APRIL 1990

DEPENDENCIES, HUMAN INTERACTIONS AND UNCERTAINTIES IN PROBABILISTIC SAFETY ASSESSMENT

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

DEPENDENCIES, HUMAN INTERACTIONS AND UNCERTAINTIES IN PROBABILISTIC SAFETY ASSESSMENT

Final Report of the NKA Project RAS 470

Edited by:

Stefan Hirschberg
ABB Atom, Sweden

Prepared by:

ABB Atom AB, Sweden
Risø National Laboratory, Denmark
Studsvik AB, Sweden
Technical Research Centre of Finland

APRIL 1990

This report is available on request from:

ABB Atom AB
Library
S-721 63 Västerås
Sweden

ISBN 87 7303 454 1
NORD 1990:57

ABSTRACT

In the context of Probabilistic Safety Assessment (PSA), three areas were investigated in a 4-year Nordic programme: dependencies with special emphasis on common cause failures, human interactions and uncertainty aspects. The approach was centered around comparative analyses in form of Benchmark/Reference Studies and retrospective reviews. Weak points in available PSAs were identified and recommendations were made aiming at improving consistency of the PSAs. The sensitivity of PSA-results to basic assumptions was demonstrated and the sensitivity to data assignment and to choices of methods for analysis of selected topics was investigated.

KEY WORDS

Benchmarks, Common Cause Failures, Decision Making, Dependencies, Finland, Human Factors, Probabilistic Safety Assessment, Risk Assessment, Safety Analysis, Sweden

This report is part of the safety programme 1985-89 sponsored by NKA, the Nordic Liaison Committee for Atomic Energy. The work has been financed in part by the Nordic Council of Ministers, in part by the participating national institutions and regulatory bodies.

SUMMARY

Probabilistic Safety Assessment (PSA) is an important tool for safety analysis within the nuclear sector in Finland and Sweden. Plant-specific PSAs, in regard of accidents which could lead to core damage, (level 1) are available for ten of the twelve Swedish nuclear power plants and for four Finnish plants. For the remaining two Swedish plants the studies are in progress. Also in the non-nuclear field there is a clear tendency of growing number of applications of PSA-techniques.

Merits of the PSAs which have been carried out are indisputable. Insights gained from the studies have in many cases led to modifications at the plants and hereby to significant safety improvements. Presently the available PSAs are being applied in the everyday safety work. At the same time there are several limitations, both intrinsic and practical, associated with use of probabilistic techniques.

The present project addressed two topics generally considered as major limitations of PSAs, i.e. dependent failures i.e. propagated failures or multiple failures of common causes, (with main emphasis on the latter), and human interactions. In addition, uncertainty aspects in the PSA-context were investigated. The purpose of the project was to study the impact of different assumptions, methods and data of PSAs in order to find ways of improving their consistency and ability of providing guidance. Furthermore, the project aimed at exploring the question of accounting for uncertainty in PSA analyses.

The project included Benchmark studies, where different groups performed parallel and independent analysis of selected reference cases. Previous PSA studies were also critically reviewed.

The following Benchmark Exercises and Reference Studies were carried out within the project:

- Common Cause Failure (CCF) Data Benchmark Exercise
- Reference Study on Human Interactions
- Reference Study on Uncertainty and Sensitivity Analysis.

Four Nordic working groups participated in the above studies. A common basis for analysis was established in terms of agreed assumptions and boundary conditions. The remaining degree of freedom varied between the studies, being highest in the Reference Study on Human Interactions.

In the Benchmark Exercise on CCF-data, motor-operated valves (MOVs) at Swedish Boiling Water Reactor (BWR) plants were selected for the study. As primary sources of information, failure reports from the Scandinavian Nuclear Power Reliability Data system and Swedish Licensee Event Reports were used. The study was divided into two phases, one qualitative (focused on CCF-identification) and one quantitative (application to four redundant MOVs in a safety system at the Forsmark 1 plant).

The Reference Study on Human Interactions concerned manual depressurization at the Forsmark 3 plant. According to the PSA for that plant this particular operator interaction is critical in accident sequences situated by loss of feedwater.

The Reference Study on Uncertainty and Sensitivity Analysis concerned the risk dominant accident sequence identified in the Forsmark 3 PSA. The selected sequence is dominated by CCF-contributions for motor-operated valves (previously studied within the CCF-data Benchmark Exercise) and by operator failure to initiate manual depressurization (previously studied within the Reference Study on Human Interactions). The study was followed up by an investigation of the principal problem of decision making in view of uncertainties.

Retrospective analyses of previous PSAs were carried out in regard of treatment of dependencies, treatment of human interactions and sensitivity studies of common cause failures and human interactions. PSAs for six plants (Barsebäck 1, Forsmark 3, Oskarshamn 1, Oskarshamn 3, Ringhals 1 and Ringhals 2) were included in the retrospective analyses.

Other topics considered in the project include time-dependent phenomena in PSA, combination of data sources and treatment of external events.

The dependencies among the components of system subject to PSA are constituting possibilities of failures. Significant dependencies were identified in several PSAs which otherwise hardly would have been detected. The treatment of functional and shared-equipment dependencies, and of equipment-related Common Cause Initiators is well-established, although completeness and consistency of the reviewed PSAs can be improved. Some simple rules exist with regard to modeling of physical and human interactions dependencies. Difficulties encountered in treatment of errors of commission (i.e. incorrect operative actions) may, however, introduce complex dependencies, and call for future

research. Potentially significant contributors, such as dynamic effects (pipe whips, jets, secondary missiles) which may follow upon a pipe break are often disregarded. This calls for guidance in order to establish a more systematic approach in the PSAs.

The CCF-data Benchmark Exercise demonstrated that available failure reports may provide sufficient basis for identification of potential common cause failures (CCF). The methods used for CCF-identification are straight-forward, but availability of more detailed background material is desirable. Thus, improvement of failure reports originating from the periodical overhauls of the reactors is of primary interest.

It was observed that estimates of CCF-contributions vary considerably. This is generally due to differences in the treatment of data (e.g. interpretation of failure reports, use of application- and design-oriented screening, use of extension schemes and weighting of potential CCFs) rather than to the choice of a particular estimation method. Use of parametric models represents a suitable approach when good quality single failure data (e.g. Swedish Reliability Data Book) are available. It was confirmed that the alpha-factor method provides a more correct representation of statistical uncertainties than the Multiple Greek Letter (MGL) model. An important finding is that relatively few component types constitute the principal CCF-contributors. Thus, future efforts regarding improvements of data should primarily concern these components.

Some main weaknesses of the current state of CCF-analysis which would justify further development were identified. They concern qualitative aspects such as limited understanding of relevant failure mechanisms as well as of the possibility of defensive measures against CCFs. The same applies to CCF-contributions in systems with ultra high redundancy level.

The studies performed in the project show that human interactions have a relatively strong impact on PSA-results. Contrary to the treatment of dependencies, analyses of human interactions in the Swedish PSAs are usually rather superficial. Here, PSAs have thus far been concentrated on the hardware functions; justified in part by a "30 minutes rule", reducing the need of operator interactions within 30 minutes of an accident; by the fact that there are rather few critical operator actions for the Swedish BWRs; and beacuse well-established methods for treatment of human interactions are still missing.

The principal human interactions contributing to failures that form parts of the risk dominant sequences include:

For BWRs

- manual depressurization of the reactor pressure vessel after transients with loss of ordinary and auxiliary feedwater systems (Forsmark 3, Oskarshamn 3)
- back-flushing of screens in the emergency core cooling system and containment cooling spray system after large or medium loss of coolant accident (Barsebäck 1, Oskarshamn 1, Ringhals 1).

For PWRs according to the PSA of Ringhals 2

- failure to depressurize and failure to switch to "high-head" recirculation after a small loss of coolant accident (some other operator actions have, however, only a slightly smaller importance).

There are large uncertainties in quantification of the failure probabilities of manual depressurization and back-flush operation. In the case of back-flush operation, questions remain with respect to the time available for the action. For plants where depressurization only can be activated manually in the aboved mentioned transients, modification of the action signal logic of the pressure relief system is presently being discussed. This would lead to substantial reduction of the total core damage frequency of the affected plants.

Only few accident sequences involving actions for recovery of control have been modeled in the Swedish PSAs. As mentioned above in the context of human interaction dependencies, errors of commission have so far been disregarded in the available studies and should be given more attention.

It is important that boundary conditions are clearly specified for the analysis of human interactions. This was demonstrated in the reference study concerning manual depressurization. When given equal boundary conditions agreement between analyses performed by the different groups was satisfactory. This applies also to the comparison of THERP (Technique for Human Error Rate Prediction) method and HCR (Human Cognitive Reliability) model, as far as the probability of misdiagnosis is concerned. Some flaws of the HCR-method have been pointed out.

The project study also resulted in concrete recommendations concerning both ergonomical and procedural improvements. In addition, the usefulness of simulator exercises as a supporting tool for analysis of human interactions was demonstrated.

The Reference Study on Uncertainty and Sensitivity Analysis showed that the statistical uncertainties associated with the estimated frequency of the analysed accident sequence are large, since the overall uncertainty interval covers at least two decades. This was expected since the sequence involved a critical human interaction combined with common cause failure in a system with high level of redundancy. There are no data to allow an estimate of the failure rate of the particular operator action. Thus, the estimate will have to rely on subjective judgement. In the case of common cause failures the estimates of the overall uncertainty mainly depends on the choice of screening assumptions, on methods of quantification and on probability distributions.

The numerical agreement between the analyses performed by the different groups was drastically improved in the course of the reference study due to modeling refinements and provision of more realistic data.

"State-of-knowledge" dependencies, here component failure probabilities originating from the same data source were shown to have a surprisingly large impact on the numerical results. Consequently, the result of a traditional point value analysis may not be representative for the uncertainty distribution.

Additional methodological insights concern the significance of higher order terms in the uncertainty polynomial, measures for uncertainty contributors, and application of the Bayesian approach.

Computer codes for Monte Carlo analysis of uncertainty propagation (MONTEC, MOCARE, SAMPLE, SPASM) were compared and appear to be in good agreement. However, the precision of mean and standard deviation generated by Monte Carlo technique is much more dependent on the sample size than precision of percentiles.

Bayesian methods are generally used to describe the parametric uncertainties. By these methods it is relatively easy to utilize "learning from experience". The Bayesian thinking presupposes acceptance of the concept of subjective probability. This type of probability can be assigned also to nonstatistical events, a concept which is of great importance in the context of uncertainty handling in risk analyses. In the future one can foresee a further development where subjective probabilities will be used also for description of modeling uncertainties.

According to basic probability laws one can express the total uncertainty with integral probability values, i.e. without any further uncertainty bounds. This will greatly facilitate the decision making process, where one tries to find the action alternative that corresponds to the minimum expected risk.

The present report consists of six chapters and two appendices. The first chapter provides project background, objectives, scope, organization and time schedule. Studies of dependencies, i.e. Common Cause Failure Data Benchmark Exercise and retrospective qualitative analyses, are described in chapter 2. Chapter 3 covers analyses of human interactions including Reference Study and retrospective qualitative analyses. Uncertainty aspects are illustrated in chapter 4 which contains a summary of the Reference Study on Uncertainty and Sensitivity Analysis and sensitivity studies of common cause failures and human interactions. Furthermore, limitations of PSA and the problem of decision making in view of uncertainties, are treated. Chapter 5 illustrates studies of selected topics such as time-dependent phenomena in PSA, combination of data sources and treatment of external events. Chapter 6 presents insights, conclusions and recommendations. Appendix A contains a list of project publications and Appendix B glossary of abbreviations.

A more detailed (Executive) summary of the present project may be found in "Risk Analysis and Safety Rationale" (Editor Gunnar Bengtsson), the final report of a joint Nordic research program in nuclear safety, NORD-report 1989:91.

SAMMANFATTNING (in Swedish)

Probabilistisk Säkerhetsanalys (PSA) används som ett viktigt verktyg för säkerhetsanalys inom kärnkraftssektorn i Finland och Sverige. Blockspecifika PSA, som behandlar olycks-sekvenser som kan leda till härdskada (nivå 1), finns tillgängliga för tio av de tolv svenska kärnkraftverken och för samtliga fyra finska kärnkraftverk. För de återstående två svenska verken pågår arbetet med att ta fram nivå 1 PSA. Även inom det icke-nukleära området finns en klar tendens att använda probabilistiska metoder i ökad omfattning.

Fördelarna med de PSA som utförts är odiskutabla. Resultat och slutsatser från studierna har i många fall lett till modifieringar på verken och därigenom till signifikanta förbättringar av säkerheten. För tillfället används de tillgängliga PSA studierna i det dagliga säkerhetsarbetet. Samtidigt finns det ett flertal begränsningar, både inherenta och praktiska, förknippade med användandet av probabilistiska metoder.

Det aktuella projektet behandlade två områden som allmänt anses utgöra viktiga begränsningar; beroende fel, dvs följdfel eller fel med gemensam orsak (där tyngdpunkten i projektet var på det senare) och mänsklig växelverkan. Dessutom behandlades även osäkerhetsaspekter i PSA sammanhang. Målsättningen för projektet var att undersöka och belysa inverkan av olika antaganden, metoder och data för PSA-resultat och med utgångspunkt från detta finna sätt och metoder som ger ett bättre perspektiv på studiernas slutsatser och förbättrar möjligheten till att använda PSA-studier. Dessutom syftade projektet till att undersöka frågan om osäkerhetsanalyser i PSA-sammanhang.

Analyserna genomfördes mestadels som Benchmarkövningar, dvs parallella och oberoende analyser utfördes på utvalda referenssekvenser av olika arbetsgrupper. Vidare utfördes granskningar av tidigare analyser.

Följande Benchmarkövningar och referensstudier utfördes inom projektet:

- Benchmarkövning avseende data för fel med gemensam orsak (CCF)
- Referensstudie avseende mänsklig växelverkan
- Referensstudie avseende osäkerhets- och känslighetsanalys.

Fyra nordiska arbetsgrupper deltog i ovanstående studier. En överenskommelse om gemensamma antaganden och randvillkor för analysen gjordes innan analysarbetet påbörjades. Frihetsgraden varierade mellan studierna och var högst för referensstudien avseende mänsklig växelverkan.

För Benchmarkövningen avseende CCF-data valdes motormanövrerade ventiler i svenska kokvattenreaktorer som analysobjekt. Som primära feldatakällor användes felrapporter från ATV-kansliet (Arbetsgruppen för Tillförlitlighet, Värmekraft) och RO-rapporter (Rapportervärd Omständighet) från SKI. Studien delades in i två faser, en kvalitativ fas (vilken fokuserades på CCF identifiering) och en kvantitativ fas (där applikationen gällde fyra redundanta motormanövrerade ventiler i ett säkerhetssystem vid Forsmark 1 verket).

Referensstudien avseende mänsklig växelverkan behandlade manuell tvångsnedblåsning vid Forsmark 3 verket. Enligt PSA-studien för Forsmark 3 är detta operatörsingrepp en av händelserna i den mest dominerande olyckssekvensen.

Referensstudien avseende osäkerhets- och känslighetsanalys behandlade den ur risksynpunkt dominerande sekvensen identifierad i Forsmark 3 PSA. Den utvalda sekvensen domineras av CCF-bidrag från motormanövrerade ventiler (vilka tidigare studerades i CCF-data Benchmark övningen) och av misslyckad manuell tvångsnedblåsning (vilket tidigare behandlats i referensstudien avseende mänsklig växelverkan). Studien följdes upp med ett arbete avseende det principiella problemet hur man hanterar osäkerhetsaspekter vid beslutsfattande.

Retrospektiva analyser av tidigare gjorda PSA-studier utfördes med avseende på behandling av beroenden och av mänsklig växelverkan samt med känslighetsstudier av fel med gemensam orsak (CCF) och mänsklig växelverkan. PSA för sex svenska verk (Barsebäck 1, Forsmark 3, Oskarshamn 1, Oskarshamn 3, Ringhals 1 och Ringhals 2) behandlades i de retrospektiva analyserna.

Övriga specifika områden som behandlats inom projektet är tidsberoende fenomen i PSA, kombinering av datakällor och behandling av yttre händelser.

Beroenden mellan komponenter utgör en möjlighet till fel. Signifikanta beroenden har identifierats i ett flertal PSA-studier, vilka knappast skulle ha upptäckts annars. För de beroenden som är explicit modellerade är idag behandling av funktionella beroenden, av beroenden som uppstår via gemensam utrustning samt av utrustningsrelaterade inledande händelser som resulterar i systemväxelverkan ("Common Cause Initiators"; CCIs), väletablerad. Dock kan fullständighet och konsistens i behandlingen av dessa frågor förbättras i befintliga PSA-studier. Några enkla regler finns för modellering av fysiska beroenden och

mänsklig växelverkan med potential för beroenden. De svårigheter som finns beträffande behandling av aktiva operatörsingrepp (errors of commission), vilka troligen leder till komplexa beroenden, påkallar dock behovet av framtida forskning inom området. Potentiellt viktiga bidrag som t ex dynamiska effekter efter ett rörbrott (jetstrålar, sekundära missiler) har i ett flertal fall förbisetts. För fall av denna art behövs procedurer och guider för att etablera ett systematiskt angreppssätt.

Benchmarkövningen för CCF-data visade att tillgängliga felrapporter kan utgöra tillräcklig bas för att identifiera fel med gemensam orsak (CCF). De metoder som används för CCF-identifiering är relativt enkla men tillgång till ytterligare bakgrundsinformation är önskvärd. Kvalitetsförbättring av felrapporter som härstammar från verkens årliga avställnings-perioder är av största intresse.

Den observerade skillnaden i estimeringen av CCF-bidrag kan oftast hänföras till olikheter i behandling av data (t ex tolkning av felrapporter, användning av applikations- och design-orienterade anpassningar, användning av utvidgningsscheman och viktning av potentiella CCF), snarare än till val av olika estimeringsmetoder. Användning av parametriska modeller är ett godtagbart angreppssätt då högkvalitativa enkelfelsdata föreligger (t ex den svenska T-boken). Bekräftelse erhölls på att alfa-faktor metoden ger en mer korrekt bild av de statistiska osäkerheterna än vad MGL (Multiple Greek Letter) metoden ger. En viktig slutsats är att relativt få komponenttyper ger CCF-bidrag av stor betydelse för resultat av PSA. Framtida arbeten och förbättringar bör därför koncentreras på dessa komponenttyper.

Den nuvarande CCF-analysens huvudsakliga svaghet, vilket motiverar vidare forskning och utveckling inom området, är behandling av kvalitativa aspekter som t ex begränsad förståelse för relevanta felmekanismer och möjligheten till försvarsåtgäder mot CCF. Utvecklingsinsatser är också motiverade inom området CCF-bidrag för högredundanta system.

De inom projektet utförda studierna visade att mänsklig växelverkan har en relativt stor inverkan på PSA-resultat. I motsats till behandling av beroenden är analyser av mänsklig växelverkan generellt relativt översiktliga i svenska PSA-studier. Förklaringen till detta är att den första generationen PSA-studier koncentrerade sig på hårdvaran i systemanalysen. Detta i sin tur delvis motiverat tack vare "30 minuters regeln", som reducerar operatörens

roll i ett 30 minuters intervall vid ett tillbud, delvis genom att det finns ganska få kritiska operatörsingrepp för svenska kokvattenreaktorer samt det faktum att det initiellt inte fanns några genomarbetade, väletablerade metoder för behandling av mänsklig växelverkan.

De huvudsakliga bidragen från mänsklig växelverkan i dominerande sekvenser omfattar:

För kokvattenreaktorer

- misslyckad initiering av tvångsnedblåsning i reaktortanken vid transienter med förlust av både ordinarie- och hjälpmatarvattensystem (Forsmark 3, Oskarshamn 3).
- misslyckad backspolning av härdnödkylningssystemets och reaktorinneslutningskylsystemets silar efter en stor eller medelstor LOCA (Barsebäck 1, Oskarshamn 1, Ringhals 1).

För tryckvattenreaktorer enligt Ringhals 2 PSA

- misslyckad trycknedsättning och misslyckad omkoppling till "high-head" recirkulation efter liten LOCA (även andra operatörsingrepp har något mindre dock jämförbar betydelse).

Kvantifieringsosäkerheterna är stora kring sannolikheten för misslyckad manuell tvångsnedblåsning och backspolning. Fortfarande kvarstår frågor kring tillgänglig tid för åtgärder. För verk där manuell tvångsnedblåsning är nödvändig för ovan nämnda transienter diskuteras för närvarande ändringar i signallogiken för tryckavlastningssystemet. Detta skulle leda till en signifikant reduktion av den totala härdskadefrekvensen för aktuella verk.

Endast ett fåtal återställningsåtgärder har modellerats i de svenska PSA-studierna. Som tidigare nämnts har man vad avser beroenden som uppstår via mänsklig växelverkan, i princip bortsett ifrån aktiva operatörsingrepp (errors of commission). I framtida studier borde dessa ges en större uppmärksamhet.

Betydelsen av att ha klara specifikationer vad gäller grundantaganden och randvillkor vid analys av mänsklig växelverkan har visats i referensstudien för manuell tvångsnedblåsning. Med samma grundantaganden stämde det numeriska resultatet ganska väl överens mellan de olika grupperna. Detta gäller också för jämförelsen mellan THERP- (Technique for Human Error Rate Prediction) metoden och HCR- (Human Cognitive Reliability) modellen vad avser sannolikheten för felaktig diagnos. Några brister i HCR-modellen har dock konstaterats.

Referensstudien resulterade också i konkreta rekommendationer avseende både ergonomiska och procedurförbättringar. Dessutom har nyttan av simulatorövningar som ett hjälpverktyg vid analys av mänsklig växelverkan klart framgått.

Referensstudien avseende osäkerhets- och känslighetsanalys visade att de statistiska osäkerheterna för de analyserade sekvensernas frekvenser är stora, det totala osäkerhetsintervallet spänner över minst två dekader. Detta var väntat eftersom sekvenserna domineras av ett kritiskt operatörsingrepp kombinerat med ett fel med gemensam orsak (CCF) i ett system med en hög redundansnivå. Eftersom det inte finns några erfarenhetsdata för operatörsingreppet blir estimeringen av felsannolikheten starkt beroende av subjektiva bedömningar. Vad gäller felet med gemensam orsak (CCF) varierar estimeringen av osäkerhetsintervallet beroende på valet av metod för anpassning ("screening"), för kvantifiering samt val av sannolikhetsfördelningar.

Den numeriska överensstämmelsen mellan gruppernas resultat förbättrades drastiskt under arbetet med referensstudien. Detta tack vare modelleringsförbättringar och ansättning av mer realistiska feldata.

"State-of-knowledge" beroenden, i detta fallet komponentfeldata som härstammar från samma databas visade sig ha förvånansvärt stor inverkan på det numeriska resultatet. Som en konsekvens av detta kan inte traditionell punktuppskattningsanalys vara representativ för osäkerhetsfördelningar.

Ytterligare metodinsikter har erhållits avseende betydelsen av högre ordningens termer i osäkerhetspolynomet, mått på olika händelsers bidrag till osäkerheten och användning av det bayesianska angreppssättet.

Monte Carlo-baserade datorprogram för osäkerhetsberäkningar (MONTEC, MOCARE, SAMPLE, SPASM) jämfördes och visade på en god överensstämmelse. Studien visade vidare att precisionen för medelvärdet och standardavvikelsen är mycket mer beroende av antalet simuleringar än precisionen för percentilvärdena.

Bayesianska metoder är generellt användbara för att beskriva den parametriska osäkerheten. Med hjälp av dessa metoder är det förhållandevis lätt att successivt beakta nya data och erfarenheter. Det bayesianska tänkesättet bygger på begreppet subjektiv sannolikhet. Denna typ av sannolikhet kan ansättas även för icke repeterbara händelser, vilket är en mycket viktig egenskap i samband med osäkerhetshantering inom riskanalys. I framtiden kan man förutse en ytterligare utveckling mot att använda subjektiva sannolikheter även för modelleringsosäkerheter.

I enlighet med grundläggande sannolikhetslagar kan den totala osäkerheten uttryckas med hjälp av integrala sannolikhetsvärden, dvs utan några osäkerhetsintervall. Detta kommer att åtskilligt underlätta beslutsfattandeprocessen där man söker det alternativ som svarar mot minst förväntad risk.

