ASEA)
Box 53
S-721 04 Västerås

Swedish Nuclear Power Inspectorate (SKI)
Box 27106
S-102 52 Stockholm