Föreliggande sammanfattningsrapport består av sex kapitel och två appendix. Det första kapitlet innehåller projektbakgrund, mål, omfattning, organisation och tidsschema för arbetet. Studier av beroenden, dvs CCF-data Benchmarkövning och retrospektiva kvalitativa analyser finns beskrivna i kapitel 2. Kapitel 3 behandlar analyser av mänsklig växelverkan vilket inkluderar referensstudie och retrospektiva kvalitativa analyser. Osäkerhetsaspekter täcks in i kapitel 4 som innehåller en sammanfattning av referensstudien avseende osäkerhets- och känslighetsanalys samt känslighetsstudier av fel med gemensam orsak och mänsklig växelverkan. Vidare behandlas begränsningar i PSA och problematiken kring osäkerhetshantering vid beslutsfattande. Kapitel 5 beskriver studier gjorda inom speciella områden såsom tidsberoende fenomen i PSA, kombinering av datakällor samt behandling av yttre händelser. Kapitel 6 ger slutsatser och rekommendationer. I appendix A finns en lista över projektets publikationer och rapporter och Appendix B innehåller en lista över använda förkortningar.

En mer detaljerad sammanfattning ("Executive Summary") av föreliggande projekt återfinns i "Risk Analysis and Safety Rationale" (Editor Gunnar Bengtsson), som är slutrapporten i ett gemensamt nordiskt forskningsprogram inom kärnkraftssäkerhet, NORD-rapport 1989:91.

LIST OF CONTENTS

1. INTRODUCTION

In 1985 a Nordic project "Risk Analysis" (RAS-470) was initiated as a part of the research programme of the Nordic Liaison Committee for Atomic Energy (NKA). The participants in this project included both authorities, utilities, research institutes and the Swedish vendor of nuclear power plants. The project activities were completed in 1989. RAS-450, another related research project carried out within the same programme concerned optimization of technical specifications using probabilistic methods (Laakso et al., 1990)

This report summarizes the results of work carried out within the RAS-470 project. Some closely related insights from SUPER-ASAR (G. Johanson, ed., 1990), a parallel Swedish project aiming at consistent comparison of Swedish Probabilistic Safety Assessment (PSA) studies for nuclear power plants, with due regard to differences in assumptions, modeling and completeness aspects, will also be reviewed. The two projects have been partially coordinated in the sense that RAS-470 continuously provided methodological insights which then directly were applied within SUPER-ASAR.

The present report is mainly based on material published in the form of summary reports, articles and conference contributions during the course of the project. All previous publications address specific topics, while the present report provides an overall review of the project findings.

1.1 What Is Probabilistic Safety Assessment ?

The main objective of safety analyses of industrial facilities is to minimize the potential for injuries and loss of human life, for negative impact on the environment and for damage of the facility itself, which may follow upon an uncontrolled development of accident conditions. Basic steps in a safety analysis involve:

- identification of primary disturbances (initiating events)
- analysis of progression of selected disturbances with due regard to plant/operator responses
- analysis of releases of toxic or radioactive substances
- analysis of environmental transport and consequences.

These steps are carried out independently of the type of safety analysis being performed. However, in a deterministic safety analysis pessimistic assumptions are made and conservative criteria are chosen for safety functions. Components and operators are assumed to act deterministically and accidents occur also deterministically. Different protection barriers are analysed one at a time with new pessimistic assumptions. Finally, the safety level is not quantified in a deterministic safety analysis. Such analysis is not capable to result in a realistic picture of accident propagation and of the associated environmental consequences. In addition, it cannot reflect the relative importance of different accident sequences. By definition deterministic analyses frequently focus on the worst possible cases. Traditionally, the results of a deterministic approach showing that the plant considered can be brought to a stable and safe state after occurrence of selected postulated safety challenging incidents, have been used as a deterministic unquantified assurance of the safety of the plant.

A supplementary and more balanced picture may be obtained by superimposing a probabilistic perspective on the main steps of safety analysis. By nature failure modes of technical systems are stochastic, human interactions with the systems are hardly deterministic and initiating events occur randomly. Probabilistic Safety Assessment (PSA) provides a structured and logical procedure for identification of credible accident sequences, for assessment of corresponding likelihood and delineation of associated consequences.

In nuclear power applications three PSA levels can be distinguished.

Level 1 PSA comprises identification and quantification of accident sequences leading to core damage.

Level 2 PSA includes analysis of core melt progression and containment response, which combined with Level 1 results leads to determination of the magnitude, isotope contents and frequency of radioactive releases.

Level 3 PSA together with results of Level 2 covers environmental transport of radionuclides and assessment of radiation doses to the population. Hereby an estimate of public risks is obtained.

Within the nuclear sector in Finland and Sweden use of PSA-techniques is today regarded as a natural element in everyday safety work. The principal merits of PSAs include the potential to identify possible weak spots in the design and operation of the plants and to rank the dominant risk contributors. These insights may directly lead to safety improvements at the plants by means of design modifications and/or procedural changes. Swedish PSAs have resulted in implementation of numerous significant improvements. At the same time the PSAs increase operator's awareness of the safety significance of various operational and maintenance tasks, and consequently make them better prepared for possible emergency situations. Examples of practical applications of PSAs involve planning and reviewing of plant modifications, establishment of the basis for a systematic evaluation of operating experience when analysing disturbances and incidents, and supplying input for giving priority to research projects. Also in the non-nuclear field there is a clear tendency of growing number of applications of PSA-techniques.

PSAs also have serious limitations which impact their applicability. The merits of PSAs are, however, indisputable given that the analysts are aware of the limitations and the practitioners use the results within the intended frame.

1.2 Project Background

The applications of PSA-techniques in Nordic countries have been continuously supported by an extensive research programme. In particular, several Benchmark Exercises and Reference Studies have been performed within the safety programmes initiated by the Nordic Liaison Committee for Atomic Energy (NKA).

The first major project of this type NKA/SÄK-1 ("Probabilistic Risk Assessment and Licensing") was carried out in the period 1981-85 (Dinsmore, ed., 1985). The project aimed also at presentation of the guidelines for the application of probabilistic methods in the regulatory work, including evaluation of benefits and limitations. The main emphasis was on fundamental modeling issues associated with systems analysis and with subsequent probabilistic evaluation of accident sequences at nuclear power plants. In this context, the fact that existing alternative techniques can benefit from comparisons and verification, has been recognized. In order

to provide a practical framework for comparison work, two Benchmark Exercises were performed (Mankamo et al., 1985):

- Reliability analysis of a typical high pressure injection system for a PWR plant

and

- Modeling and quantification of disturbance sequences resulting in the loss of feedwater in a BWR plant.

As a supplement to these two exercises two additional Benchmark type studies have been performed within the NKA/SÄK-1 project:

- Comparison of computer codes for minimal cut-set identification and quantification (Pulkkinen, 1985)
- Comparison of methods for quantification of Common Cause Failure (CCF) contributions (Pulkkinen, ed., 1987).

In view of the results of the research projects it was evident that the state-of-the-art in PSA has reached a certain degree of maturity. There was a general agreement that the studies have significant merits and should be used (in several cases had already been used) as an important tool for decision-making. At the same time there are many remaining problems and limitations in using probabilistic techniques. Some of them are intrinsic and difficult (or impossible) to overcome, while other are matters of practice and thus bound to be resolved as understanding of analytical methods becomes more widespread (Lewis, 1984). The limitations of PSA techniques contribute to the overall uncertainty of the results. Two selected topics, namely:

- dependent failures (particularly CCFs)

and

- human interactions,

have been clearly identified as major limitations. The treatment of these issues influences the credibility of the studies, the question of completeness and the interpretation of results. During the last years one has witnessed a deeper understanding as well as an increasing number of methods for handling of these two topics. Alternative approaches, based on different assumptions, have been used. It is rather natural that such an intensive development has led to a situation, where models have sometimes been applied in a somewhat

uncontrolled way, without due consideration of basic assumptions, associated limitations and uncertainties. Furthermore, the models developed have frequently not been compatible with the status of data sources for CCFs and human errors. Although the nature of these limitations is to a certain extent intrinsic, there is a great potential for progress. A more disciplined approach to the problems could certainly provide valuable insights, eliminate existing inconsistencies and decrease potential for possible misuse of available studies. Consequently the use of PSAs as a tool for decision making would be facilitated.

The efforts proposed to be undertaken within the RAS-470 project (Hirschberg, 1985) were intended to contribute to progress in the treatment of the above mentioned issues.

1.3 Objectives and Scope of the RAS-470 project

The following objectives were specified for the RAS-470 project:

1) Review and evaluate the current state of PSA-techniques with special emphasis on treatment of dependencies, human errors and uncertainties, which could lead to identification of significant differences in analytical approaches of selected PSA-studies.

2) Investigate the sensitivity of results obtained from PSA-studies to basic assumptions, to data assignments and to choices of methods for analysis of selected topics.

3) Identify weak points and suggest improvements of practised approaches.

4) Exchange new ideas and supply methodological support to current and planned projects related to topics mentioned above.

The participants in the project were convinced that these objectives will be best met by concentration of the resources on CCF and human interaction aspects. In relative terms significantly larger efforts were devoted within the RAS-470 project to studies of dependencies than to studies of human interactions. Application of Benchmark and Reference Studies, and use of retrospective analyses have been recognised at an early stage of the project as a suitable form for investigation and comparison of alternative modeling approaches.

Thus, the main tasks of the RAS-470 project involved:

- Common Cause Failure Data Benchmark Exercise (Hirschberg, ed., 1987); covered in subchapter 2.2 of this report.

- Retrospective Qualitative Analysis of Treatment of Dependencies in Swedish (Hirschberg, 1987) and Foreign PSAs (Pulkkinen and Simola, 1987); see subchapters 2.3 and 2.4, respectively.

- Reference Study on Human Interactions (Hirschberg, ed., 1989); see subchapter 3.2.

- Retrospective Qualitative Analysis of Treatment of Human Interactions in Swedish (Bengtz and Hirschberg, 1987) and Foreign PSAs (Pyy and Pulkkinen, 1988); see subchapters 3.3 and 3.4, respectively.

- Reference Study on Uncertainty and Sensitivity Analysis (Hirschberg et al., 1989b); see subchapter 4.2.

- Sensitivity Studies of Common Cause Failures and Human Interactions in Swedish PSAs (Hirschberg et al., 1989a); see subchapter 4.3.

- Decision Making in View of Uncertainties (Pulkkinen and Pörn, 1990); see subchapter 4.5.

Other topics specifically addressed within the RAS-470 project include:

- Time-dependent Phenomena in PSA (Simola et al., 1988); see subchapter 5.1.

- Combination of Data Sources (Pulkkinen et al., 1987); see subchapter 5.2.

- Treatment of External Events (Hirschberg and Gunsell, 1989); see subchapter 5.3.

Organization of the present report is indicated in the list of main tasks given above.

1.4 Organization and Time Schedule of the Project

The project has been carried out by four working groups:

- ABB Atom (ATOM), Sweden

- Risø National Laboratory (RISØ), Denmark

- Studsvik AB (STUDSVIK), Sweden

- Technical Research Centre of Finland (VTT).

The work has been directed by a Project Group composed of one representative from each working group and of experts from the Swedish

Nuclear Power Inspectorate, Finnish Centre for Radiation Protection and Nuclear Safety, Imatran Voima Oy, Teollisuuden Voima Oy and the Swedish State Power Board. In addition, the project activities have been followed by representatives of OKG and Sydkraft.

Table 1.1 shows the project schedule and expended resources.

Table 1.1

Project schedule and expended resources

Tasks	Person-months	1985	1986	1987	1988	1989
1. Prestudy	2.0	2.0	-	-	-	-
2. Studies of Dependencies						
- CCF-data Benchmark Exercise	25.0	7.5	13.5	4.0	-	-
- Retrosp. Qualit. Analysis						
. Swedish PSAs[a]	3.5	-	1.0	2.5	-	-
. Foreign PSAs	4.0	-	1.5	2.5	-	-
3. Studies of Human Interactions						
- Reference Study	8.0	-	3.0	3.5	0.5	1.0
- Retrosp. Qualit. Analysis						
. Swedish PSAs[a]	3.0	-	0.5	2.5	-	-
. Foreign PSAs	3.5	-	1.5	2.0	-	-
4. Sensitivity and Uncertainty Analysis						
- Reference Study	25.5	-	-	-	12.5	13.0
- Sensitivity Studies[a]	8.0	-	-	0.5	6.0	1.5
- Decision Making	4.0	-	-	-	2.0	2.0
5. Studies of Selected Topics						
- Time-dependent Phenomena	4.0	-	-	1.5	2.5	-
- Combination of Data Sources	1.5	-	-	1.5	-	-
- External Events	1.0	-	-	-	-	1.0
6. Project Coordination	5.0	1.0	1.0	1.0	1.0	1.0
7. Dissemination of Project Results (including Final Report)	14.0	-	0.5	3.0	4.5	6.0
Person-years total	9					

[a]Partially carried out and funded within the SUPER-ASAR project

1.5 References

Bengtz, M. and Hirschberg, S.(1987)
Retrospective Analysis of Human Interactions in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. Report RAS-470(87) 5 (ABB Atom Report RPC 87-54), July 1987.

Dinsmore, S., ed. (1985)
PRA Uses and Techniques, A Nordic Perspective. Summary Report of the NKA project SÄK-1, Nordic Liaison Committee for Atomic Energy, 121 pp., June 1985.

Hirschberg, S. (1985)
NKA-project 85-89: "Risk Analysis" - Proposed Technical Content. Report RAS-470(85)1 (ABB Atom Report KPA 85-124), May 1985.

Hirschberg, S. (1987)
Retrospective Analysis of Dependencies in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. Report RAS-470(87)4 (ABB Atom Report RPC 87-36), July 1987.

Hirschberg, S., ed. (1987)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report RAS-470(86)14 (ABB Atom Report RPA 86-241), June 1987.

Hirschberg, S., ed. (1989)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Reference Study on Human Interactions. Report RAS-470(89)17 (ABB Atom Report RPC 89-112), December 1989.

Hirschberg, S., Björe, S. and Jacobsson, P. (1989a)
Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA '89 -International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S., Jacobsson, P., Petersen, K.E., Pulkkinen, U., Pörn, K. (1989b)
A Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Hirschberg, S. and Gunsell, L. (1989)
Defensive Measures Against External Events and Status of External Event Analysis in Swedish Probabilistic Safety Assessments for Nuclear Power Plants. Second International Post - SMiRT Seminar "Probabilistic Risk Assessment (PRA) of Nuclear Power Plants for External Events", Irvine, California, U.S.A., August 21-22, 1989.

Johanson, G., ed. (1990)
SUPER-ASAR, Final Report (in Swedish), to be published 1990.

Laakso, K., Knochenhauer, M., Mankamo, T. and Pörn, K. (1990)
NKA/RAS 450 Final Report: Optimization of Technical Specifications Using Probabilistic Methods - A Nordic Perspective, to be published 1990.

Lewis, H. W. (1984)
Probabilistic Risk Assessment, Merits and Limitations. 5th International Meeting on Thermal Nuclear Safety, Karlsruhe, Federal Republic of Germany, September 10-13, 1984.

Mankamo, T., Petersen, K.E., Pörn, K. and Ericsson, G., (1985)
Experiences from the Nordic Benchmark Analyses. International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, U.S.A., February 24 -March 1, 1985.

Pulkkinen, U. (1985)
Experiences from a Benchmark Study on Reliability Modelling and Computer Codes. Scandinavian Reliability Engineers Symposium, Trondheim, Norway, September 30 - October 2, 1985.

Pulkkinen, U., ed. (1987)
Proceedings of the CCF Workshop, Lepolampi, Espoo, Finland, May 10-11, 1984. Report RAS-470(87)14 (VTT Work Report SÄH 38/37), December 1987.

Pulkkinen, U., Huovinen, T. and Kuhakoski, K. (1987)
Combination of Several Data Sources. PSA '87 - International SNS/ENS/ANS Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Pulkkinen, U. and Pörn, K. (1990)
Uncertainty in Safety Analyses and Safety Related Decision Making. Report RAS-470(89)12, to be published 1990.

Pulkkinen, U. and Simola, K. (1987)
A Retrospective Analysis of Dependencies in Five Selected PRAs. Report RAS-470(87)9 (VTT Report SÄH 35/87), December 1987.

Pyy, P. and Pulkkinen, U. (1988)
Human Reliability in Probabilistic Risk Assessment. A Retrospective Study. Report RAS-470(87)10 (VTT Research Notes 908), November 1988.

Simola, K., Pulkkinen, U. and Huovinen, T. (1988)
Treatment of Time Dependent Phenomena in PSA. Report RAS-470(87) 15 (VTT Work Report SÄH 13/88), October 1988.

2. STUDIES OF DEPENDENCIES

2.1 Overview

Studies of dependencies carried out within the RAS-470 project comprise Common Cause Failure Data Benchmark Exercises (Hirschberg, ed., 1987 and Hirschberg et al., 1987), retrospective qualitative analyses of treatment of dependencies in Swedish (Hirschberg, 1987 and Hirschberg and Bengtz, 1987) and foreign PSAs (Pulkkinen and Simola, 1987). The Nordic perspective on this subject has been summarized in (Hirschberg, 1989). In addition, retrospective sensitivity studies of CCFs in Swedish PSAs have been performed. This task will be covered separately in chapter 4 of the present report, which specifically addresses uncertainty aspects.

2.2 Nordic Common Cause Failure Data Benchmark Exercise

Following the recommendation of a pre-project (Hirschberg, 1985b), carried out in the spring of 1985, it was decided that during the initial phase the RAS-470 project will concentrate on a Benchmark Exercise (BE) concerning CCF-data, thus addressing one of the most uncertain issues in current level 1 PSAs. The exercise shows some similarities with a parallel CCF Reliability Benchmark Exercise coordinated by Ispra Establishment (Poucet et al., 1987). However, the Nordic BE concentrated on the data problem and did not concern system modeling issues. It was felt that by choosing this approach the efforts will be directly focused on the weakest link of CCF-analysis.

2.2.1 Organization and time schedule of the Benchmark Exercise

The main steps in the exercise were:

1) Collection of relevant background material, i.e. a set of failure events for the particular component type analysed.

2) Stipulation of common rules concerning identification of CCFs and formulation of general directives for the estimation of CCF-contributions.

3) Practical carrying out of the exercise including study of related problems; this step consists of two phases, identification and quantification.

Table 2.1 shows the project schedule of the Benchmark Exercise.

Table 2.1

Project schedule of the Benchmark Exercise

Task	Person-months	1985						1986											
		7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
Collection & preparation of background material	1.5	———																	
Stipulation of common rules for BE	0.5	———																	
CCF-identification	6.0	———	———	———	———	———	———	———	———	———									
CCF-classification	1.5							———	———	———									
CCF-quantification incl. uncertainty and sensitivity analysis	8.0									———	———	———	———	———					
Final report	3.0													———	———	———	———	———	———
Project coordination	1.5	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———
Meetings, administration	3.0	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———	———
Person-months, total	25.0																		

2.2.2 Identification of common cause failure events

Identification of CCFs which have occurred during the operation of the plants constitutes the central task of the Benchmark, and is necessary as a starting point for analysis of related problems, i.e. classification and estimation of CCF-contributions with associated uncertainties.

2.2.2.1 Problem description and background material

Motor-operated valves (MOVs) in Swedish Boiling Water Reactor (BWR) plants were chosen as the object of the CCF-data Benchmark Exercise (BE).

ABB Atom supplied the four groups participating in the BE with a common set of failure events involving MOVs from seven Swedish BWRs. The database comprised 340 failure reports from the Scandinavian Nuclear Power Reliability Data system (ATV-system; Ekberg et al., 1985) and two Swedish Licensee Event Reports (LERs). The following time periods have been covered:

Barsebäck 1	771001--821231
Barsebäck 2	790101--821231
Forsmark 1	810101--821231
Forsmark 2	810701--821231
Oskarshamn 1	740101--821231
Oskarshamn 2	760101--821231
Ringhals 1	761001--821231

Additional information collected by ATOM and distributed to all working teams included (Björe and Hirschberg, 1985):

- a list of all MOVs covered by failure reports, including operation times, test intervals, number of activations and number of critical failures during commercial operations
- a list of all overhaul periods
- failure codes used in the ATV-system
- flowsheets of relevant systems.

2.2.2.2 Basic principles, boundary conditions and limitations

In the initial phase of the project several suggestions were made concerning specification of the features which are required as basic characteristics of a CCF. For the purpose of the exercise it seemed sufficient to point out such features in general sense, rather than trying to formulate a strict definition. The proposed frame for the identification procedure (Hirschberg, 1985c; supplemented in Vaurio, 1985), involved the following elements:

1) Only multiple failures (actual or potential) are of interest.
2) It should be possible to point out one or several common causes as a source of each CCF.

3) Critical time period is of great importance when dependencies are considered. Failure of identical components can be manifested directly when the failure occurs or a long time after the occurrence.

4) Cascade failures and other dependencies which originate from basic design principles (e.g. functional dependencies related to power supply, signal exchange or to other explicitly modeled auxiliary systems), are not regarded as CCFs in this study.

5) Many failures are not manifested as multiple, since measures are taken before they occur. In some cases the failure event has such a character that even if only a single failure has actually occurred, the same failure mechanism with the same cause may be detected in other units. Furthermore, seemingly independent multiple failures which occur close in time cannot a priori be regarded as fully independent. One way to model such failures is to include them in the group of potential (opposite to actual) CCFs (Fleming et al., 1985). This category can even include components in degraded condition whenever they occur in conjunction with actual failures in a dependent fashion.

6) The aim of the work is to identify all relevant CCF-events in the supplied material, which involve identical components within each plant. Consequently, the analysis is not a priori limited to redundant components within single systems. It is, however, expected that the evidence of CCFs involving identical components within different systems (intercomponent -intersystem CCFs) will be rather weak.

In addition several boundary conditions and limitations associated with the identification procedure were suggested (Hirschberg, 1985c), and the following guidelines were accepted:

1) For physical boundaries of the components the definition given in the Reliability (T-) Data Book (Bento et al., 1985), should be used.

2) Only critical failures should be classified as actual CCFs. Determination of what is a critical failure is to be performed independently by each institute using own judgement, ATV's original classification and ATOM's classification which constitutes the basis of the T-book.

3) Among potential CCFs the combinations involving non-critical failures may be found. The interest should be focused on cases with combinations of e.g. a critical and a non-critical failure or violations of Technical Specifications. Combinations of non-critical failures discovered during the overhaul period are less serious.

Due to a rather general formulation of the guidelines, specific differences were identified in the actual interpretations of the CCF-definition and in applications of boundary conditions. The observed deviations concern:

- treatment of intersystem CCFs
- treatment of multiple failure events including non-redundant components
- length of critical time period

- failure criticality
- definition of potential CCFs
- treatment of failures reported during the overhaul period
- treatment of different failure modes.

Several of these problematic issues were resolved by common agreement but some were not resolved due to differences in scope or judgement. Treatment of multiple failure events detected during the overhaul period proved to be one of the most controversial and unresolved issues in the Benchmark Exercise. While three of the groups treated such CCFs in the same way as failures detected during operation, the fourth group (ATOM) considered them as potential CCFs.

Since this methodological decision has a significant impact on the quantitative results, the quoted reasons for the separate treatment of CCF-candidates detected during the overhaul period, are given below.

Nine such cases were identified by ATOM; seven of them concern internal leakages. The transfer of these failures to the category of potential CCFs was motivated by the group using the arguments of the Reliability (T-) Data Book:

"Specifications for leakages on containment isolation valves are very strict and therefore leakages reported very seldom are significant in a risk analysis. In respect of open/close operations the valves often have sufficient function but they do not meet with the Technical Specifications for leakages".

Additional quoted motives for making a distinction between operational and overhaul periods are low degree of reporting coverage during overhaul and significant potential that these CCF-candidates have been actually initiated by the activities during the overhaul.

It was anticipated that the major limitation of the identification procedure is due to incompleteness of the failure reports. Consequently, subjective judgement must be used, which may result in different interpretations of the same source of information.

2.2.2.3 Approach to identification

The analyses performed by each of the groups are covered in separate reports (Bengtz et al., 1986; Dinsmore, 1986; Kongsø et al., 1986; Pulkkinen and Järvinen, 1986a).

The working procedure chosen by ATOM (Bengtz et al., 1986) was divided into three steps:

1) Preliminary selection of CCF-candidates
2) Screening
3) Final judgement.

During the screening phase the preliminary CCF-candidates were divided into four groups: actual CCFs, potential CCFs, notable cases and excluded cases. Final decision concerning each set of failure events was made on case by case basis with due consideraton of such factors as: time of detection (degree of simultaneity), type of failures (critical/non-critical), failure modes, failure causes, measures taken, design features. The search for CCFs was performed manually.

RISØ (Kongsø et al., 1986) used the coding specifying failure causes and failure modes as the primary indication of possible dependency. Unfortunately, the coding of failure causes is incomplete and in some cases the correctness of the coding is questionable. However, the supplementary search based on failure mode codification showed to be more adequate. Final choice of CCF-candidates was also based on scrutinizing of texts describing failure events, use of information concerning failure criticality and times of failure detection. Both searches were made on an IBM PC computer.

It was found beneficial to use computer support in the screening process. It saves time and manpower, and is rather efficient. However, it must be emphasized that both failure mode codification and information on time of failure detection and test interval should be used as the basis of screening. Furthermore, it is always necessary to supplement the screening process by engineering judgement using other information sources.

STUDSVIK's analysis (Dinsmore, 1986) was limited to redundant components within single systems. After defining redundancy and identifying the redundant valve groups from the system diagrams, all reported failures for each group were arranged in chronological order. Similar or identical failure reports within a one month interval were collected. Each collected set of reports was reviewed and the failures judged as non-critical (primarily position indication failures and external leakage) were removed.

VTT (Pulkkinen and Järvinen, 1986a) used the time span between failures as a primary factor for identification. Failures within one month were further investigated with consideration given to both the failure mode, cause and criticality. Potential dependencies between different systems were not considered. Taking one system at a time all failures were plotted on a time line which considerably facilitated the identification procedure.

Table 2.2 summarizes the main features of each groups approach.

2.2.2.4 Results of identification

The final results of identification are summarized in Table 2.3. Since only two of the groups looked for intersystem CCFs, the list is limited to those CCFs which were found within individual systems. The evidence of CCFs involving identical components within different systems is anyhow rather weak; potential CCFs have been identified on a rather speculative basis. Note that three of the groups use the term "CCF-candidate", while the fourth group classifies the CCF-candidates as either potential or actual CCFs.

Generally, all supplementary information which could be obtained through direct contacts with plant personnel, would be beneficial for the quality of the identification procedure. In one doubtful case, an in-depth analysis has been perfomed (Forsmark 2, 323 V204 and 323 V214, October 21, 1981). Additional information has been obtained through direct contacts with plant personnel, which definitely facilitated judgement of these failures.

Internal leakages, torque-switch problems and seizures are the dominating failure modes associated with identified CCFs. One of the actual CCFs was caused by wrong connections after a test. There are no statistically significant trends in identified CCFs. However, a certain dominance of internal leakages at Barsebäck 1 and at Forsmark 1, has been observed.

Table 2.2

Characteristic features of analyses performed (identification phase)

Feature	Group			
	ATOM	RISØ	STUDSVIK	VTT
SCOPE				
intersystem dependencies	Yes	Yes	No	No
limited to redundancies	No	No	Yes	No
LERs considered	Yes	No[a]	No[a]	No[a]
MAIN IDENTIFICATION FACTORS				
critical time period	Yes[b]	Yes[b]	Yes[c]	Yes[c]
failure cause(s)	Yes	Yes	Yes	Yes
failure mode	Yes	Yes	Yes	Yes
BOUNDING CONDITIONS				
separate treatment of overhaul periods	Yes	No	No	No
acceptance of failure criticality according to the Reliability Data Book (Bento et al., 1985)	Yes	Yes	No	Yes[d]
distinction between potential and actual CCFs	Yes[e]	Yes[e]	Yes[e]	No
APPROACH				
computerized analysis	No	Yes	No	No

[a]Unintentionally left out
[b]One test interval
[c]One month
[d]With minor exceptions
[e]Different definitions of potential CCFs

Table 2.3
Identified multiple failure events

Event No	Plant	Compo-nents	Date	Comm-ents*	Event descrip-tion	Status ATOM	RISØ	STUDSVIK	VTT
1	Barsebäck 1	311V50	800904	r,R,FH	Internal	potential	CCF-	CCF	CCF-
	"	311V60	800904	r,R,FH	leakages	CCF	candidate	candidate	candidate
2	Barsebäck 1	721V25	800930	r,R,FH	Internal	potential	CCF-	CCF-	CCF-
	"	721V26	800918	r,R,FH	leakages	CCF	candidate	candidate	candidate
3	Barsebäck 2	322V1	810907	r,-R,FH	Wrong connec-	actual	not	not	not
	"	322V2	810907	r,-R,FH	tions	CCF	identified	identified	identified
	"	322V3	810907	r,-R,FH					
4	Barsebäck 2	311V50	800702	r,R,-FH	Sticking	notable	potential	CCF-	not
	"	311V60	800702	r,R,-FH	valves	case	CCF	candidate	identified
	"	311V70	800702	r,R,-FH					
	"	311V80	800702	r,R,-FH					
5	Forsmark 1	321V33	810627	r,R,FH	Internal	potential	not	CCF-	CCF-
	"	321V34	810718	r,R,FH	leakages	CCF	identified	candidate	candidate
6	Forsmark 1	323V201	820709	nr,R,FH	Internal	potential	potential	not	not
	"	323V214	820709	nr,R,FH	leakages	CCF	CCF	identified	identified
7	Forsmark 1	321V33	820701	r,R,FH	Int.leakage	excluded	potential	CCF-	not
	"	321V34	820816	r,R,-FH	Ext. "	case	CCF	candidate	identified
8	Forsmark 2	323V204	811021	nr,-R,-FH	Incorr.torque-	potential	potential	not	not
	"	323V214	811021	nr,-R,FH	switch settings	CCF	CCF	identified	identified
9	Forsmark 2	322V401	820510	nr,R,FH	Internal	excluded	potential	not	CCF-
	"	322V305	820511	nr,R,FH	leakages	case	CCF	identified	candidate
10	Oskarshamn 1	322V1	771116	r,-R,FH	Incorr.torque-	actual	CCF-	CCF	not
	"	322V20	771116	r,-R,FH	switch settings	CCF	candidate	candidate	identified
11	Oskarshamn 1	322V1	790518	nr,R,-FH	Sticking	potential	CCF-	not	CCF-
	"	322V7	790522	nr,R,FH	valves	CCF	candidate	identified	candidate
12	Oskarshamn 1	721V27	741210	r,R,-FH	No information	excluded	CCF-	CCF-	not
	"	721V28	741210	r,R,-FH	available	case	candidate	candidate	identified
13	Oskarshamn 2	321V2	810723	nr,R,FH	Internal	potential	potential	not	not
	"	321V32	810730	nr,R,FH	leakages	CCF	CCF	identified	identified
14	Oskarshamn 2	323V3	780628	nr,R,FH	Internal	potential	CCF-	not	not
	"	323V15	780714	nr,R,FH	leakages	CCF	candidate	identified	identified
15	Oskarshamn 2	721V25	770707	r,R,FH	Sticking	potential	CCF-	CCF-	CCF-
	"	721V26	770703	r,R,FH	valves	CCF	candidate	candidate	candidate
16	Ringhals 1	323V3	811105	r,R,-FH	External	notable	CCF-	CCF-	not
	"	323V4	811105	r,R,-FH	leakages	case	candidate	candidate	identified
17	Ringhals 1	322V7	791028	r,-R,FH	Incorr.torque	not	not	not	CCF-
	"	322V8	791028	r,-R,FH	switch settings	identified	identified	identified	candidate

* r = redundant components -R = normal operation
nr = non-redundant components FH = critical failures
R = overhaul period -FH = non-critical failures

Excluding the differences in scope and neglecting the differences in definitions, 9 of the 11 events involving redundant valves were identified by at least three of the groups. The two remaining events were identified by one institute each; the background to these events is an organization misunderstanding and a very complicated failure report, respectively. The result is considered encouraging and indicates that basic identification can be resonably performed with the available raw data.

On the other hand, including the differences in what each event is defined to be, produces much worse agreement and the very process of comparing the different definitions is essentially impossible. Thus, the requirement of clear and concise definition is supported by the study. Interpretation of subsequent work must then be done in light of these definitions.

Bearing in mind the complexity of the identification procedure and the significant importance of subjective judgement as a part of the process, the results of the analyses performed indicate that some consistency is possible. The majority of observed discrepancies may be explained by differences in scope, bounding conditions and type of approach (see Table 2.2).

2.2.2.5 Use of classification systems

Recently, several systems for classification of dependent events have been developed (Fleming et al., 1985; Los Alamos Technical Associates Inc., 1984 and 1985). The use of such systems has been recommended in these reports. Two of the groups applied them to identified CCF-events in order to investigate the possible merits and drawbacks of classification systems. Some of the central questions in this context are:

- Do they (classification systems) facilitate transfer of information between PRA-analysts?
- Do they promote better understanding of dependencies?
- Do they simplify the search for dependencies?
- Do they make it possible to supplement the Nordic experience with events from U.S. plants when estimating plant-specific CCF-parameters?
- Do they facilitate specification of defensive measures?

In five cases (all design inadequacies; events no. 1, 2, 5, 6, 13) there was a total agreement between the classifications performed by ATOM (Bengtz et al., 1986) and VTT (Pulkkinen and Järvinen, 1986b), while differences have been observed in six cases (events no. 3, 8, 10, 11, 14, 15). Table 2.4 shows examples of results of classification for cases analysed by ATOM and VTT; for explanation of symbols and codes for cause categories, used in the cause-effect diagrams, we refer to (Fleming et al., 1985).

The discrepancies illustrate the differences in postulating the course of the events and the fact that different interpretations of incomplete failure reports are frequently made.

Based on the experience from the performed classifications following conclusions were drawn:

1) Classification systems are in the first place intended for structuring and breaking down complex event descriptions. U.S. Licensee Event Reports (LERs) frequently contain this type of information and in many cases situations with several components involved, are described. On the other hand, ATV-reports concern specific components. Thus classification systems are much more effective as a tool for analysis, in the case of U.S.-failure reports.

2) Classification systems are cause-oriented. ATV-reports supply in the first place information about failure modes. When specifying the nature of the cause the analyst must rely on his judgement; in many cases guesses are inevitable.

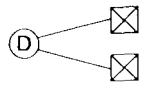
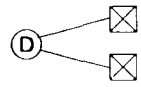
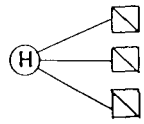
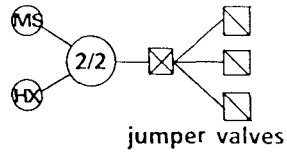
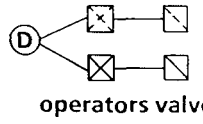
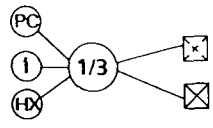
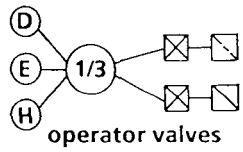
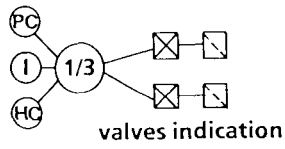
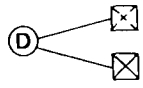
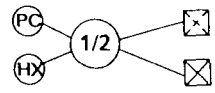
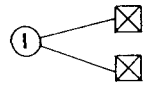
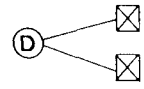
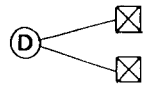
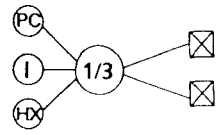
3) Classification systems may facilitate CCF-identification in some doubtful cases. In the first place the diagrams provide the possibilities to present the results in a systematic way and supply a good framework for exchanging information and experiences between analysts.

2.2.3 Quantification of common cause failure contributions

The individual contributions to the quantification phase of the exercise are described in separate reports (Bengtz and Hirschberg, 1986; Dinsmore and Pörn, 1986; Kongsø and Petersen, 1986; Pulkkinen et al., 1986).

Table 2.4

Examples of cause-effect diagrams for CCFs identified in Nordic CCF-data Benchmark Exercise

CCF no.	Cause-effect diagrams	
	ABB Atom	VTT
1		
3		
8		
10		
11		
14		
15		

2.2.3.1 Methods for CCF-quantification

In the previous major Nordic research project (NKA/SÄK-1), concerned with development of PRA-techniques, substantial effort has been directed towards improving the models for CCF-quantification (Dinsmore, ed., 1985). Significant improvements were made which consistently take into account the high level of redundancy and diversity typical for safety systems in the newer Nordic nuclear power plants.

A recent workshop was dedicated to a thorough study of methods for quantitative CCF-analysis (Pulkkinen, ed., 1987). Certain inconsistencies have been discovered in models used in some studies in the U.S.A. (Hirschberg, 1985a and Mankamo, 1985). However, a common feature of the applications of higher-order models in the analyses presented at and following the above mentioned workshop is use of simulated (idealized) set of data. On the other hand, the search of optimal methods for estimation of CCF-contributions should be compatible with the information which can be extracted from available databases. For this reason, despite the uncertainties and difficulties (the collected material is rather poor from the statistical point of view), it is more interesting to confront the reality experienced by PRA-analysts. This has been done in the quantification phase of the Benchmark Exercise.

The PSAs performed in Sweden during the last few years have all used parametric models with single failure probability as a basic parameter for quantification of CCF-contributions. Four high-order methods are of particular interest. Multiple Greek Letter (MGL) method (Fleming and Kalinowski, 1983) gave most promising results in the comparative evaluation based on a simulated database (Hirschberg, 1985a), and has been applied in five of the recent Swedish PSAs. The Binomial Failure Rate (BFR) model has been the subject of continuous improvements (Atwood, 1980 and Atwood, 1983c). BFR-method was used for detailed data analysis concerning diesel generators (Steverson and Atwood, 1982), pumps (Atwood, 1983a), valves (Steverson and Atwood, 1983), and instrumentation and control assemblies (Atwood, 1983b). In addition, Additive Dependence (ADDEP) model (Mankamo and Pulkkinen, 1985) has been developed in Finland. Recently, it has been shown in (Apostolakis and Moieni, 1986) that in special conditions (no observed failures of high multiplicity), the MGL method underestimates the

CCF-contributions. More generally, in another paper (Apostolakis and Moieni, 1987) the same authors point out the fact that the MGL-parameters are used improperly in statistical calculations and that the component-related definition of these parameters results in an artificial information increase of the statistical evidence. They proposed an alternative method, called Multinomial Failure Rate (MFR) model. The alpha-factor model (Mosleh and Siu, 1987) was developed after the completion of the Nordic Benchmark Exercise on CCF-data. Comparison of the alpha-factor model (Mosleh and Siu, 1987) with MGL-method (Fleming and Kalinowski, 1983) will be described in chapter 4.

No systematic comparison of the methods mentioned above, when applied to four unit systems, has been performed earlier. Of high interest is also a comparison with direct assessment, if such could be performed using supplied data.

Furthermore, the descriptions of the models, given in reference reports, supply only a frame containing a set of basic equations. In practical applications, especially these concerning four train systems, some extensions based on engineering judgement are necessary. These aspects have been illustrated in the Benchmark Exercise.

2.2.3.2 Common data base and principles for CCF-quantification

Based on the results from the identification phase, the list of CCFs given in Table 2.3, has been chosen as the starting point for the quantification phase. Following main principles for quantification were formulated (Hirschberg, 1986):

1) CCF-contributions are to be estimated for four redundant motor operated valves (diameter 150 mm) in a safety system (e.g. emergency core cooling) at Forsmark 1.

2) All failure multiplicities should be considered. The results should be given as P_i (i=2,3,4), i.e. probability of observing exactly i failures at a test or at a demand.

3) The associated uncertainties should be estimated.

4) The common data base, given in Table 2.3, is to be used as a starting point for the quantification. However, it is up to each analyst to decide

which of the events are relevant for the present application. All assumptions should be specified and reasons for exclusion of certain events should be thoroughly motivated.

5) In the common data base CCF-events involving non-redundant components belonging to the same system, are included. Each group must decide about the applicability of this type of data to the present case.

6) Each group is free to choose anyone of the available methods for CCF-quantification. Hopefully, each of the teams will try at least two different approaches.

7) The redundant trains in Forsmark 1 (and in Forsmark 2) are strictly separated. Corresponding information about valves from other plants involved in CCF-events given in Table 2.3, is not available. Collection of this type of information would be time consuming and is not motivated for the sake of the Benchmark Exercise. In practice, a "walk-through" analysis would be needed. Most of the identified failure modes are probably not affected by separation. Whenever necessary it should be assumed that the degree of separation in older plants is generally lower than in Forsmark 1; in many cases there is no separation at all (e.g. 721V25, 721V26 in Barsebäck 1&2, and in Oskarshamn 2).

8) Due to general design principles and formulation of procedures for testing and for maintenance, the probability of systematic wrong connections in Forsmark 1, may be regarded as extremely low.

As an additional information a short description of principles governing test performance at different plants, has been given (Hirschberg, 1986).

2.2.3.3 Screening

Two types of screening have been employed:

- exclusion of "non-CCF" events
- design- and application-oriented screening.

All groups made some changes in their "identified" CCFs (Table 2.3) indicating that none of the initial search techniques produced an all inclusive set.

Table 2.5 summarizes which multiple failure events have been excluded by different groups with reference to "non-CCF" nature of these events. The reason for exclusion is either non-criticality or different types of failures in question. The numbers given in Table 2.5 correspond to numbers assigned to multiple failure events in Table 2.3.

Table 2.5
Excluded "non-CCF" events

Group	Event no.
ATOM	4,7,12,16
RISØ	4,7,16
STUDSVIK	7
VTT	4,7,12,16

In addition, the events involving non-redundant valves (events 6, 8, 9, 11, 13, 14) were excluded by RISØ and STUDSVIK and in some cases (model-dependent) by ATOM and VTT.

Design-oriented screening has been used only by one of the groups (ATOM). Other analysing teams felt it was not possible to perform any type of "data pruning" to remove events not applicable to Forsmark 1 from the common data base, considering that information available within the Benchmark Exercise was not sufficient. As a result of this type of screening, event 3 was excluded in ATOM's analysis (Bengtz and Hirschberg, 1986), which was motivated by extremely low probability of systematic wrong connections at Forsmark 1. A more general concern was raised by one of the groups that the a priori removal of failure events when analysing new designs should be done with great caution. The process is complicated by the substantial uncertainties in determining the cause of observed CCFs.

Since the identified CCFs originate mainly from plants with lower level of redundancy than Forsmark 1, it must be decided on a case by case basis if three or four valves (if present) would have been affected by the shock in question. This may lead to extension of some of the observed failures to higher multiplicity. This type of data modifications was performed in some cases by ATOM (Bengtz and Hirschberg, 1986), RISØ (Kongsø and Petersen, 1986) and STUDSVIK (Dinsmore and Pörn, 1986). According to VTT's opinion such extensions are of Bayesian nature and should be included in prior distributions, which cannot be done completely by using available methods.

2.2.3.4 Approach to quantification

ATOM used MGL-, BFR- and MFR-methods. Following cases were considered:

1) MGL-method
   - only CCFs involving redundant components included ($MGL_{AA}I$)
   - all CCFs included ($MGL_{AA}II$)
2) BFR-method
   - potential CCFs weighted using $w_{p=}$ 0.1 ($BFR_{AA}I$)
   - no weighting ($BFR_{AA}II$)
3) MFR-method
   - due to the available formulation of the method only P_4 has been estimated (MFR_{AA}).

RISØ (Kongsø and Petersen, 1986) analysed three cases (best, optimistic and pessimistic estimate, depending on choice of impact vectors for failure extension) using the MGL-method. The cases are denoted by MGL_RI, MGL_RII and MGL_RIII, respectively. These cases have been chosen to show the sensitivity of the results to differences in data extensions which are based on judgement. RISØ would generally prefer direct assessment whenever possible, but found such approach very difficult in the actual case due to lack of information. Also the BFR-method was studied by RISØ, but this model was found to be too sensitive to assumptions.

STUDSVIK (Dinsmore and Pörn, 1986) chose the direct assessment employing the Bayesian method based on a noninformative (Dirichlet) prior distribution for the unknown probabilities. The probability of CCFs is estimated using this prior distribution combined with a multinomial likelihood consisting of the number of observed CCFs and the number of opportunities. This requires an estimate of the number of times each group of redundant valves was tested.

The process leading to determination of these numbers was time consuming but not particularly difficult, given the comprehensive list of valve actuations. Two cases were studied by STUDSVIK, one with both potential failures and extension (DA_SI) and one using only observed failures (DA_SII).

VTT (Pulkkinen et al., 1986) used following approaches:

1) ADDEP-model ($ADDEP_V$)

2) BFR-model (without any identification of nonlethal shocks)
   - without lethal shocks (BFR_VI)
   - with lethal shocks (BFR_VII)

3) Direct (Bayesian) estimations; with noninformative prior distribution using only data from Forsmark 1 (DA_VI), and with informative prior based on the evidence from other plants (DA_VII).

Internal leakage failures were separated from failures with other modes in the VTT analysis. The VTT-group identified the redundant valves. This was based on the position of the valves in the system and on the number and dates (if available) of demands. Also the number of "simultaneous" demands of redundant valves was necessary for parameter estimation and for the assessment of uncertainty intervals (in ADDEP- and DA_V-cases). The VTT-group used both the method of maximum likelihood and Bayesian method in parameter estimation.

Both STUDSVIK (Dinsmore and Pörn, 1986) and VTT (Pulkkinen et al., 1986) showed by performing simple statistical tests that there exists significant statistical evidence of dependency between redundant valves.

Table 2.6 summarizes the main differences and similarities between the analyses performed by different groups. The methods used in the analyses are described and commented from mathematical point of view in (Pörn, 1989).

2.2.3.5 Results of quantification

Results of the analyses performed are summarized in Table 2.7; only the most representative cases are covered by the table.

For comparison also the independent failure contributions obtained by VTT, are presented in the last line of Table 2.7. The calculated independent failure probabilities are based on the total number of component demands according to the VTT-analysis. Comparison of the numerical values obtained in this case with other results clearly demonstrates the impact of CCF-contributions on multiple failure probabilities.

Table 2.6

Differences and similarities between quantative analyses

Group	Method	Excluded "non-CCF" events (out of 17)	Exclusion of non-redundant valve events	Design-oriented screening	Extension	Weighting of potential CCFs
ATOM	$MGL_{AA}I$	4	Yes	Yes	Yes	Yes[a]
	$MGL_{AA}II$	4	No	Yes	Yes	Yes[a]
	$BFR_{AA}I$	4	No	Yes	No	Yes[a]
	$BFR_{AA}II$	4	No	Yes	No	No
	MFR_{AA}	4	Yes	Yes	Yes	Yes[a]
RISØ	$MGL_{R}I$	3	Yes	No	Yes[c]	No
	$MGL_{R}II$	3	Yes	No	Yes[c]	No
	$MGL_{R}III$	3	Yes	No	Yes[c]	No
STUDSVIK	$DA_{S}I$	1	Yes	No	Yes	Yes[a]
	$DA_{S}II$	1	Yes	No	No	No
VTT[b]	$ADDEP_{V}$	4	Yes	No	No	No
	$BFR_{V}I$	4	Yes	No	No	No
	$BFR_{V}II$	4	No	No	No	No
	$DA_{V}I$	4	Yes	No	No	No
	$DA_{V}II$	4	Yes	No	Yes[d]	No

[a]Weighting factor $w_p = 0.1$
[b]Internal leakages treated separately
[c]Different impact vectors
[d]Concerns number of demands

Table 2.7

Estimated probabilities of observing exactly i (i=2,3,4) failures per demand

Method	P_2	P_3	P_4
$MGL_{AA}I$	$8.7 \cdot 10^{-4}$	$1.2 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$
$MGL_{R}I$	$1.3 \cdot 10^{-3}$	$4.5 \cdot 10^{-4}$	$4.4 \cdot 10^{-4}$
$DA_{S}I$	$1.2 \cdot 10^{-3}$	$5.2 \cdot 10^{-4}$	$8.1 \cdot 10^{-4}$
$DA_{V}II$	$1.1 \cdot 10^{-3}$	$3.1 \cdot 10^{-4}$	$1.0 \cdot 10^{-4}$
MFR_{AA}	-	-	$2.3 \cdot 10^{-4}$
$ADDEP_{V}$	$1.1 \cdot 10^{-3}$	$8.3 \cdot 10^{-4}$	$9.4 \cdot 10^{-6}$
$BFR_{AA}II$	$5.8 \cdot 10^{-3}$	$5.2 \cdot 10^{-4}$	$1.9 \cdot 10^{-5}$
$BFR_{V}I$	$6.7 \cdot 10^{-3}$	$3.2 \cdot 10^{-4}$	$6.9 \cdot 10^{-6}$
INDEP	$6.5 \cdot 10^{-4}$	$4.6 \cdot 10^{-6}$	$1.2 \cdot 10^{-8}$

The differences between the methods increase with growing failure multiplicity, but with exception of BFR- and ADDEP-estimates of P_3 and P_4, are not dramatic.

2.2.3.6 Uncertainty and sensitivity analysis

Uncertainty analysis was performed by ATOM (Bengtz and Hirschberg, 1986), STUDSVIK (Dinsmore and Pörn, 1986) and VTT (Pulkkinen et al., 1986).

ATOM quantified uncertainties in the estimation of parameters of the MGL-method, using the beta-distribution. Figure 2.1 shows the simulated cumulative distributions of the CCF-parameters for the $MGL_{AA}I$-case. In order to obtain the simulated confidence intervals for the BFR-cases, parameters of this method were assumed to be gamma-distributed (with exception of p, the probability of failure for each unit given a nonlethal shock, which was treated as a constant). The intervals for P_i (i=2,3,4) were obtained by using lower and upper bounds of all parameters; this approach is conservative.

STUDSVIK (Dinsmore and Pörn, 1986) used a multidimensional beta-distribution (Dirichlet) as the noninformative prior. This prior was combined with a multinomial likelihood function leading to a posterior distribution of the same kind as the prior. The confidence bounds were calculated using the corresponding marginal (onedimensional) beta-distributions.

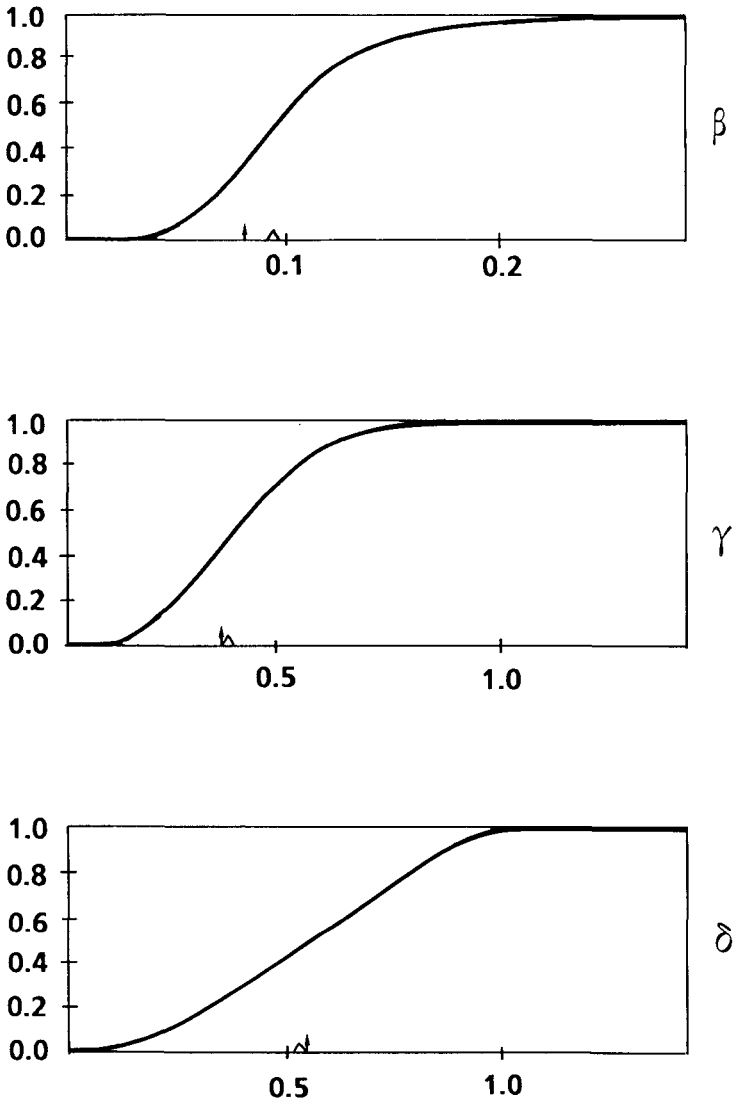


Figure 2.1
Simulated cumulative distributions of CCF-parameters ($MGL_{AA}I$)

VTT (Pulkkinen et al., 1986) applied both Bayesian and classical statistical methods in determining the uncertainties of CCF probabilities and model parameters. The classical methods were applied to BFR- and ADDEP-models to yield the variances of model parameters. The results concerning the BFR-model were not presented, because approximations and assumptions used led to incorrect values of variances. The confidence bounds for ADDEP-parameters were calculated using normal distribution approximation. The Bayesian methods were used in direct estimation of multiple failure parameters. The Dirichlet-prior distribution and its beta-marginal distribution approximation were applied and the final confidence bounds were obtained with Monte Carlo simulation. Figure 2.2 shows the Bayesian posterior distributions of multiple failure probabilities obtained for the case with informative prior, based on the data from all plants.

Figure 2.3 shows the probabilities of observing exactly i (i=2,3,4) failures per demand and corresponding 90% confidence intervals, as estimated by different groups. Confidence intervals in the $MGL_{AA}I$ case do not take into account the uncertainty in the single failure probability.

Sensitivity analyses were performed with respect to:

- assumptions and parameters of the BFR-model
- variation of weighting factors
- number of system actuations
- characteristic features of different approaches (see Table 2.6).

Figure 2.4 (Bengtz and Hirschberg, 1986) shows the results obtained using the BFR-method and different times between demands. The variation is substantial, although it should be remembered that extreme values of test interval length were used in $BFR_{AA}III$ and $BFR_{AA}IV$. In a similar way the sensitivity of the BFR-method to the assigned number of non-lethal shocks has been demonstrated (Bengtz and Hirschberg, 1986). Using the MGL-method multiple failure probabilities are increased by a factor of about 2 when increasing the weighting factor for potential CCFs from 0.1 to 1.0 (Bengtz and Hirschberg, 1986).

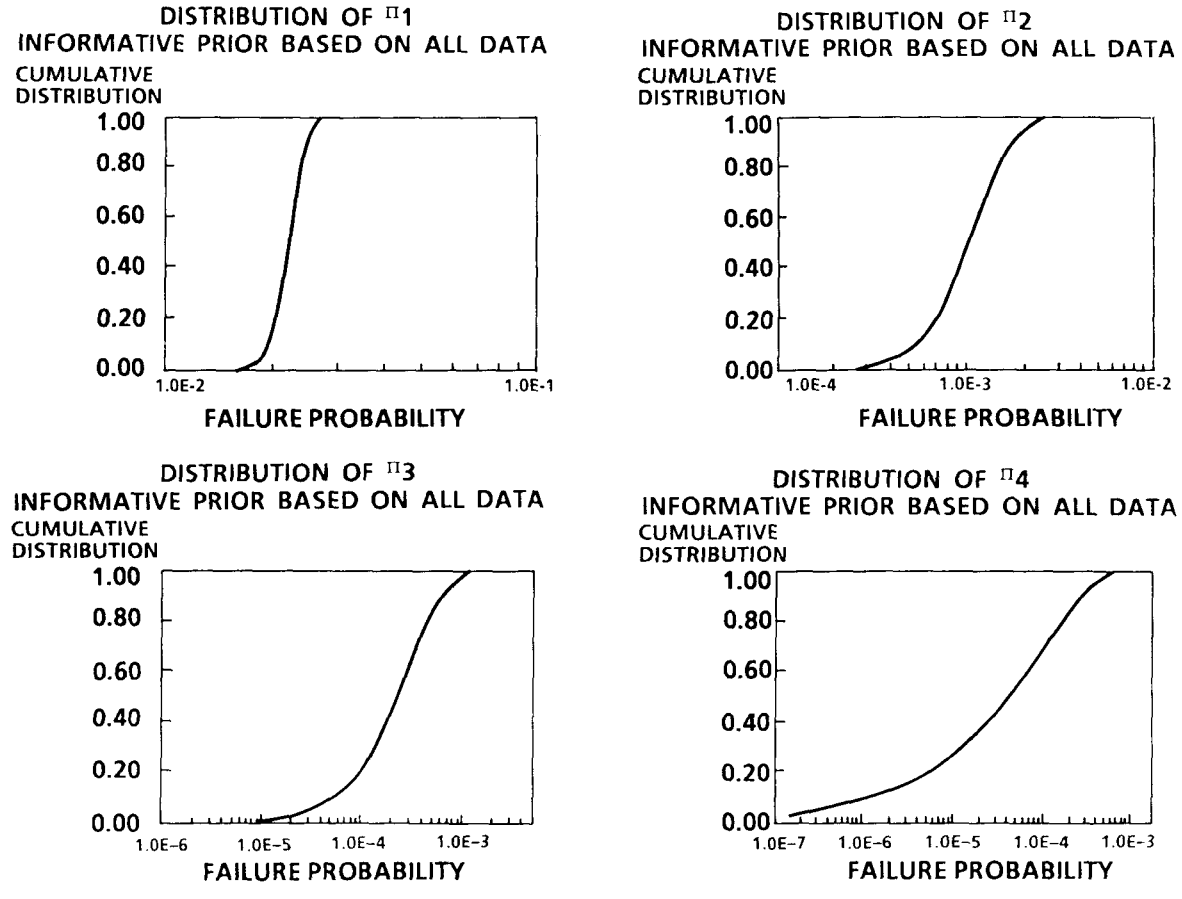


Figure 2.2

Bayesian posterior distributions of multiple failure probabilities
(informative prior based on data from all plants)

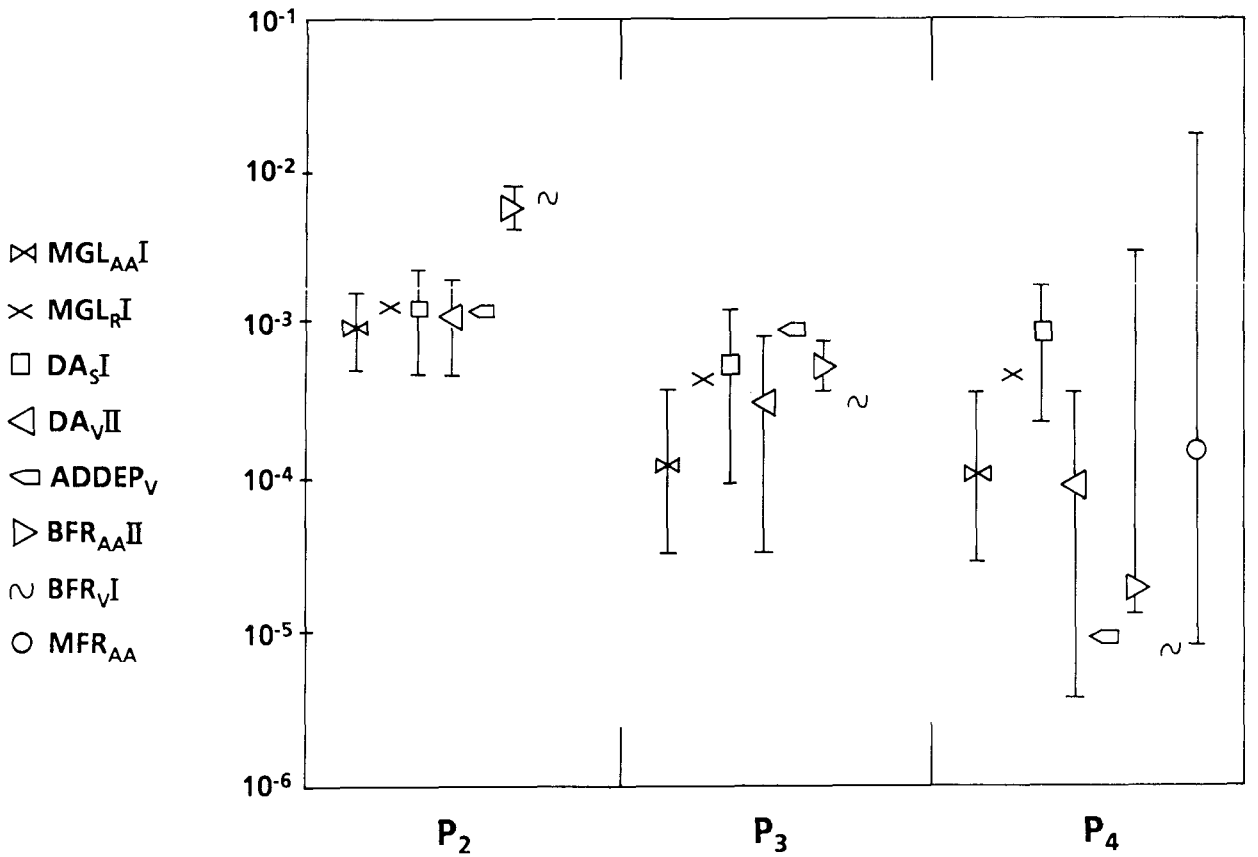


Figure 2.3

Estimated probabilites of observing exactly i (i=2,3,4) failures per demand and corresponding 90% confidence intervals

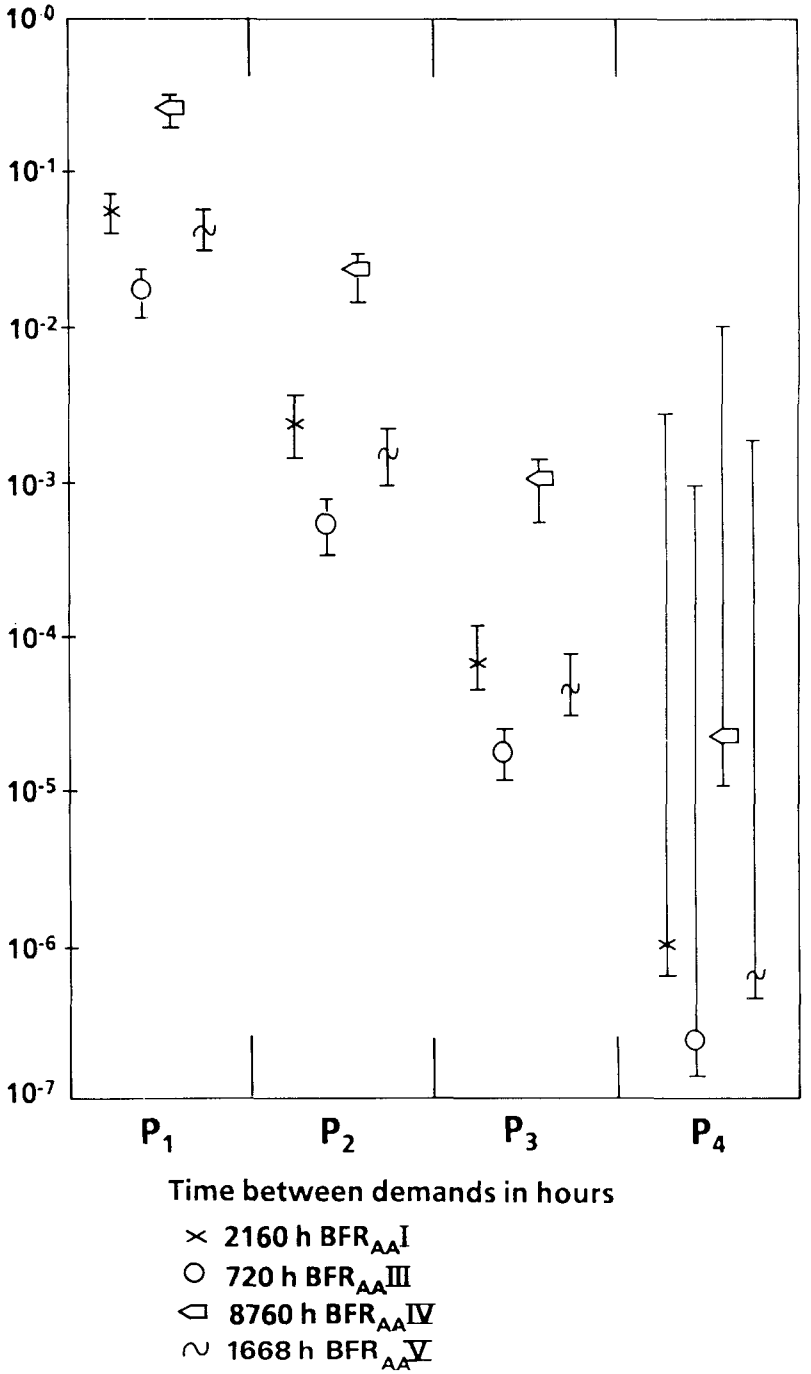


Figure 2.4

Estimated probabilities of observing exactly i (i=1,2,3,4) failures per demand (BFR_{AA}I, III, IV & V).

STUDSVIK (Dinsmore and Pörn, 1986) performed one sensitivity study where ATOM's CCF-events according to Table 2.3 were used as a basis. However, in this sensitivity study STUDSVIK applied its own extension scheme. The use of ATOM's data where a majority of CCFs is classified as potential, highlighted the impact of the methodological decision made by STUDSVIK not to "extend" potential failures. The results for the statistical data, the STUDSVIK extended data, and the ATOM extended data are given in Figure 2.5. As can be seen from the plot, the identification and definition of CCF-events have a greater impact on the mean values (ATOM vs. STUDSVIK data) than the expansion of data (statistical vs. expanded data). The identification and definition also have a substantial impact on how wide the uncertainty bound will be.

VTT (Pulkkinen et al., 1986) performed sensitivity analysis with respect to:

- assumptions concerning the redundant valve groups
- test interval in the case of BFR-model
- different prior distributions in the case of Bayesian evaluation of multiple probabilities.

The sensitivity analyses with respect to the redundant valve groups were performed for both BFR- and ADDEP-models. It was noticed that BFR-model is very sensitive to the redundancy level assumptions and that the sensitivity of ADDEP to these assumptions is not so strong. The Bayesian estimation may be rather sensitive to the choice of prior distribution, especially in the case of small evidence. This fact was demonstrated again in VTT's sensitivity studies.

STUDSVIK and VTT performed finally a sensitivity study using ATOM's screened and extended data from the $MGL_{AA}I$ - case, and direct assessment based on noninformative prior and informative prior, respectively. Studsvik varied also the number of demands. Both own estimate (3834) and ATOM's estimate for the MFR-case (3489), were used. The number used in VTT's calculations is 4865. The results of this sensitivity study are given in Table 2.8 and in Figure 2.6, which also shows the confidence intervals. The estimated mean values are quite close to each other. As was previously mentioned the uncertainty intervals of MGL-method are not complete (the uncertainty of the component failure probability was not taken into account),

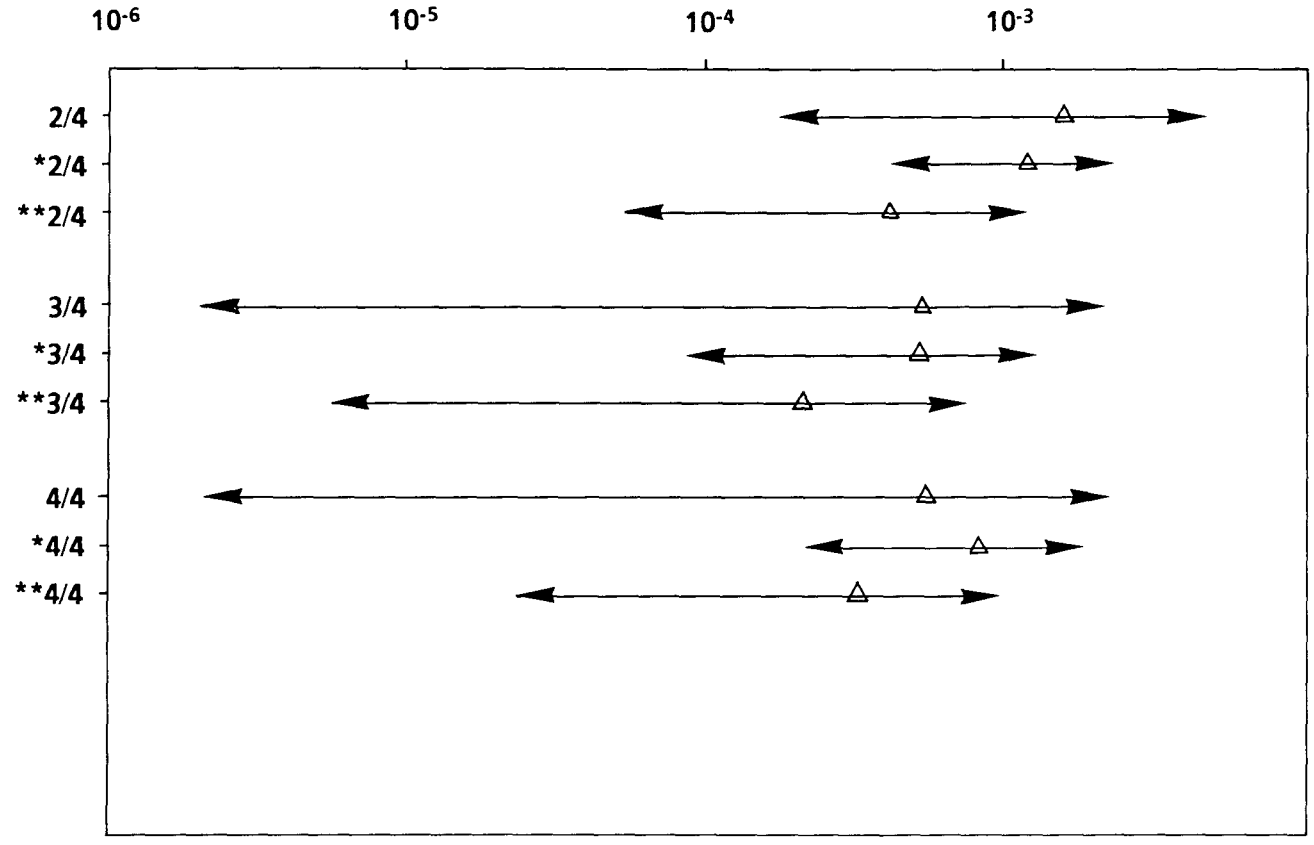


Figure 2.5

Plot of the confidence intervals for the CCF probability of i (i=2,3,4) out of four valves failing

* Includes "Assigned failures" = Mean value

** Includes "Assigned failures" and based on ATOM data

and therefore they are substantially smaller than the others. The lower mean values of P_3 and P_4 provided by MGL-method may be due to the intrinsic features of this method.

Table 2.8

Sensitivity study based on statistical evidence of the $MGL_{AA}I$-case, direct assessment and different number of demands

Method	Number of demands	P_2	P_3	P_4
$MGL_{AA}I$	-	$8.7 \cdot 10^{-4}$	$1.2 \cdot 10^{-4}$	$1.1 \cdot 10^{-4}$
DA_SI	3834	$6.0 \cdot 10^{-4}$	$2.1 \cdot 10^{-4}$	$2.1 \cdot 10^{-4}$
DA_SI	3489	$6.6 \cdot 10^{-4}$	$2.3 \cdot 10^{-4}$	$2.3 \cdot 10^{-4}$
DA_VII	4865	$4.6 \cdot 10^{-4}$	$1.6 \cdot 10^{-4}$	$1.6 \cdot 10^{-4}$

Most essential results from sensitivity studies may be summarized:

1) BFR-model is extremely sensitive to assumptions.

2) With few exceptions most of the discrepancies in the estimated CCF-contributions can be explained by differences in the treatment of data (CCF-definition in general, definition of potential CCFs, screening, use of impact vectors and weighting factors etc.).

2.2.4 Conclusions and recommendations of the CCF-data Benchmark Exercise

The search for CCFs and quantification of CCF-contributions has been performed using rather small resources (4 person-months per group). However, the total effort is considered as adequate for the purpose of the Benchmark Exercise. The methods used for CCF-identification are straightforward and require as a minimum information failure descriptions containing failure mode, cause, criticality and time of detection. However, availability of much more detailed background material including data on type of MOVs, physical locations, manufacturers, maintenance policies etc, would decrease the impact of subjective judgement on the results. These aspects should be

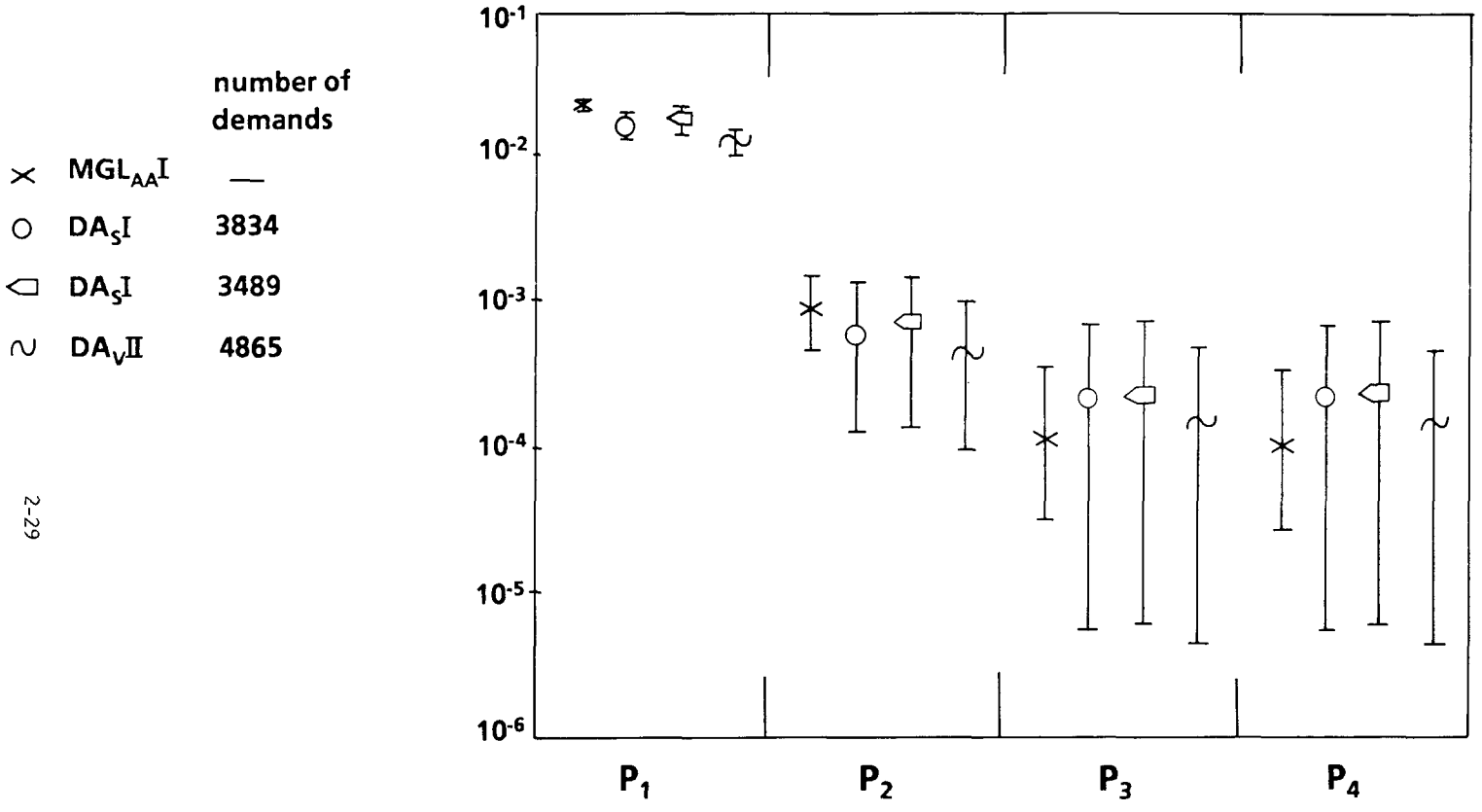


Figure 2.6

90% confidence intervals for cases according to Table 2.8

considered in future applications. A natural limitation of the study is its completeness. Main emphasis has been put on identification of CCFs within each individual system. Furthermore, many aspects of the selection process are subjective and sometimes rather speculative. Therefore, we cannot claim that the list (Table 2.3) is complete. An in-depth study including collection of additional information from sources available at the plant (interviews with personnel, study of maintenance logs etc.) has been performed for one doubtful case. In a large scale application of search procedures this should be done for a majority of CCF-candidates.

The use of computers to aid in searching, sorting and generally reorganizing failure reports is highly recommended. However, dependence on the computer alone to directly identify CCF-candidates is discouraged. In the latter case, it is necessary to depend heavily on the coding which is a major source of uncertainty.

Some desirable information is not available when the original failure reports are written; failure cause specification - if it is ever available - is often delayed. The uncertainty concerning the quality of reports originating from the overhaul periods is a serious drawback. Since a majority of CCF-candidates has been detected during this period, any improvement of these reports would be most welcome. In addition, when carrying out the screening procedures attention should be given to the types of tests carried out during normal operation and during overhaul, and their capability of revealing critical failures. Treatment of multiple failure events detected during the overhaul period proved to be one of the most controversial and unresolved issues in the Benchmark Exercise. Use of expert systems for generating of the reports has been suggested as a possible improvement.

Due to the nature of ATV-reports (concern only single components) the use of classification systems is of limited value. Possibly, decisions could be facilitated in some doubtful cases. The classification systems are cause-oriented, while ATV-reports supply in the first place information about failure modes. Among the advantages of the classification systems we could mention that they provide a systematic and standardized way of presenting and saving of the results as well as a good framework for exchanging information and experiences between analysts. Consequently, understanding of foreign CCF-events may be facilitated by use of a good classification scheme.

The quantitative analysis has shown that direct assessment of CCF-contributions is possible, given comprehensive information containing system flowschemes for identification of redundancies, and number of actuations and failures of all relevant components. Simple parametric methods (MGL, ADDEP) are still of major interest; in particular for components which are not so common at the plant as valves. They are easy to apply and suitable for checking the impact of modified assumptions. Additionally, no attempt was made to apply direct estimation to continuously operating components where data collection may be more difficult. From the practical point of view it is important to note that these methods may be directly combined with the information on single failure probabilities, given in the Swedish Reliability Data Book (Bento et al., 1985). The MGL-method may in special cases underestimate the mean value and variance of CCF-contributions (see chapter 4).

The complexity of the BFR-model makes it difficult to identify critical elements and to perform sensitivity studies. The main disadvantage of the BFR-method is that the available version does not contain any specifications or recommendations on how to integrate detailed plant-specific information into the model. The criteria for classification of failures are vague which apparently may result in arbitrariness.

The MFR-method has been previously applied only to an assumed set of data. Input information for MFR-model requires an as detailed knowledge of background data (e.g. number of system demands) as in the case of direct assessment, which limits the usefulness of the MFR-model (the same effort is required for direct assessment which should be preferred). As expected (Apostolakis and Moieni, 1987), the MFR-model leads to a somewhat higher estimate of P_4 and to broader confidence intervals in comparison with the MGL-method.

The search for CCFs has shown that identification of such events can be reasonably performed using the available failure reports. Excluding the differences in scope and neglecting the differences in definitions, the agreement between the groups is satisfactory. On the other hand, including these differences produces much worse agreement. This fact supports the

requirement of providing a clear and concise specification of boundary conditions when performing studies of operational CCF-experience. The differences in scope should be seen mainly as an organization problem in the context of a Benchmark Exercise.

The role of subjective judgement would be significantly decreased if more information, particularly on failure causes, could be included in the descriptive part of failure reports. Major improvements would be expected as a result of involving plant personnel in the scrutiny of failure reports describing the identified CCF-candidates. This could supply additional information and facilitate forming a final opinion.

With few exceptions most of the discrepancies in the estimates of CCF-contributions obtained by different groups can be explained by differences in the treatment of data, i.e. definition of criticality, screening, use of impact vectors and weighting factors etc. Consequently, several of the factors which are essential in the process of CCF-identification have also a major impact on quantification. These findings are consistent with the results of the CCF Reliability Benchmark Exercise coordinated by Ispra Establishment (Poucet et al., 1987).

The recommended approach to quantification, in applications when in-depth studies of raw data are possible, would be based on direct assessment of CCF-contributions. Use of simple parametric methods, such as MGL- and ADDEP-models, is still of major interest; they may be directly combined with data on single failure probabilities given in the Swedish Reliability Data Book (Bento et al., 1985), are easy to apply, are suitable for checking the impact of modified assumptions, and represent in practice the only option which may be applied to components which are not as common at the plants as valves. On the other hand, the BFR-model is complex and its use may result in arbitrariness. The MFR-method needs as input the same type of information as direct assessment.

2.3 Retrospective Qualitative Analyses of Treatment of Dependencies in Swedish PSAs

Analyses of dependencies in the Swedish PSAs contain a variety of models, data and assumptions. Thus, it is possible that modeling aspects could explain some of the differences in the results of different studies. The impact of CCF-contributions on the predicted core damage frequency of a four-divisional Swedish BWR is shown in Figure 2.7 (Hirschberg and Knochenhauer, 1987). At the same time it is obvious that use of an alternative quantification model or data could lead to a different picture.

In view of the substantial uncertainties associated with the treatment of certain types of dependencies, a major effort was undertaken to systematically compare the analyses performed in the Swedish PSAs. The work concerning qualitative analysis has ben carried out mainly within the present RAS-470 project but was coordinated with the SUPER-ASAR project (Carlsson et al., 1987) aiming at an overall comparative review of the available Swedish PSAs. The main emphasis in the summary of work which follows below will be on the treatment of common cause failures. Details concerning explicitly modelled dependencies may be found in SUPER-ASAR reports addressing event tree and fault tree analyses.

2.3.1 Scope of work

The focus in the summary of findings which follows below will be on qualitative aspects of dependency analyses in the Swedish PSAs. This should be interpreted in a wide sense, i.e. also the quantitative methods and data applied will be covered. However, the results of sensitivity studies which have been based on the input from the qualitative phase will be described separately (chapter 4).

Only the studies completed at the time when the review started have been considered, i.e. level 1 PSAs for five ABB Atom BWR plants (Ringhals 1, Swedish State Power Board, 1984; Barsebäck 1, Sydkraft, 1987; Forsmark 3, ABB Atom AB, 1985; Oskarshamn 3, OKG AB, 1986 and Oskarshamn 1, OKG AB, 1987) and for one Westinghouse PWR plant (Ringhals 2, NUS-Corporation, 1984). The basic versions of the studies include internal events such as transients and loss of coolant accidents (LOCAs), while external events have been treated in supplementary analyses (see chapter 4).

For details of the comparative review we refer to the main report (Hirschberg, 1987).

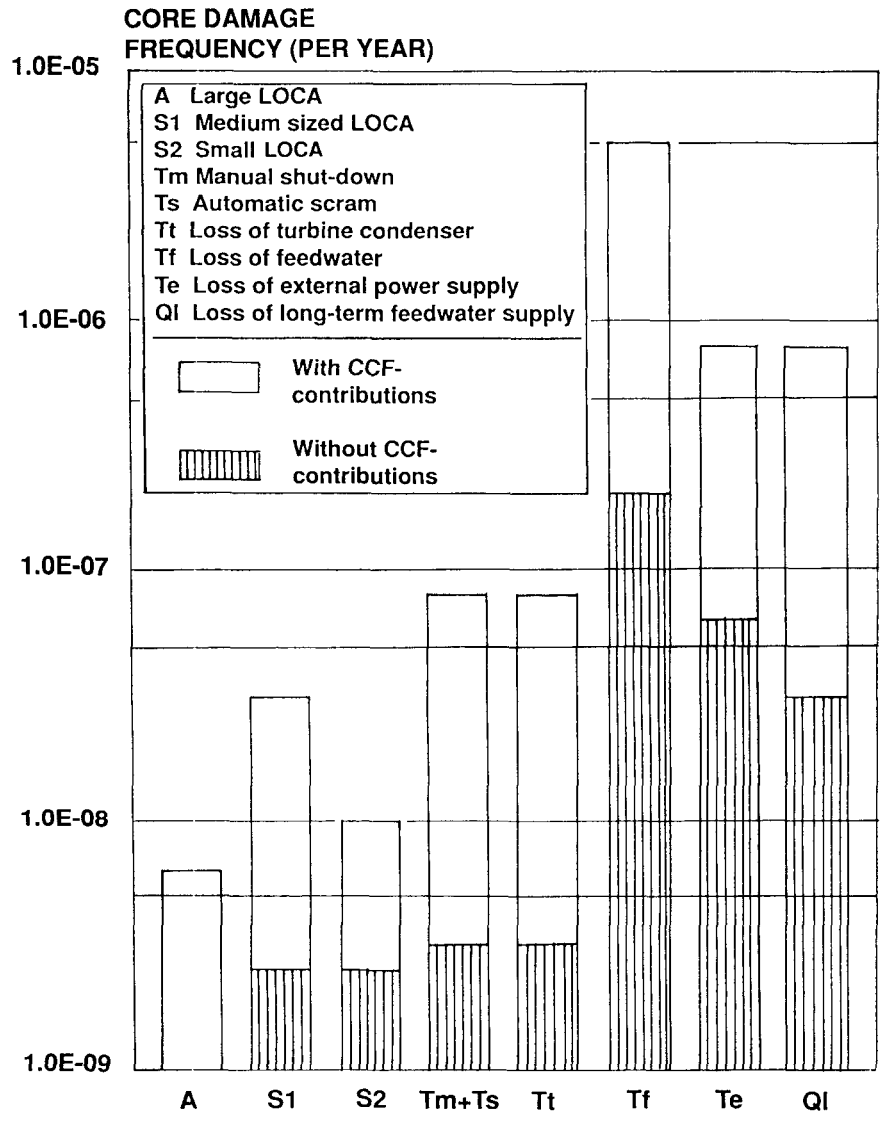


Figure 2.7

Accident frequencies according to Forsmark 3 PSA with and without CCF-contributions

2.3.2 Categories of dependent failures

A systematic classification of dependent failures is necessary when carrying out the comparative studies. For the purpose of the present study the classification of PRA Procedures Guide (U.S. Nuclear Regulatory Commission, 1983) has been adopted (Table 2.9).

Table 2.9

Definition of dependent failure categories (U.S. Nuclear Regulatory Commission, 1983)

Type 1. Common-cause initiating events (external events): external and internal events that have the potential for initiating a plant transient and that increase the probability of failure in multiple systems. These events usually, but not always, result in severe environmental stresses on components and structures. Examples include fires, floods, earthquakes, loss of offsite power, aircraft crashes, and gas clouds.

Type 2. Intersystem dependencies: events or failure causes that create inter-dependencies among the probabilities of failure for multiple systems. Stated another way, intersystem dependencies cause the conditional probability of failure of a given system along an accident sequence to be dependent on the success or failure of systems that precede it in the sequence. There are several subtypes of interest in risk analysis.

Type 2A. Functional dependencies: dependencies among systems that follow from the plant design philosophy, system capabilities and limitations, and design bases. One example is a system that is not used or needed unless other systems have failed; another is a system that is designed to function only in conjunction with the successful operation of other systems.

Type 2B. Shared-equipment dependencies: these are dependencies of multiple systems on the same components, subsystems, or auxiliary equipment. Examples are (1) a collection of pumps and valves that provide both a coolant-injection and a coolant-recirculation function when the functions appear as different events in the event tree and (2) components in different systems fed from the same electrical bus.

Type 2C. Physical interactions: failure mechanisms, similar to those in common-cause initiators, that do not cause an initiating event but nonetheless increase the probability of multiple-system failures occurring at the same time. Often they are associated with extreme environmental stresses created by the failure of one or more systems after an initiating event. For example, the failure of a set of sensors in one system can be caused by the excessive temperature resulting from the failure of a second system to provide cooling.

Type 2D. Human-interaction dependencies: dependencies introduced by human actions, including errors of omission and commission. The persons involved can be anyone associated with a plant-life-cycle activity, including designers, manufacturers, constructors, inspectors, operators, and maintenance personnel. A dependent failure of this type occurs, for example, when an operator turns off a system after failing to correctly diagnose the condition of the plant - an event that happened during the Three Mile Island accident when an operator turned off the emergency core cooling system.

Type 3. Intercomponent dependencies: events or failure causes that result in a dependence among the probabilities of failure of multiple components of subsystems. The multiple failures of interest in risk analysis are usually within the same system or the same minimal cut set that has been identified for a system or an entire accident sequence. Subtypes 3A, 3B, 3C, and 3D are defined to correspond with subtypes 2A, 2B, 2C and 2D, respectively, except that the multiple failures occur at the subsystem and component level instead of at the system level. Type 3 dependencies should be analyzed as part of the evaluation of fault trees.

2.3.3 Approaches to modeling of dependencies

It is apparent from the comparison which has been carried out that differences exist between the studies with respect to the degree of coverage. Specific problems have been identified, which are accounted for in some of the studies, but not in the others. These differences may be pointed out and should be the subject of future studies. At the same time the PSAs exhibit many similarities in the approaches to dependency analysis. This is not surprising since by and large the same main frame for the analysis (small event tree/large fault tree approach) has been used. In spite of the similarities, the parallel studies of accident sequence and systems analysis modeling disclosed specific discrepancies with regard to functional and shared-equipment dependencies, which do not necessarily origin from actual design differences, but are due to different perception of the design, different assumptions, or mistakes.

The main problem from the point of view of the comparative analyses is the varying standard of the documentation of the studies. This means that some of the PSAs may be reasonably complete, but their credibility would be greater and the review process would be facilitated given an improved documentation.

Generally, treatment of dependencies is considered as a strong part of the Nordic PSAs. Characteristically, most of the findings in form of identified plant deficiencies, involve unintended dependencies. In several cases the insights have led to introduction of modifications at the plants and, consequently, to significant safety improvements. Some examples originating from different plants follow below:

1) Some safety systems were connected to the same overcurrent protection switch as non-safety equipment (not qualified for accident environment) inside containment. Short-circuit (resulting from e.g. internal flooding) in the non-safety equipment might disable several safety systems.

2) Two of three water level sensors were fed from the same bus. Loss of this bus in connection with a single failure in the auxiliary feedwater system leads to loss of make-up water.

3) High temperature in only one train of shutdown secondary cooling system results in loss of shutdown cooling system function.

4) Inadvertent switch on of a breaker results in interconnection of two AC-buses and loss of power supply to equipment in several safety systems. The most serious consequence is that only auxiliary feedwater system is available for water make-up to the reactor.

Characteristically, no dependency-related design deficiencies were identified in PSAs for the latest generation of ABB Atom plants. This may be attributed to the basic design principles of four-divisional plants. The main features include complete separation of the redundant trains of the main safety functions and of the corresponding supporting functions, separation of operational and safety equipment from the physical and functional point of view, application of diversity for some critical safety functions (e.g. reactor shutdown, containment isolation), and absence of complicated links, interactions and interconnections between safety related functions (Hirschberg and Tirén, 1989).

Below follows a short summary of the insights gained from the comparison. The analysis of CCFs will be covered separately in 2.3.4.

1) The issue of equipment related Common Cause Initiators (CCIs) has been addressed in all PSAs. However, only the Ringhals 1 and Forsmark 3 studies contain a systematic and dedicated analysis of CCIs. Significant CCIs have been identified in the Ringhals 1 and Oskarshamn 1 PSAs. The coverage of the Ringhals 1 analysis is not fully clear.

2) Functional dependencies are handled in all studies by the small event tree/large fault tree approach. Discrepancies which cannot be explained by design differences exist and are caused by different perception of the design, different assumptions, or errors in the analysis. A detailed survey of these differences has been generated within the SUPER-ASAR project. Some functional deficiencies have been identified by the Ringhals 1 and Barsebäck 1 PSAs.

3) Shared-equipment dependencies are covered in all studies by fault trees which in most cases are characterized by a high degree of detail (see Table 2.10). Possible problems may origin from computerized Boolean reductions or/and from manual reductions of these large logical models.

4) None of the Swedish PSAs contains a documented, systematic and comprehensive search for physical interaction dependencies. However, a relatively thorough survey has been made within the Barsebäck 1 PSA. Documentation of a similar study within the Oskarshamn 1 PSA is not available. Influence of normal environment is covered by fault trees and residual CCFs. The back-flush operation in the context of LOCA is considered to be important in the Ringhals 1 and Barsebäck 1 PSAs on the one hand, and not necessary in the Oskarshamn 1 study. Only the Forsmark 3 PSA contains an analysis of dynamic effects which may follow upon a pipe break. Such effects may be much more significant for the other plants, particularly those which do not belong to the latest generation of ABB Atom plants.

5) Human interaction dependencies are represented in the fault trees and event trees, and also covered by residual CCFs. Generally, the Ringhals 1 PSA contains the most ambitious analysis of human interactions. None of the studies addresses the problem of errors of commission. Systematic misconfiguration of redundant components has been addressed in the Ringhals 2 PSA for some motor-operated valves, in the Forsmark 3 PSA sensitivity study, and qualitatively in the Ringhals 1 PSA.

6) Non-standard methods for identification and evaluation of dependencies have been used in some of the studies. Examples comprise e.g. extended signal analysis within the Forsmark 3 PSA and systematic walk-through analyses within the Barsebäck 1 and Oskarshamn 1 PSAs. The limitations of this type of approach are substantial.

7) Residual CCFs, which account for the dependencies not covered explicitly by the event tree/fault tree model, have been used in all PSAs.

Table 2.10

Rough survey of degree of detail in systems modelling of different PSAs[a]

PSA \ Systems	Make-up water	Residual heat removal	Reactor shut-down	Elec-trical power supply	Reactor protec-tion (RPS)	Other auxili-ary func-tions
Ringhals 1	H	H	H	L	H	M
Barsebäck 1	H	H	M	M	H	L
Forsmark 3	H	H	H	M	H	M
Oskarshamn 3	H	H	H	M	H	L
Oskarshamn 1	H	H	L	H	-[b]	L

[a]The degree of detail is denoted as high (H), medium (M) or low (L).

[b]A note given in the study states that fault trees for RPS exist, but have not been included.

2.3.4 Treatment of common cause failures

2.3.4.1 Definition

There is a variety of definitions of Common Cause Failures (CCFs) in the Swedish PSAs. As a rule none of the studies supplies a strict definition, but rather a number of characteristic features attributed to CCFs have been specified. Among them we may mention: multiplicity, common cause, simultaneity and criticality. From the practical point of view the exact wording used in definitions is of secondary interest. Several examples may actually be found where terminology is mixed-up and the more general term "dependency" is used instead of "common cause failure" or vice versa. In practice CCFs are in all studies considered as a subset of dependencies. This means that CCFs, which are usually referred to as residual common cause failures, account for the dependencies which are not explicitly included in the analytical models (event trees and fault trees).

2.3.4.2 CCF-representation

CCFs are represented in Swedish PSAs on three levels in the fault trees:

- component tree level (B1, O3 and O1 PSAs)
- system train tree level (F3 PSA)
- function tree level (R1 and R2 PSAs).

Table 2.11 summarizes the advantages and disadvanteges of different ways of incorporation of CCF-contributions into the fault trees.

2.3.4.3 Degree of coverage

The intended degree of coverage is almost identical in all PSAs. CCF-contributions have been quantified for active, redundant components (e.g. motor-operated valves, pumps and diesel generators) in safety systems. As a rule only intrasystem contributions have been considered. Consequently, contributions from passive components, diversified equipment, intersystem CCFs, have been neglected. Some exceptions from this rule have been found, but they are not characteristic for any of the studies.

Table 2.11

Alternatives for incorporation of CCF-contributions into the fault trees

CCF-representation in Fault Trees	Advantage	Disadvantage
Component tree level (B1-, O1- and O3 PSAs)	Systematic procedure	Large complex fault trees for four-divisional systems
	Completely automatic calculations	
System train tree level (F3 PSA)	Relatively compact model even in the case of four-divisional systems	Some handmade calculations may be necessary
		Complete symmetry necessary
Function tree level (R1- and R2 PSAs)	Compact model	Correct distinction between different failure multiplicities not possible

2.3.4.4 Quantification of CCF-contributions

The choice of a suitable method for quantification of CCF-contributions has always been controversial. A number of parametric models have been developed and used in the context of PSA-studies. In an ideal world some requirements could be placed on these methods:

1) Simplicity
2) Clear definition of parameters
3) Correctness (within specified limitations)
4) Generality
5) Compatibility with existing data sources
6) Assurance of realism
7) Possibility to consider design- and system-specific factors
8) Possibility to distinguish between different failure multiplicities.

In practice some of the above requirements may be in conflict with each other and the final choice is a matter of compromise. Evaluation of the different approaches used, has been made on the basis of earlier comparisons of quantitative methods (Pulkkinen, ed., 1987 and Hirschberg, 1985a) and experiences from the Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987).

The following quantitative methods have been used in the Swedish PSAs:

- extended C-factor model (R1 PSA)
- beta-factor model (B1 PSA)
- C-factor model (R2 PSA)
- MGL-model (F3-, O3- and O1 PSAs).

CCF-data in Swedish PSAs are based on:

- U.S.-experience (R1-, R2- and O3 PSAs)
- engineering judgement (B1- and O1 PSAs)
- limited study of the Swedish operating experience (F3 PSA).

In principle all these approaches may be acceptable, given a proper treatment of data. The following deficiencies have been identified in this context:

1) Ringhals 1 and Oskarshamn 3 C- and beta-factors, respectively, correspond to plant-specific data for Ringhals 2 and Seabrook. Direct application of such data to other plants is not in line with the intentions behind the parametric models.

2) Oskarshamn 1 gamma-factors correspond to reduced Seabrook-data (see point 1 above) and are judged as optimistic.

3) Assignment of CCF-parameters in Barsebäck 1 and Oskarshamn 1 PSAs is based on engineering judgement. Consequently, completeness and precision can be questioned.

4) CCF-parameters of Forsmark 3 PSA are in some cases based on a rather limited material (from statistical point of view).

Table 2.12 summarizes advantages and disadvantages of different approaches to assignment of CCF-data, as applied in the Swedish PSAs.

Table 2.12

Different Sources of CCF-Data in Swedish PSAs

Source	Advantage	Disadvantage
U.S.-experience (R1-, R2, O3-PSA) [a]	Relatively comprehensive material	In principle not applicable to Swedish conditions (differences in design, operation, maintenance)
		Extremely difficult to adjust data to Swedish conditions
Engineering judgement (B1-and O1-PSAs)	Plant-specific data directly obtained	Completeness questionable
	Qualitative results useful for the utility	Highly dependent on quality of analysis
		Applicability limited to operating plants with moderate or poor separation
		Experience from other plants not used
Swedish/Finnish experience (F3 PSA)	Relevant material	Experience not very comprehensive
	Good knowledge of the background	
	Valuable for specification of defensive measures	

[a]All three studies use US-experience, but while data for Ringhals 2 have been obtained after proper design- and application-oriented screening, data for Ringhals 1 are plant-specific Ringhals 2-data and data for Oskarshamn 3 are reduced Seabrook-specific data.

Beta-factors from Forsmark 3 and Oskarshamn 3 PSAs and C-factors from Ringhals 1 and 2 PSAs are given in Table 2.13. Beta-factors in Barsebäck 1 and in Oskarshamn 1 PSAs are not component-type specific. In these studies three respectively two different values of beta-factor (0.01, 0.05, 0.10 and 0.05, 0.10), have been used. The choice of the beta-factor was in each particular case dependent on the significance factors assessed in the qualitative analysis.

CCFs for failure to run have been neglected in case of diesel generators at Barsebäck 1, Oskarshamn 3 and Oskarshamn 1. These contributions can be significant; in Ringhals 1 and in Forsmark 3 they constitute 54% and 42%, respectively, of the corresponding CCFs for failure to start.

The higher order parameters, gamma and delta have been assigned values of 0.4 and 0.6, respectively, in the Forsmark 3 PSA, and 0.3 and 0.9, respectively in Oskarshamn 1 and 3 PSAs. Factor 0.5 has been used in Ringhals 1 PSA when extending the C-factor model to 4 x 50%, 3 x 100% or 4 x 100% systems. No such extensions have been used in the Ringhals 2 and Barsebäck 1 PSAs.

The numerical differences are very significant. Comparison of CCF estimates for diesel generators shows that quadruple CCF-contribution for diesel generators in the Oskarshamn 3 PSA is 30 times lower than in Ringhals 1 and 14 times lower than in Forsmark 3 (a twin plant). Such large discrepancies will naturally have a dramatic impact on accident sequences resulting from loss of offsite power. These discrepancies are not motivated by actual differences in design and operation of diesel generator systems.

2.3.4.5 Treatment of systems with non-standard success criteria

The previously mentioned methods for quantification of CCF-contributions may in their basic formulations only be applied to systems with at most four redundant components. In certain systems (e.g. groups of control rods, pressure relief valves, frequency converters, reactor scram modules), a larger number of identical components with the same functions may occur. This leads to non-standard success criteria for these systems and to requirements on non-standard approach to quantification of the corresponding CCF-contributions.

Table 2.13

Beta-factors of Forsmark 3 and Oskarshamn 3 Studies and C-factors of Ringhals 1 and 2 Studies

Component	Failure mode	Beta-factor		C-factor
		F3	O3	Ringhals 1&2
Air-operated valve	Fails to operate	0.16	-	0.14
Scram valve	Fails to open	0.08	coupling factors used	0.14[a]
314-main valve	Fails to open	0.04	-	0.14[a]
Motor-operated valve	Fails to operate	0.07	0.022	0.042[b] 0.0096[c]
Motor-operated valve	Wrong configuration[d]	-	-	0.25
Check valve	Fails to open	0.01	-	-
Safety valve	Opens inadvertently	0.02	0.02	-
Fan	Fails to start	-	-	0.039
Centrifugal pump	Fails to start	0.02	0.085	0.039[b]/0.0097[c]
-"-	Fails to run	-	-	0.029
Piston pump	Fails to start	0.02	0.026	not applicable
Turbine driven pump	Fails to start	not applicable	not applicable	0.039[a]
-"-	Fails to run	-"-	-"-	0.029[a]
Diesel generator	Fails to start[e]	0.03	0.0065	0.054
-"-	Fails to run	0.03	-	0.008

[a]Applicable only to Ringhals 1.
[b]No repair.
[c]With repair; applied only in Ringhals 2 PSA in situations where repair can be made in a 6 to 9 hours time interval.
[d]Applies only to MOVs which do not receive a conformatory open or close signal upon system initiation.
[e]The corresponding beta-factors for diesel generator in Oskarshamn 1 and Barsebäck 1 are 0.11 and 0.03, respectively.

Different methods have been used for estimation of such CCF-contributions. In Ringhals 1 PSA the extended C-factor method has been applied. However, only one failure combination has been considered (this applies also to the Oskarshamn 1 PSA) which probably leads to underestimation of CCF-contributions. Both Barsebäck 1 and Oskarshamn 3 PSAs use coupling factors for quantification of CCF-contributions for reactor shutdown functions. Such approach is in principle correct, but the factors are arbitrary and not supported by the operating experience. The Forsmark 3 PSA uses an extended MGL-method. Having in mind the uncertainties associated with the parameters involved, this method should be seen as an extended sensitivity study. It should be noted that the frequencies of ATWS-sequences are in most cases proportional to these very uncertain CCF-contributions.

2.3.4.6 Impact of CCFs on dominant accident sequences

Table 2.14 shows an example of the impact of CCFs on the dominant accident sequences.

It is apparent from the tables that the intercomponent CCFs have a decisive impact on the results of the studies. The principal CCF-contributors are in the first place motor-operated valves and pumps (mainly centrifugal). Thus, the future efforts should be concentrated on supplying better estimates of CCF-contributions for these components. In the case of MOVs a comprehensive background material has been collected and evaluated; this material could be used for estimation of plant-specific CCFs for Swedish BWRs. As indicated in the Forsmark 3 PSA, the existing statistical evidence for pumps is signifcantly weaker than that for MOVs. Other important components in the context of CCF-contributions are e.g. diesel generators, gas turbines, scram valves, RPS-logic channels and pressure relief valves.

Table 2.14

Impact of intercomponent CCFs on top ten dominant accident sequences of the Ringhals 1 PSA

Accident Sequence	Sequence Frequency (per year)	CCFs Represented in x out of Y Cut Sets (X/Y)	CCFs Represented in Cut Set No. (among top ten)	Principal CCF-contributor	Total CCF Importance (%)
S1W1	$6.5 \cdot 10^{-7}$	8/21	3,4,5,6,7,8,9	322-MOVs 711-pumps 322-pumps	49
S1 V1	$4.3 \cdot 10^{-7}$	5/41	1,2,3,5	323-pumps 323-MOVs	90
R	$2.7 \cdot 10^{-7}$	-	-	-	-
AW1	$2.1 \cdot 10^{-7}$	8/21	3,4,5,7,8,9	322-MOVs 711-pumps	37
Sy	$1.9 \cdot 10^{-7}$	-	-	-	-
S1Y	$1.8 \cdot 10^{-7}$	-	-	-	-
AV1	$1.0 \cdot 10^{-7}$	5/41	1,2,3,5	323-pumps 323-MOVs	90
AY	$9.0 \cdot 10^{-8}$	-	-	-	-
T_EUV1Q'	$7.1 \cdot 10^{-8}$	36/49	1,2,3,4,5,7,8	323-pumps 323-MOVs	55
T'_FC2H3	$6.0 \cdot 10^{-8}$	2/14	1,2	211-valves 516-relays	100

2.3.5 Conclusions and recommendations

2.3.5.1 Completeness issue

The central questions to be addressed with respect to completeness of the Swedish PSAs are:

- What has been missed?
- Are there any scenarios not explicitly included?
- Have the studies been successful in identification of dependencies?

It is obvious from the comparison which has been carried out that differences exist between the studies with respect to the degree of coverage. Since the PSAs reflect state of knowledge (some of them better than the others) it is not possible to decide if any one of them is complete in the absolute sense. The answer would probably be negative due to the fact that new findings are still being made and the methodology for treatment of some problem areas is not well established yet. Apart from that, all the studies are limited in scope and some of potentially significant dependencies have been excluded from the analyses. In order to assure reasonable completeness the review process (internal and external) is extremely important. It should be remembered that some of the studies compared in this report have not yet been subject to external review.

The comparison of the degree of coverage of the studies provides anyway in the relative sense a picture of completeness of the PSAs. Specific problems have been identified, which are accounted for in some of the studies but not in the others. These differences may be pointed out and should be the subject of future studies. At the same time the PSAs exhibit many similarities in the approaches to dependency analysis. This is not surprising since by and large the same main frame for the analysis (small event tree/large fault tree approach) has been used. In spite of the similarities, the parallel studies of accident sequence and systems analysis modeling have disclosed specific discrepancies with regard to functional and shared-equipment dependencies, which do not necessarily origin from the actual design differences, but are due to different perception of the design, different assumptions or mistakes.

The main problem from the point of view of the comparative analyses, is the varying standard of the documentation of the studies. This means that some of the PSAs may be reasonably complete, but their credibility would be higher and the review process would be facilitated given an improved documentation.

The overall picture is anyhow positive. The identified dependencies constitute major findings of several studies and without performing the PSAs would hardly been detected. This emphasizes the fact that qualitative analysis of dependencies is one of the strongest advantages of PSA-methodology and not a weakness. It is important to stress that point since due to a rather common misconception, dependency analysis is sometimes viewed as a weakness in the current state of PSA. On the other hand, quantification of common cause failure contributions is a definite limitation.

2.3.5.2 Recommendations for future work

Based on the conclusions of the comparative study some recommendations have been made, concerning:

1) Quantitative analyses (sensitivity studies)
2) Future research projects within the field of dependency analysis
3) Possible improvements of existing analyses.

The sensitivity studies were proposed to address the following problems:

1) Case studies of CCF- models and data.
   Diesel generators, motor-operated valves and pumps are components of primary interest. For motor-operated valves a good basis established within the Nordic Benchmark Exercise exists. This material could be used for generation of plant-specific CCF-parameters for all plants and subsequent requantification of dominating accident sequences. Another subject of interest is the influence of not distinguishing between all failure multiplicities. A comparison between the alpha-factor model (Mosleh and Siu, 1987) and the MGL-method (Fleming and Kalinowski, 1983) was also recommended.
2) Systematic misconfiguration of redundant components.
3) CCFs in systems with non-standard success criteria.

The sensitivity studies have been performed and are described in detail in subchapter 4.3.

The research projects which could improve the current state-of-the-art in Nordic countries are (the order reflects priority given to these projects):

1) Collection of CCF-data based on the Swedish/Finnish operating experience and using experiences gained in the Nordic (Hirschberg, ed., 1987) and Euratom (Poucet et al., 1987) Benchmark Exercises. In the long perspective also combination with foreign experience should be considered. The problem of combining different data bases has been studied within the RAS-470 project (Pulkkinen et al., 1987).

2) Search for Common Cause Initiators using the Swedish and Finnish operating experience (transients) and basic methodology given in (Laakso, 1984). The root causes behind the incidents are very important since they may provide valuable information of generic character. Possibly, potential interactions involving diversified systems could be identified.

In view of findings of the present work, some supplementary PSA analyses should be performed. They are specified below in the order of priority, which in this case is quite subjective since the phenomena are plant-specific.

1) CCI-analyses (Ringhals 2, Barsebäck 1, Oskarshamn 1). Power supply systems are suggested as the primary (but not only) subject of the studies.

2) Physical interaction dependencies, in particular dynamic effects after LOCA (Ringhals 1, Ringhals 2, Barsebäck 1, Oskarshamn 1).

3) Human interaction dependencies (all plants with the possible exception of Ringhals 1). The analyses should take more advantage of the knowledge and experience of operating personnel by performing systematic talk-through/walk-through studies.

2.4 Retrospective Qualitative Comparisons of Treatment of Dependencies in Foreign PSAs

2.4.1 Introduction

Trials to analyse the contribution of dependent failures to the core damage frequencies in selected PSAs have been made earlier; for instance within the Principal Working Group 5 of the OECD/NEA/CSNI [a] review of dependency analyses of five PRAs was carried out (Camarinopoulos et al., 1986). The purpose of the earlier analyses was not detailed study of the dependency analysis methods and consequently the analyses are quite superficial. Because of the lack of detail in the earlier studies it was felt important to make a review of the dependency analyses methods used in some recent foreign PSAs.

This report deals with five selected PSAs; Biblis B PSA, Sizewell B PSA, Calvert Cliffs 1 PSA, Oconee 3 PSA and Seabrook PSA. These studies were chosen because they represent different PSA generations and because they were available for this purpose. The selected five PSAs were made within different programs with different co-sponsors and for varying purposes. Some of the selected PSAs are rather old; on the other hand, some of the PSAs were made for plants which were not completed during the course of the studies. Due to the above differences direct comparison of the PSAs is not feasible and, thus, the results of this study should be used with care.

The Bibilis B PSA (German Risk Study (DRS);Electric Power Research Insititute, 1981a), was initiated in late 1976 and completed in 1979. It was based on WASH-1400 methodology (U.S. Nuclear Regulatory Commission, 1975). The study was performed by Gesellschaft für Reaktorsicherheit (GRS). The dependency analyses of the phase B of the Bibilis B study are also covered in the present study, based on two reports by GRS (Bongartz et al., 1985 and Hennings and Mertens, 1985).

The Sizewell B study, performed by Westinghouse, was completed in 1982. The results reviewed in this report are based on the Sizewell PSA-report (Westinghouse Electric Corporation, 1982) and the CSNI-report (Camarinopoulos et al., 1986).

---

[a] NEA: Nuclear Energy Agency; CSNI: Committee on Safety of Nuclear Installations

The Calvert Cliffs Study was completed in 1984. The analysis is a part of the Interim Reliability Evaluation Program (IREP) and it was performed by Sandia National Laboratories (SNL) (U.S. Nuclear Regulatory Commission, 1984).

Oconee 3 Study was started in 1980 and was completed in 1984. The study was performed by Nuclear Safety Analysis Centre (NSAC) of Electric Power Research Institute (EPRI) together with the Duke Power Company (Electric Power Research Institute, 1984).

Seabrook Study (SSPS) was started in 1982 and completed in 1984. It was performed by Pickard, Lowe & Garrick (PLG) (Pickard, Lowe and Garrick Inc., 1983).

The ratings of the plants vary from 845 to 1200 MWe. All these plants are PWRs which may restrict the applicability of the results of this study to BWR PSAs. However, the methods for dependency analyses do not depend on the plant type.

The background information needed in this kind of retrospective analysis is not documented in detail in the above mentioned PSA-reports. This makes the analysis very difficult and the objectivity of the analysis will suffer. Retrospective analysis should preferably be done in close co-operation with the original analysts and the personnel of the studied plant. This has not been possible in the present very limited overview.

For the purpose of the present study the classification of dependencies according to the PRA Procedures Guide (U.S. Nuclear Regulatory Commission, 1983) has been adopted (see paragraph 2.3.2). Plant external initiating events are discussed only briefly because they are not included in all studies. Common cause failures are of special interest though only two of the reviewed PSAs used parametric models for CCFs. Human-interaction dependencies will be reviewed separately in section 3.4 of this report.

2.4.2 Common cause initiating events

2.4.2.1 External events

Oconee and Seabrook PSAs include a profound study of external initiating

events. Oconee studied the effects of earthquakes, floods, tornadoes and fires, obtaining the result that 79% of the total core damage frequency is due to external events. For Seabrook the corresponding contribution is 26%, including fires, seismic events, missiles, and aircraft crashes. A short overview of external events is given in the German Risk Study phase A but a more detailed analysis has been prepared for the phase B report. In contrast, Calvert Cliffs and Sizewell PSAs do not consider external initiators at all.

In Oconee PSA, the dominant external events were turbine-building floods caused by a leak or a rupture in the condenser-circulating-water system (8.8×10^{-5} per year), and earthquakes (6.3×10^{-5} per year) causing a LOCA or a loss of offsite power. An analysis was performed for the flood caused by failure in the Jocassee Dam situated 12 miles upstream from Oconee. A cold shutdown of the plant could be achieved, but the flooding would disturb the decay heat removal. This accident would cause a core damage with a frequency 2.5×10^{-5} per year.

External events and spatial interactions were treated separately in Seabrook PSA. Seismic events cover 12% of the total core damage frequency. An analysis of spatial interactions was performed to identify initiators due to spatial commonalities. These incidents include for example floodings and fires. The fire analysis consists of grouping of fire events according to different fire locations and degrees of damage. Fire induced events contributed 11% of the core damage frequency. Other external CCIs (e.g. turbine and tornado missiles, floodings etc.) give a contribution of 3% to the total core damage frequency.

2.4.2.2 Loss of offsite power and other plant internal CCIs

In Seabrook PSA, common cause initiators were clearly separated from other intitiating events. Of all 58 initiating events 38 were considered as CCIs. In order to identify plant common cause initiators, seven support systems and subsystems known to contain potential CCIs were reviewed. To find out the final CCIs, a bottom-up type failure modes and effects analysis was performed for six systems. The most important initiators in solid state protection system and engineered safety features actuation systems were identified in master logic diagram and fault tree approach based on heat

balance analysis. Many of the failure modes were found to cause a plant shutdown prior to a plant trip, or were judged to be unimportant and thus were not included in the final list of initiating events. The four identified CCIs and their frequencies are loss of offsite power (1.35×10^{-1} per year), loss of DC-bus (3.35×10^{-2}), total loss of service water (2.3×10^{-6}), and total loss of component cooling water (1.38×10^{-6}). The event data for Seabrook PSA were partly generic but also plant specific data were used, and a review of several data sources was made to ensure the completeness of the initiating event list.

In Sizewell PSA, a search for common cause initiators has been made but the dependencies between systems are treated explicitly in the event trees and in the system analysis. In other studies, the expression "common cause initiator" was not used but some initiating events identified in Calvert Cliffs and Oconee PSAs could be classified as CCIs because they can cause a reactor trip and simultaneously degrade safety systems.

In Calvert Cliffs PSA, loss of service water system (SRWS) and failure of one DC-bus were identified as potential CCIs causing a reactor shutdown and also degrading safety systems required after the trip. Loss of SRWS would cause a reactor trip, loss of main feedwater, demand of auxiliary feedwater, and degradation of a number of safety related systems. Initiating event frequency from IREP quantification guide has been used in this context, giving a value of 1.8×10^{-3} per year. The failure of one DC-bus was assigned frequency 1.83×10^{-2} per year for a single bus. This value is plant specific for the Oconee PSA. For the system with two buses a frequency of 3.6×10^{-2} per year was used. The loss of offsite power was also included in the study of plant internal initiating events and it had a frequency of 1.4×10^{-1} per year.

Oconee PSA reported three special initiating events that can be considered as common cause initiators. The principal source of data was the study of PWR transients (Electric Power Research Institute, 1982) but data from plant operating experiences of three Oconee units was also largely used. The loss of service water system does not cause a reactor trip immediately, but a manual trip is likely in order to protect important plant equipment because many other systems require service water for operation. The mean annual frequency used was 4.0×10^{-3} per year, obtained by a detailed analysis of the

system, identifying failure modes unique for Oconee. The failure of instrument air system (annual core damage frequency estimated as 3.2×10^{-6}) has potential for causing a reactor trip and failing instrumentation and equipment that may be needed for the response to the trip. The mean annual frequency for the loss of offsite power was estimated from the data given in a report including LOSP frequencies for nuclear plants by region (McClymont and Poehlman, 1981). The value obtained was 1.7×10^{-1} per year consisting of two different failure types: failure of the grid of feeders and the substation failure.

In the Biblis PSA, the CCIs have not been treated separately, though some of the analysed initiating events could be clearly classified as common cause initiators. The loss of offsite power contributes 14% to the total core damage frequency.

The impact of CCIs on the core damage frequency including only internal initiators at different plants is summarized in Table 2.15. The reader should notice that the core damage frequencies do not contain external events, and thus differ from the total ones (Oconee and Seabrook).

Table 2.15
Total core melt frequencies caused by internal initiators and the contribution of CCIs

Plant	Total core damage frequency (per year)	LOSP[a] (%)	Other significant CCIs (%)
Sizewell	1.4×10^{-6}	0.8	
Oconee	5.4×10^{-5}	4.4	24 (LSW)[b]
Biblis	9.0×10^{-5}	14	
Calvert Cliffs	1.3×10^{-4}	12	16 (DC)[c]
Seabrook	1.7×10^{-4}	39	4 (all others)

[a]LOSP = Loss of offsite power
[b]LSW = Loss of service water system
[c]DC = Loss of DC-bus

2.4.3 Intersystem dependencies

Intersystem dependencies considered in this review are functional and shared-equipment dependencies, and physical interactions. Human-interaction dependencies are treated separately in section 3.4 and thus are not included here. Functional and shared-equipment dependencies are modeled in event and fault trees in all of the studies but the degree of detail differs between the PSAs. For example, Sizewell PSA uses large event trees and small fault trees, often calculated by hand, while Oconee PSA approach is based on large fault tree modeling.

In Seabrook PSA, all categories of intersystem dependencies are modeled explicitly in the event tree logic. Large event trees are divided into modules involving the separation of frontline and auxiliary systems. Dependecy matrices were constructed to facilitate the documentation of shared equipment dependencies. A separate analysis of spatial interactions was performed to identify physical interactions due to location. A fault tree was developed based on the event trees of the plant model. The computer code SETS was used to obtain the minimal cut-sets which were then quantified conservatively using point estimates. For potentially important scenarios, the conservative treatment was replaced by a more realistic model for the final quantification.

Functional interdependencies at Calvert Cliffs are incorporated into the event tree structure. Support system fault trees were constructed to model the interfaces with the frontline systems. The identification of dependencies between frontline and support systems was done by looking at each major component and determining what kind of support it required.

Sizewell PSA used large event trees to identify the intersystem dependencies. Supercomponents were made up of several components in the system and their unavailabilities were quantified. For especially complex supercomponents, fault trees were constructed. Fault trees used in this approach were small and the minimal cut-sets could be calculated manually.

In Oconee PSA, two sets of small event trees (one for LOCAs, one for transients) were developed and the functions were modeled using large,

detailed fault trees. Intersystem dependencies were identified during the development of the event trees and these dependencies were explicitly included in the fault trees. Fault trees model connections between systems and support requirements for each necessary component. Dependency matrices are not shown but interfaces with other systems are listed in detailed system analysis. The analysis of physical dependencies due to spatial and environmental commonalities was limited to an overview.

In German Risk Study, the frontline and support systems were modeled in the event trees, and the fault trees included interactions between systems. The study points out that most of the dependencies described in WASH-1400 (U.S. Nuclear Regulatory Commission, 1975) cannot occur in Biblis due to different plant design. Loops are spatially separated and protected, and diversity is used for redundant safety features.

2.4.4 Intercomponent dependencies

The identification and modeling of intercomponent dependencies is very similar to the methods used for intersystem dependencies. Exceptions are common cause failures that are not covered by explicit modeling in the fault trees. This section concentrates on the review of modeling and quantification of these failures.

Common cause failures were modeled implicity in Seabrook PSA and in the German Risk Study, Phase B Report. In the last mentioned PSA, different parametric models were compared and the Marshall-Olkin model was used in the final quantification. The Seabrok study used the beta-factor model for most of the components because of the two-train redundancy, but additional models were developed to cover other configurations. In other studies, common cause failures were modeled explicitly in the fault trees.

In Sizewell PSA, an additive cut-off contribution was used for the treatment of the commor cause failures. This approach was explained by the argument that the geometric mean approach (U.S. Nuclear Regulatory Commission, 1975) would underestimate the CCF-contribution and the beta-factor model would give too conservative values. The selection of the cut-off value was based on British safety criteria and on engineering judgement, which was motivated by the lack of statistical data (the plant has not been built yet).

Calvert Cliffs PSA modeled common cause failures explicitly in the fault trees. The fault trees were developed in detail to the component level and common hardware, test, maintenance and human errors were included. Other common mode failures such as environmental conditions or manufacturing defects were not considered in the study.

In Oconee study, the CCFs were included directly (explicitly) in the fault trees. Dependency-related effects were found to dominate the internal sequences, primarily due to failure of support systems and to operator actions.

Seabrook PSA quantified the common cause failures mainly implicitly using the beta-factor method. However, explicit models were used for physical interactions like fires and floods, and for certain human interactions. The basic two-component model covered most situations because of the two-train redundancy in most systems and additional 12 models were used for other configurations. These include both symmetrical and non-symmetrical configurations with three or more units. Collected failure data were classified into four categories: common cause failures, independent failures, potential CCFs, and "non-failures". These categories were weighted subjectively and the Bayesian methodology was used to develop the beta-factor distributions. The analysis of common cause failures showed that the numerical contribution of explicitly modeled common causes was small. In contrast, many systems were dominated or had major contributions made by the common cause failures estimated using the beta-factor model.

A study of common cause failures was performed as a part of German Risk Study phase B report. Several parametric models were reviewed and the advantages and disadvantages ot the models were pointed out. The discussed implicit methods were Square Roots Bounding method (i.e. geometric mean approach), beta-factor method, Marshall-Olkin model, Binomial Failure Rate model and Multiple Greek Letter method. The review of parametric models contained the following arguments: the geometric mean approach was judged to be arbitrary and unacceptable, and thus out of question. Beta-factor method is easy to use and can be applied to model also dependencies between different components but it gives too conservative values for more than two-redundant systems. In the Marshall-Olkin model the failure rates are

calculated separately for all configurations and the modeling is independent of the degree of redundancy. In the BFR-model, the different configurations can be described with only two parameters but the assumed exponential behaviour can generally not be proved. If no data is available for CCF of several components the extrapolated values are highly dependent on the amount of considered degree of redundancy.

The CCF-data for the German Risk Study were obtained from U.S. Licensee Event Reports. The data were selected to be suitable for German plants by excluding data from old plants (operation started before 1968), and some data considered not relevant for German plants. The remaining event data were further divided into groups according to failure mode, and dependent and independent failures were separated. The comparison of the estimated CCF-rates and those used in phase A study shows a significant difference between the results. Phase A results are about one magnitude greater than the CCF-rates estimated from the data from LERs. This difference raises the question whether the values used in phase A are too conservative or the new estimated rates are too optimistic (e.g. due to the neglect of some important events of the LERs). The earlier failure rates were estimated from German data where events with no (or only slight) significance are also taken conservatively into account. The report suggests that as long as the connection between independent and common cause failures is not resolved, the CCF-rates should be evaluated from the generic data by BFR-modeling with parameters estimated from Marshall-Olkin model.

2.4.5 Conclusions

This limited study confirmed the well known fact that dependencies are treated in various ways in modern PSAs. The main reasons for the differencies are connected with the plant being subject of the analysis, the analysis team, the purpose of the study and the generation of dependency analysis methods used. The results of the analyses cannot be directly compared because of the different assumptions and methods. One of the differencies between the analysed studies is of semantic nature: in certain studies some events are analysed as dependent events, while in other studies the same events are analysed in a quite similar way, but they are not

explicitly called dependent events. This reflects the lack of common language which still causes misunderstanding both in the analyses and in their interpretations.

The CCIs are in principle considered in all studies but some of the studies make the treatment more explicit. A good example of this is the Seabrook study where CCIs are treated in detail. Other studies consider the CCIs limited to the most important events such as loss of offsite power.

The differencies in treatment of the intersystem dependencies are reflected in the detailness of the fault trees and the event trees. For example, the Oconee PSA is fault tree oriented and the Seabrook PSA uses large event trees. In Seabrook study a special spatial analysis is performed to identify the most important spatial dependencies of the systems. This kind of analysis is missing in the other studies.

The intercomponent dependencies are also treated differently. For example in the Oconee study these events are almost without exception modeled explicitly in the fault trees. The quantitative models used in the studies are the beta-factor model with modifications, the Binomial Failure Rate model, the Marshall-Olkin model and the "cutoff-model" of the Sizewell study. Consistent use of these models can give reasonable results.

The data used in the quantitative evaluations are based mainly on the U.S.-experience. This is due to the well-known fact that the dependent failure data have not been analysed widely elsewhere. The estimates of the parameters vary significantly from study to study.

The contribution of the dependent events to the total core damage frequency varies also significantly from one study to another. The main causes for this are, of course, the different assumptions and models used in the dependency analyses and also the structure of the plants. In this limited study it was not possible to go into the details of the system models, i.e. the fault trees and the event trees. This would require close co-operation between the plant personnel and the respective PSA-analysts.

2.5 References

ABB Atom AB (1985)
Forsmark 3 Safety Study (in Swedish), 1985.

Apostolakis, G., Moieni, P. (1986)
On the Correlation of Failure Rates. Fifth European Reliability Data Bank Association (EuReData) Conference on Reliability Data Collection and Use in Risk and Availability Assessment, Heidelberg, Federal Republic of Germany, 9-11 April, 1986.

Apostolakis, G., Moieni, P. (1987)
The Foundation of Models of Dependence in Proabilistic Safety Assessment. Reliability Engineering, 18, pp. 177-195, 1987.

Atwood, C.L. (1980)
Estimators for the Binomial Failure Rate Common Cause Model. Report NUREG/CR-1401, April 1980.

Atwood, C.L. (1983a)
Common Cause Fault Rates for Pumps. Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Plants, January 1, 1972 through September 30, 1980. Report NUREG/CR-2098, February 1983.

Atwood, C.L. (1983b)
Common Cause Fault Rates for Instrumentation and Control Assemblies. Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1978. Report NUREG/CR-2771, February 1983.

Atwood, C.L. (1983c)
Data Analysis Using the Binomial Failure Rate Common Cause Model. Report NUREG/CR-3437, September 1983.

Bengtz, M., Björe, S. and Hirschberg, S. (1986)
NKA Project Risk Analysis (RAS-470), Identification of Common Cause Failure Events for Motor Operated Valves in Swedish Boiling Water Reactor Plants. Final Report RAS-470(86)4 (ABB Atom Report RPA 86-40), January 1986.

Bengtz, M. and Hirschberg, S. (1986)
NKA-project Risk Analysis (RAS-470), Benchmark Exercise, Phase 2: Quantification of Common Cause Failure Contributions. Final Report RAS-470(86)8 (ABB Atom Report RPA 86-160), July 1986.

Bento, J.-P., Björe, S., Ericsson, G., Hasler, A., Lydén, C.-O., Wallin, L., Pörn, K. and Åkerlund, O. (1985)
Reliability Data Book for Components in Swedish Nuclear Power Plants. Prepared by ABB Atom AB and Studsvik AB for Nuclear Safety Board of the Swedish Utilities and Swedish Nuclear Power Inspectorate, May 1985.

Björe, S. and Hirschberg, S. (1985)
NKA-project Risk Analysis (RAS-470), Background Material to CCF-data Benchmark Exercise (in Swedish). Report RAS-470(85)3 (ABB Atom Communication KPA 85-167), September 1985.

Bongartz et al., (1985)
Nutzung ausländischer Betriebserfahrungen zur Ableitung von Zuverlässigkeitskenngrössen - insbesondere für abhängige Ausfälle. Kernforschungsanlage Jülich GmbH, 1985.

Camarinopoulos, L., Kröger. W., Hirschmann, H., Becker, G. and Marx, J. (1986)
Critical Review of Analytical Techniques for Risk Studies in Nuclear Power Stations. CSNI Report 123, Paris, 1986.

Carlsson, L., Hirschberg, S. and Johanson, G. (1987)
Qualitative Review of Probabilistic Safety Assessment Characteristics. PSA '87 - International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Dinsmore, S. (1986)
Common Cause Events Identification from Plant Data. Final Report RAS-470(85)11 (Studsvik Report/NR-85/120), February 1986.

Dinsmore, S., ed. (1985)
PRA Uses and Techniques: A Nordic Perspective. Nordic Liaison Committee for Atomic Energy, June 1985.

Dinsmore S. and Pörn, K. (1986)
CCF Quantification from Plant Data. Final Report RAS-470(86)10 (Studsvik Report/NP-86/72), September 1986.

Ekberg, K., Andersson, M. and Bento, J-P. (1985)
The ATV-system and Its Use. International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, U.S.A., February 24 -March 1, 1985.

Electric Power Research Institute (1981)
German Risk Study - Main Report: A Study of the Risk Due to Accidents in Nuclear Power Plants (Translation from German). Report EPRI NP-1804-SR, April 1981.

Electric Power Research Institute (1982)
ATWS: A Reappraisal, Part 3, Frequency of Anticipated Transients. Report EPRI NP-2230, January 1982.

Electric Power Research Institute (1984)
Oconee PRA - A Probabilistic Risk Assessment of Oconee Unit 3, vol. 1-4. Report NSAC-60, June 1984.

Fleming, K.N. and Kalinowski, A.M. (1983)
An Extension of the Beta Factor Method to Systems with High Levels of Redundancy. Report PLG-0289, August 1983.

Fleming, K.N., Mosleh, A., Acey, D.L., Chapman, J.R., Lydell, B.O.Y., Sattison, M.B., Staub, J., Stillwell, D.W., Wakefield, D.J. (1985)
Classification and Analysis of Reactor Operating Experience Involving Dependent Events. Report PLG-400, EPRI NP-3967, February 1985.

Hennings, W. and Mertens, J. (1985)
Metodische Behandlung abhängiger Ausfälle in Risikostudien. Kernforschungsanlage Jülich GmbH, 1985.

Hirschberg, S. (1985a)
Comparison of Methods for Quantitative Analysis of Common Cause Failures - A Case Study. International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, U.S.A, February 24 -March 1, 1985.

Hirschberg, S. (1985b)
NKA-project 85-89: Risk Analysis - Proposed Technical Content. Report RAS-470(85)1 (ABB Atom Report KPA 85-124), May 1985.

Hirschberg, S. (1985c)
NKA-project Risk Analysis (RAS-470), General Outline of the CCF-data Benchmark Exercise. Report RAS-470(85)4 (ABB Atom Report KPA 85-168), September 1985.

Hirschberg, S. (1986)
NKA-project Risk Analysis (RAS-470), Common Base for CCF-quantification within Benchmark Exercise. Report RAS-470(86)3 (ABB Atom Report RPA 86-41), January 1986.

Hirschberg, S. (1987)
Retrospective Analysis of Dependencies in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. Report RAS-470(87)4 (ABB Atom Report RPC 87-36), July 1987.

Hirschberg, S. (1989)
Treatment of Common Cause Failures. The Nordic Perspective. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-20, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 9-29.

Hirschberg, S., ed. (1987)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report RAS-470(86)14 (ABB Atom Report RPA 86-241), June 1987.

Hirschberg, S. and Bengtz, M. (1987)
Retrospective Analysis of Dependencies and Human Interactions in Swedish PSA-studies. Scandinavian Reliability Engineers Symposium, Helsingør, Denmark, October 5-7, 1987.

Hirschberg, S., Bengtz, M., Dinsmore, S., Petersen, K. E. and Pulkkinen, U. (1987)
Nordic Common Cause Failure Data Benchmark Exercise. PSA '87 -International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

Hirschberg, S. and Knochenhauer, M. (1987)
The Role of Sensitivity Analysis in Probabilistic Safety Assessment. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Hirschberg, S. and Tirén, I. (1989)
Design-related Defensive Measures Against Dependent Failures. ABB Atom's Approach. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-20, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 71-100.

Kongsø, H.E., Martinez, G. and Petersen, K.E. (1986)
NKA Benchmark Exercise on CCF-data. Identification Phase. Final Report RAS-470(85)11, Risø, June 1986.

Kongsø, H.E. and Petersen, K.E. (1986)
NKA-project Risk Analysis, RAS-470, Benchmark Exercise, Phase II, Quantification of Common Cause Failure Contributions. Final Report RAS-470(86)11, Risø, November 1986.

Laakso, K. (1984)
A Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants. Ph.D. Thesis (in Swedish), Helsinki University of Technology, December 1984.

Los Alamos Technical Associates, Inc. (1984)
Common Cause Failures - Phase I: Classification System. EPRI NP-3383, Interim Report, January 1984.

Los Alamos Technical Associates, Inc. (1985)
Common Cause Failures - Phase II: Final Classification System. EPRI NP-3837, Interim Report, June 1985.

Mankamo, T. (1985)
SHACAM, Shared Cause Model. A review of the Multiple Greek Letter Method and a Modified Extension of the Beta-Factor Method. Avaplan Oy, Technical Report, December 1985.

Mankamo, T. and Pulkkinen, U. (1985)
ADDEP - Additive Dependence Model. VTT Research Report, February 1985.

McClymont, A.S. and Poehlman, B.W. (1981)
Loss of Off-site Power at Nuclear Power Plants: Data Analysis. Report EPRI NP-2301, 1981.

Mosleh, A. and Siu, N.O. (1987)
A Multi-parameter Common Cause Failure Model. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

NUS-Corporation (1984)
Ringhals 2 Safety Study. Report NUS-4365, May 1983 (Revised February 1984).

OKG AB (1986)
Oskarshamn 3 Safety Study (in Swedish), 1986.

OKG AB (1987)
Oskarshamn 1 Safety Study (in Swedish), 1987.

Pickard, Lowe and Garrick, Inc. (1983)
Seabrook Station Probabilistic Safety Assessment. Report PLG-0300, 1983.

Poucet, A., Amendola, A. and Cacciabue, P.C. (1987)
CCF-RBE Common Cause Failure Reliability Benchmark Exercise. Report EUR 11054 EN, Ispra Establishement, 1987.

Pulkkinen, U., ed. (1987)
CCF Workshop, Lepolampi, Espoo, Finland, May 10-11, 1984. Report RAS-470(87)14 (VTT Work Report SÄH 38/37), December 1987.

Pulkkinen, U. and Järvinen, J. (1986a)
Identification of Common Cause Failure Events, Phase 1. Final Report RAS-470(86)5 (VTT Work Report SÄH 35/85), March 1986.

Pulkkinen, U. and Järvinen, J. (1986b)
Classification of Common Cause Failure Events, Phase 2. RAS-470(86)6 (VTT Work Report SÄH 10/86), March 1986.

Pulkkinen, U., Järvinen, J. and Huovinen, T. (1986)
Quantification of Common Cause Failure Events, Phase 3. Final Report RAS-470(86)7 (VTT Work Report SÄH 15/86), November 1986.

Pulkkinen, U. and Simola, K. (1987)
A Retrospective Analyis of Dependencies in Five Selected PRAs. Report RAS-470(87)9 (VTT Report SÄH 35/87), December 1987.

Pulkkinen, U., Huovinen, T. and Kuhakoski, K. (1987)
Combination of Several Data Sources. PSA '87 - International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

Pörn, K. (1989)
Some Comments on CCF-quantification, The Experience from the Nordic Benchmark. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 243-256.

Steverson, J.A. and Atwood, C.L. (1982)
Common Cause Fault Rates for Diesel Generators. Estimates Based on Licensee Event Reports at U.S. Nuclear Power Plants 1976-1978. Report NUREG/CR-2099, June 1982.

Steverson, J.A. and Atwood, C.L. (1983)
Common Cause Fault Rates for Valves. Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, 1976-1978. Report NUREG/CR-2770, February 1983.

Swedish State Power Board (1984)
Ringhals 1 Safety Study (in Swedish), October 1983 (Revised August 1984).

Sydkraft (1987)
Barsebäck 1 Safety Study (in Swedish), January 1985 (Revised January 1987).

U.S. Nuclear Regulatory Commission (1975)
Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Report NUREG-75/014 (WASH-1400), 1975.

U.S. Nuclear Regulatory Commission (1983)
PRA Procedures Guide. Report NUREG/CR-2300, January 1983.

U.S. Nuclear Regulatory Commission (1984)
Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant. Report NUREG/CR-3511, 1984.

Vaurio, J.K. (1985)
A Position Paper on Common Cause Failures. Report RAS-470(85)7 (Imatran Voima Oy, Loviisa Power Plant), October 1985.

Westinghouse Electric Corporation (1982)
Sizewell B Probabilistic Safety Study. Report WCAP 9991, 1982.

3. STUDIES OF HUMAN INTERACTIONS

3.1 Overview

Human interactions attract growing attention in the context of safety analysis. They are widely recognized as an important factor when evaluating the reliability and safety of complex industrial facilities such as nuclear power plants. This fact has been reflected in several PSAs, often leading to the conclusion that human errors significantly contribute to the estimated risk level of the plants.

Opposite to the treatment of dependencies the analyses of human interactions in the Swedish PSAs are relatively superficial. The reasons for that will be given later on in the present chapter. Also the research activites in Sweden within the area of probabilistic treatment of man-machine interactions have been rather limited. International progress within this field, including development of a well-structured organisational framework for systematic incorporation of human-hardware interactions into PSAs (Systematic Human Action Reliability Procedure, SHARP (Hannaman and Spurgin, 1984)), has been closely followed.

Studies of human interactions carried out within the RAS-470 project comprise a reference study on a critical operator action (Hirschberg, ed., 1989), and retrospective qualitative analyses of treatment of human interactions in Swedish PSAs (Bengtz and Hirschberg, 1987 and Hirschberg and Bengtz, 1987) and in foreign PSAs (Pyy and Pulkkinen, 1988). In addition, retrospective sensitivity studies of human interactions in Swedish PSAs have been performed. This task will be covered separately in chapter 4 of the present report, which specifically addresses uncertainty aspects.

3.2 Reference Study on Human Interactions

3.2.1 Motivation for a reference study

As concluded in a qualitative review of human interaction analyses in the Swedish PSAs (Bengtz and Hirschberg, 1987; see subchapter 3.3) the attention given to human reliability analysis varies significantly. At the same time,

however, later sensitivity studies demonstrated that human interactions have a major impact on the results of the Swedish PSAs (Hirschberg et al, 1989a; see subchapter 4.3). Of particular interest is manual depressurization, a critical operator action for Forsmark 1, 2, 3, TVO 1, 2 and Oskarshamn 3. The sensitivity aspects for this interaction have been highlighted in (Jacobsson, 1988b). Thus, accident sequences which involve manual depressurization constitute 75% of the total core damage frequency of the PSA for Forsmark 3 (ABB Atom AB, 1985) and 29% in the case of PSA for Oskarshamn 3 (OKG AB, 1986). The analyses of this particular human interaction, carried out within the PSAs, are quite superficial and quantification was based exclusively on engineering judgement.

In view of above a more detailed analysis of manual depressurization was highly motivated.

3.2.2 Objectives, scope and organization of the reference study

The objectives of the reference study were not clearly specified from the beginning. It should be emphasized that the resources allocated to this activity were very limited in view of the associated complexity, i.e. typically 1-2 person-months per group. The study differs significantly from the other Benchmark and Reference Studies performed within the RAS-470 project, both in terms of resources spent and much more loosely defined boundary conditions. Originally, only two working groups (RISØ and STUDSVIK) participated in the study. At that stage the main purpose was to compare the approaches to the problem, to identify factors which have decisive impact on the quantitative results and to investigate the importance of assumptions behind the boundary conditions. Thus, there was no intention to compare in detail models for treatment of human interactions, which was one of the primary objectives of the Human Factors Reliability Benchmark Exercise coordinated by the ISPRA Establishment (Poucet, ed., 1989).

Later on also ATOM and VTT joined the Reference Study on Human Interactions. This was motivated by the needs of the Reference Study on Uncertainty and Sensitvity Analysis (Hirschberg et al., 1989b,c; see subchapter 4.2) which concerned an accident sequence involving manual depressurization. Thus, the contributions of ATOM (Jacobsson, 1988a) and VTT

(Pyy and Pulkkinen, 1988) were from the beginning adjusted to the boundary conditions of the latter study, while STUDSVIK's contribution (Aid, 1987) was supplemented (Aid and Pörn, 1988) and adjusted to the boundary conditions of the first phase of the Reference Study on Uncertainty and Sensitivity Analysis (Hirschberg et al., 1989c). RISØ's contribution (Petersen, 1988) was only used within the Reference Study on Human Interactions described in the present report.

Thus, the results of the first phase of the Reference Study on Uncertainty and Sensitivity Analysis are in the context of manual depressurization more directly comparable than the original ones reported here. The numerical results given in the present report should be regarded with caution having in mind the substantial differences between the different groups with respect to the boundary conditions applied.

Further evolution of the results of analysis of manual depressurization has been described in (Hirschberg et al., 1989b), which covers the second and third phase of the Reference Study on Uncertainty and Sensitivity Analysis.

As indicated above the present description is limited to the review of the original results.

3.2.3 Analysis review

3.2.3.1 Problem description

The study concerns manual depressurization following a loss of feedwater transient combined with the unavailability of the auxiliary feedwater system. Forsmark 3 was chosen as the reference plant for the study. Given the loss of main and auxiliary feedwater systems manual depressurization is a necessary operator action to enable actuation of the low pressure emergency core cooling system. Automatic depressurization can only take place when low water level in the reactor occurs in combination with high pressure in the containment. In the present case only the condition of low reactor water level would be satisfied. The sequence considered contributes 61.4% of the total core damage frequency of Forsmark 3 (ABB Atom AB, 1985).

It is anticipated that the depressurization event might lead to a relatively long shut-down period. This is due to the substantial loads to which the plant structures would be exposed in such a situation and subsequent time and resource consuming procedures involving checks of the affected equipment.

Two cases of interest were analysed by RISØ and STUDSVIK:

1) Two out of four trains in the auxiliary feedwater system retain their operational capability for a period of time after the loss of the main feedwater system.

2) All trains in the auxiliary feedwater systems are lost simultaneously directly after the initiating event occurs.

ATOM's and VTT's analyses cover only the second case which directly corresponds to the assumption made within the PSA for Forsmark 3. This case was also considered later on within the Reference Study on Uncertainty and Sensitivity Analysis (Hirschberg et al., 1989b,c).

3.2.3.2 Course of events

In the case of simultaneous loss of all inflow the consequence is a rapid fall of the water level in the reactor. The control room receives alarms for low water level and information concerning status of the make-up water systems. The water level is continuously indicated by two analog meters and a row of indication lamps in safety panels and by one digital meter in a control desk. Alarms are obtained when the water level reaches the level indicators (L1, L2, L3, L4 etc). The L4-level (0.5 m above the core) is the most important reference for the present application. At this level there are at least 10 alarms activated and the manual depressurization starts given that it was initiated earlier. According to rather simple thermal-hydraulic calculations (Jacobsson, 1988a), it takes approximately 8.5 minutes from the moment the feedwater is lost for the water level to reach L4. The results of these calculations were not known to other teams participating in the reference study at the time the exercise was performed.

If manual depressurization is not initiated at L4, the water level will continue to fall rather rapidly.

In order to initiate manual depressurization the shift personnel must perform two tasks. First to fetch a special key in the Shift Engineer's room. Second to put the key in a key-hole in the control desk and turn it. The depressurization then takes place when the water level reaches L4 or is below it (if the L4-level has already been passed).

3.2.3.3 Common assumptions

Some common assumptions have been adopted by all teams:

- No malfunctions or errors other than those given in the Forsmark 3 PSA analysis of the sequence considered, occur during the scenario.
- The Emergency Operating Procedure DI 3099 (which concerns the case of interest) is available to the operators.
- The control room team consists of one Reactor Operator (RO), one Shift Engineer (SE) and one Turbine Operator (TO). The SE sits in his room at the time of the initiating event. He is expected to arrive at the side of the RO about two minutes after this event. During the course of events the TO is fully occupied with turbine status. Thus, no assistance from the TO in the context of making the decision to initiate manual depressurization, has been credited.

Assumptions concerning success criteria will be treated separately.

3.2.3.4 Approach and analysis characteristics

Simulator exercise

The reference study was initiated by carrying out a simulator exercise at the KSU simulator in Studsvik. Among the working teams only RISØ and STUDSVIK participated in the exercise.

The following simulator runs were performed:

1) A demonstration of the simulation of the accident sequence.
2) Case A, an initial loss of two auxiliary feedwater trains with the remaining two trains still functioning in 8 minutes.
3) Case B, simultaneous loss of all four auxiliary feedwater trains immediately after the transient.

The simulated scenario was not identical with the one chosen as the object for the reference study. The simulated initiating event was loss of external

power (which leads to loss of feedwater) and not loss of feedwater (as defined by transient categories in the PSA-context).

The rate of loss of water in the reactor is somewhat faster in the first case than in the second one (mainly due to a safety valve which remains open in the first case). This means that the time available for diagnosis, decision-making and activation of manual depressurization is shorter, which is expected to affect operator failure probabilities.

The operators succeeded in performing the task within the time available (see below for the discussion of success criteria). Nevertheless the results cannot be applied directly and it is not possible to draw general conclusions from the exercise due to:

- deviations with respect to the scenario being simulated and analysed
- differences of opinion with respect to prevailing success criteria
- the crew consisted of simulator supervisor personnel and not Forsmark 3 operators
- the emergency operating procedures for the event considered were being implemented by simulator runs at the time of the exercise assuring a high degree of familiarity with these procedures
- the instructors had some prior knowledge of the nature of the sequence to be selected for the exercise
- the depressurization key was present in its position in the control desk when the exercise was started, as opposed to the real conditions (see later description)
- since the operators might feel reluctant to perform the action in view of consequences associated with inadvertent performance of depressurization, it is questionable if the stress level in the control room during the exercise is comparable to that in reality.

Therefore, specific conclusions in terms of directly transferable quantitative predictions cannot be drawn from the simulator exercise, but valuable insights concerning the environment during the accident sequence were gained. This regards the information available in the control room, the working procedures of the crew members during the accident sequence, their use of safety instructions and the dynamics of the plant. The benefits of simulator exercises in the context of analysis of human interactions have been highlighted in (Petersen and Aid, 1988).

Success criteria

Since the time available for initiating manual depressurization is expected to have a significant impact on both qualitative and quantitative aspects of the analyses, the discussion of success criteria concentrates on this parameter.

In RISØ's analysis the time to reach L4-level according to the two cases run at the simulator has been chosen as the boundary condition. The disposable times are 16 (RISØ 1) and 7 (RISØ 2) minutes, respectively.

In STUDSVIK's analysis two cases were quantified, both with the simultaneous initial loss of all auxiliary feedwater trains. In the first case the timing conditions of the Forsmark 3 PSA were adopted (30 minutes; STUDSVIK 1), while in the second case the time to reach L4 according to the simulator exercise was used (6.5 minutes; STUDSVIK 2). In addition, the case with delayed loss of the auxiliary feedwater system was analysed qualitatively.

The timing conditions chosen in VTT's analysis have not been specified since the approach to quantification is not explicitly coupled to the disposable time as in the analyses carried out by other teams. In any case the time is assumed to be at least 10 minutes (only one case has been analysed; VTT 1).

According to ATOM's analysis the criterion for activation of the manual depressurization is that it must occur at a point of time when it still can be assured that the low pressure emergency core cooling system will prevent the temperature of the reactor fuel to reach 1204°C. This state is defined as a core damage and is in accordance with PSA-praxis. The core damage does not occur at the L4-level. According to computer calculations based on conservative assumptions (Svensson, 1977), at least 25 minutes are available for activation of manual depressurization from the moment the feedwater is lost. This boundary condition corresponds to the case analysed by ATOM (ATOM 1).

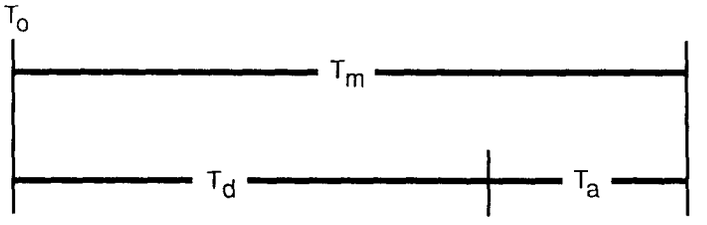
The significant discrepancies between the success criteria applied have naturally large impact on the results of the reference study. The goal of the operators is to initiate manual depressurization before the L4-level is reached (as expressed in the emergency operating procedures). However, from the point of view of core damage more time is available.

Analysis characteristics

The overall logic for analysis of human interactions, as applied by all groups, is shown in Figure 3.1.

The timing aspects of the interaction considered have been recognized by all groups as central in the context of both qualitative and quantitative analysis, although this feature is not as obvious in the VTT-analysis when compared to those of other groups.

Below the time model which has been explicitly used by ATOM, RISØ and STUDSVIK is shown.



T_o = Annunciation (or other compelling signal) of an abnormal event

T_m = Estimated maximum available time to have correctly diagnosed the abnormal event and to have completed the required post-diagnosis actions so as to achieve system success criteria established by systems analysts

T_d = Estimated available time for a correct diagnosis which still permits sufficient time to perform required post-diagnosis actions prior to T_m

T_a = Estimated time needed to get to proper locations and to perform required post-diagnosis actions after a correct diagnosis

Table 3.1 summarizes the timing characteristics of the different cases analysed. Also the corresponding success criteria and other features of the analyses are specified in footnotes to the table.

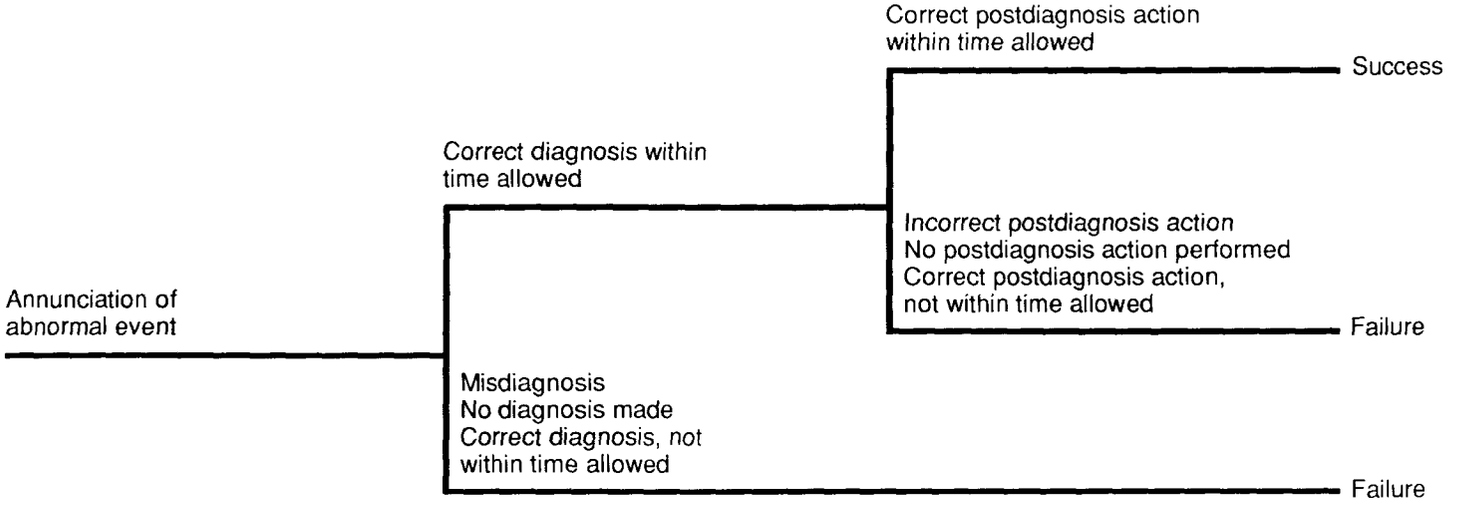


Figure 3.1

The overall logic for analysis of human interactions

Table 3.1

Timing characteristics and analysed cases

Case	Timing Characteristics		
	T_m (min)	T_d (min)	T_a (min)
ATOM 1[a,b,c]	25	8.5 + 11.5 = 20	5
ATOM 2[a,b,c]	25	7.8 + 12.2 = 20	5
ATOM 3[a,b,c]	25	9.2 + 10.8 = 20	5
ATOM 4[a,b,d]	25	20	5
RISØ 1[e,f,g]	16	10	6
RISØ 2[a,f,g]	7	3	4
STUDSVIK 1[a,b,c,h]	30	4 + 23.5 = 27.5	2.5
STUDSVIK 2[a,f,g]	6.5	4	2.5
VTT 1[i]	>10	-	-

[a]Simultaneous loss of all auxiliary feedwater trains

[b]Success criterion based on 1204°C limit

[c]Available time has been divided into time for initial diagnosis and for recovery diagnosis. Different cases in ATOM's analysis correspond to the uncertainty bounds in thermal-hydraulic calculations leading to estimation of the time at which the L4-level will be reached.

[d]No separate recovery modeling (but implicitly included)

[e]Initial loss of two auxiliary feedwater trains with the remaining two trains still functioning in 8 minutes

[f]Success criterion based on the L4-level (corresponds to the requirement expressed in the emergency operating procedure)

[g]Total available time based on the simulator exercise

[h]Available time based on Forsmark 3 PSA

[i]Available time not specified

ATOM's cases 2-4 should be seen as sensitivity analyses. STUDSVIK also analysed qualitatively the situation with delayed loss of the two remaining auxiliary feedwater trains (corresponds to RISØ 1). This case is not included in the table since no quantification has been performed. The assigned timing characteristics were similar to RISØ 1. According to the discussion in STUDSVIK's analysis, given a short available time (applies to the case with success criterion based on the L4-level), the seemingly more forgiving scenario with two trains temporarily available could be more difficult in practice. In this case the operator might be more prone to consider the consequences of manual depressurization (if inadvertent), which would act as a similar stressor as a more stringent limitation of time would have done. Thus, instead of following the procedure he could make a wrong decision as there is a potential for conflict of goals in this situation.

Some comments concerning the available instructions, possibilities for recovery and the nature of the tasks to be carried out after the right decision has been made, are of interest. Conclusive remarks included in these comments may be regarded as a common ground for the analyses performed by different groups, although they do not constitute beforehand agreed boundary conditions.

The instructions for the scenario follow a symptom-oriented and logical-flow-scheme-format. Recovery factors can compensate for a human error and prevent undesirable consequences.

A recovery cue of a misdiagnosis is a lamp in each reactor panel. The lamps start blinking at water level L4 (0.5 m above the core). Other recovery cues are the instruments showing the reactor pressure and the status of the pumps in make-up water systems. Although high pressure and loss of 327-pumps were annunciated earlier, the operator will probably look at these instruments when the L4-tile blinks.

The SE could recover a possible error made by the RO. However, in the context of diagnosis a high dependence between SE och RO would be expected. On the other hand the dependence with respect to the action to get the key should be low.

The key necessary for the initiation of depressurization is stored in a cabinet in the SE room, among more than hundred similar keys. A labeling guide is provided on the front of the transparent doors of the cabinet. Another key can also be used to activate the depressurization condition. The labeling guide does not mention this possibility, nor do the instructions.

Should initiation of depressurization with the dedicated key fail, the depressurization valves can be alternatively, directly manouvered from the safety panels (although the depressurization capacity would probably be reduced). This back-up feature is not mentioned in the instructions, and has not been credited.

A talk-through performed as a part of the analysis revealed that fetching the key from the SE room is not a part of the simulator training exercises. Thus, operators may not be adequately informed and trained in this context. In addition, the labeling problems could be anticipated. The key can easily be mixed up with other similar keys having a different function. Finally, the cabinet location is somewhat hidden (in a corner behind the SE's desk).

Given the above background the approach of the different working groups is described in the following. The analyses carried out by RISØ and STUDSVIK are described first since these teams participated in the reference study from the beginning. For the specification of cases considered by each team we refer to Table 3.1.

In RISØ's analyses the following tasks have been considered:

1) Detection
2) Diagnosis - goal I
3) Functional status
4) Actions - goal I
5) Diagnosis - goal II
6) Actions - goal II

Goal I is success in restoration of main feedwater or auxiliary feedwater systems. Goal II is turning the key allowing depressurization when the water level reaches 0.5 m above the core.

In principle, tasks 2 and 5, and 4 and 6 can be carried out in parallel. According to RISØ due to the high stress level it is more likely that operators will perform the tasks sequentially.

For the purpose of the present reference study RISØ concentrated on tasks 1, 5 and 6, while tasks 2, 3, 4 were considered only in the sense that they would delay and increase complexity of the depressurization task. The operators are facing two goals simultaneously, i.e. restoration of feedwater supply and preparation of depressurization.

The principles of RISØ's qualitative analyses are illustrated by the Operator Action Trees (OATs) given in Figure 3.2. Recovery was credited only in the RISØ 1 case.

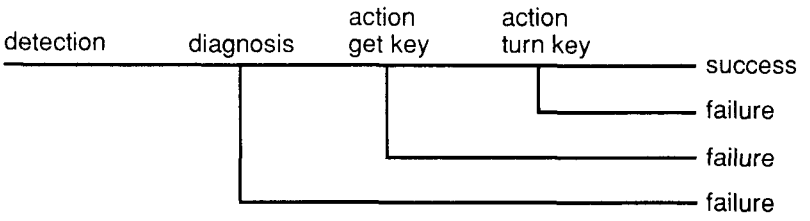
For quantification both the THERP method supported by data from Handbook of Human Reliability (Swain and Guttman, 1983) and the HCR - method (Hannaman et al., 1985), have been used.

For the HCR-application in the RISØ 1 case, where more time is available, a knowledge-based behaviour was assumed for diagnosis, a skill-based behaviour for "turn key" and a rule-based behaviour for the recovery actions. In the RISØ 2 case with less time available a rule-based behaviour was considered as more relevant for diagnosis. No recovery actions were credited.

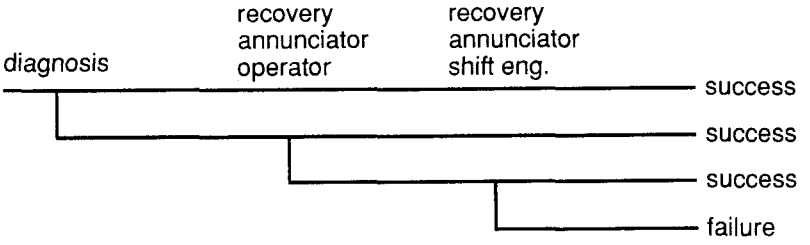
The numerical results are as follows (probabilities per demand):

Case	Task	Method		
		THERP	HCR	
RISØ 1	Misdiagnosis	$6.6 \cdot 10^{-3}$	$4.5 \cdot 10^{-3}$	
	Incorrect action	$8.5 \cdot 10^{-4}$		$(2.6 \cdot 10^{-2})$
	No depressurization	$7.5 \cdot 10^{-3}$	$4.5 \cdot 10^{-3}$	$(3.1 \cdot 10^{-2})$
RISØ 2	Misdiagnosis	$2.5 \cdot 10^{-1}$	$5.5 \cdot 10^{-1}$	
	Incorrect action	$7.9 \cdot 10^{-3}$		$(9.4 \cdot 10^{-1})$
	No depressurization	$2.6 \cdot 10^{-1}$	$5.5 \cdot 10^{-1}$	(1.0)

Main operator tasks



Diagnosis



Actions

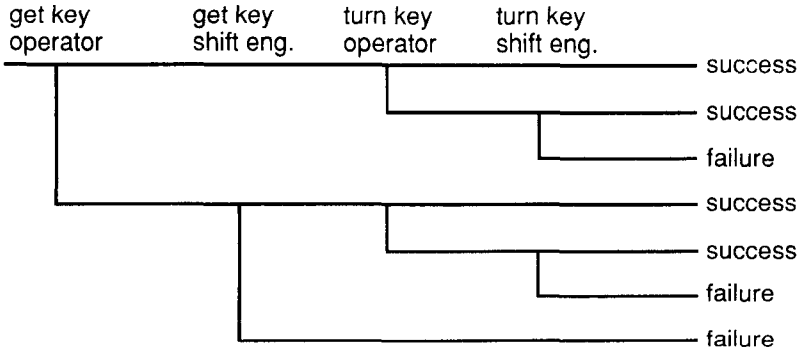


Figure 3.2
RISØ's Operator Action Trees

The probabilities of incorrect actions estimated by means of the HCR-method (given within the parentheses) are obviously not realistic and have been disregarded. Otherwise the agreement between the two methods is quite satisfactory. RISØ's conclusions concerning the features of the two methods used will be reflected in the next chapter.

In STUDSVIK's contribution task analysis sheets were used as a tool for systematic human reliability analysis (example is shown in Table 3.2). This information was later used as a background to construction of OATs. OATs for the STUDSVIK 1 case (including recovery) are shown in Figure 3.3 and an example of worksheets used for assignment of human error probabilities in Table 3.3. Handbook of Human Reliability (Swain and Guttman, 1983), has been used.

The numerical results are as follows (also the results obtained by STUDSVIK for the STUDSVIK 1 and 2 cases, using Monte Carlo simulation to propagate uncertainties, STUDSVIK 1A & 2A, are included; the point estimates are based on median values):

Case	Task	Probability (per demand)	
STUDSVIK 1	Misdiagnosis	$4.0 \cdot 10^{-3}$	
	Incorrect action	$1.1 \cdot 10^{-3}$	
	No depressurization	$5.1 \cdot 10^{-3}$	
STUDSVIK 1A	No depressurization	$6.0 \cdot 10^{-3}$	$(1.9 \cdot 10^{-2})^a$
STUDSVIK 2	Misdiagnosis	$1.5 \cdot 10^{-1}$	
	Incorrect action	$9.3 \cdot 10^{-4}$	
	No depressurization	$1.6 \cdot 10^{-1}$	
STUDSVIK 2A	No depressurization	$1.6 \cdot 10^{-1}$	$(2.4 \cdot 10^{-1})^a$

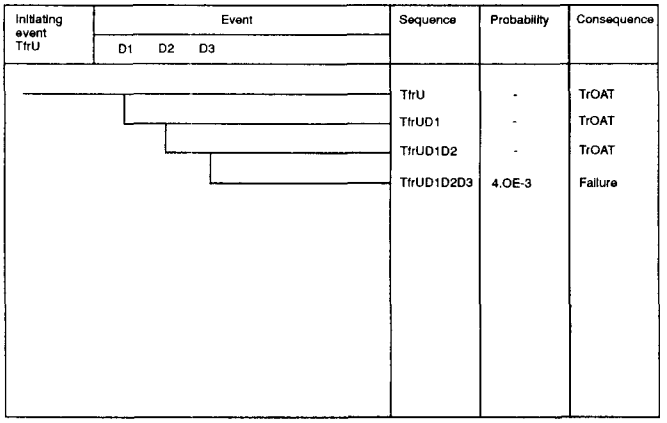
[a]Mean values given within parentheses

Table 3.2

Example of task analysis worksheet (STUDSVIK's contribution)

TASK ANALYSIS					
Step	Instrument/Control	Location	Activity	Activity cue	Remarks
A Reactor water levels L1,L2,L3,and L4	A1 Analog meters	A1 Two meters in panels KAE.102, KCE.102, KBE.102, and KDE.102 respectively	A Check water levels.If levels below stated value special instructions to be followed	A/B/C/D Procedure requires steps to be performed A Many alarms indicate need for the water check. Alarms also provide potential recovery cues	A1/B Distant readouts difficult due to decreased lighting intensity and fairly small instruments. No limit marks for "out of normal" conditions
	A2 Digital meter	A2 One meter in control desk PAE.104			A2 Average of A1-values. Easy readout. 3 red light diod digits. Decimal point after first digit.
	A3 Indicator lamps	A3 A set of four lamps in each panel mentioned in A1. Each lamp dedicated a certain level.			
B Flow of system 327	B Analog meters. Scale: 0-120% of pump capacity.	B One meter in panels KAE.102, KBE.102, KCE.102, and KDE.102 respectively.	B Check 327 flow. If < 40 kg/s special instructions to be followed.	B ANNs for lost flow	B Lamps below meters show pump status (on/off). Off-lamp blinks. Some modes of lost flow would not be indicated by the lamps.
C Reactor water level (< 1m)	C = A1, A2		C If < 1m carry out manually initiated depressureization.		
P Reactor pressure	P1 Analog meter	P1 One meter in panels KAE.102, KCE.102, KBE.102, and KDE.102 respectively.	P Check reactor pressure	P Same as A (exept procedure cue)	P Activity not required by procedure However, relatively high reactor pressure give valueble additional info of the situation.
	P2 Digital meter	P2 One meter in control desk PAE.104			

Diagnosis



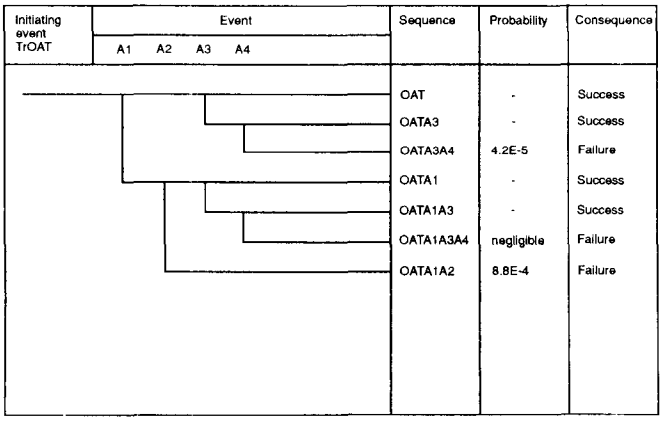
D1 = Misdiagnosis by control room personnel (P(D1) = .15)

D2 = RO fails to respond to recovery ANN cue (P(D2) = .05)

D3 = SE fails to respond to recovery ANN cue (P(D3) = .53)

TrOAT = Transfer to the OAT for carrying out the tasks

Actions



A1 = RO fails to get key (P(A1) = .016)

A2 = SE fails to get key (P(A2) = .065)

A3 = RO fails to activate depressurization condition (PA3) = .0001)

A4 = SE fails to activate depressurization condition (P(A4) = .5)

Figure 3.3

STUDSVIK's Operator Action Trees

Table 3.3

Example of human error probabillity worksheet (STUDSVIK's contribution)

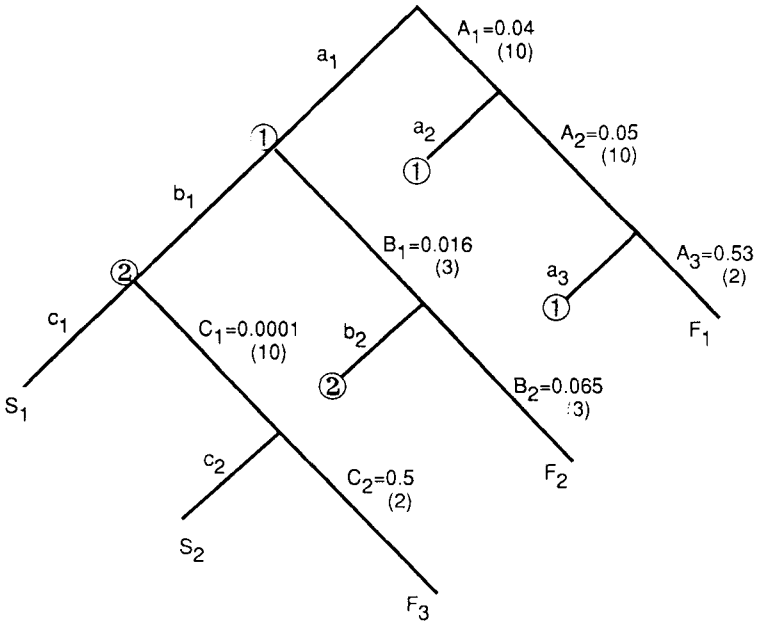
HEP WORKSHEET							
Event	Reference in NUREG/CR-1278	Nominal HEP	Depend./ Stress	Reference to adjusting factors	Adjusted HEP	UCB/EF (Reference)	Remarks
A1	Table 20-13, item (4)	.008	MH	Table 20-16, item (4)	.016	3 [Table 20-13]	No table for this specific application. Action is however judged to correspond fairly well with selection errors for locally operated valves. Tagging level not relevant here since key is assumed not to be used for any test or maintenance operations. Task is considered as procedurally guided. Note! possible ergonomical problems with the present design of the key storage has not been considered due to unsufficient information.
A2	Table 20-17, Eq 10-15	$\frac{(1+19*0.016)}{20}$	LD	-	.065	.023 to .18 [Table 20-21, item (2a) and third footnote]	
A3	Table 20-12, item (8),(5),and third footnote	.0001	0	Table 20-16, item (2)	.0001	10 [Table 20-12, item (5)]	The keyhole is the only one in the control desk.
A4	Table 20-17, Eq 10-17	.5	HD	-	.5	.25 to 1.0 [Table 20-21, item (4a)]	

ATOM's analysis is based on application of THERP methodology and in the base case quite similar to the approach used in the STUDSVIK 1A case. The HRA event tree for the ATOM 1 case is shown in Figure 3.4; Table 3.4 summarizes the basic human error probabilities used in the quantification of the ATOM 1 case. The numerical results follow below (including the results obtained using the Monte Carlo based propagation of uncertainty distributions).

Case	Task	Probability (per demand)	
ATOM 1	Misdiagnosis	$1.1 \cdot 10^{-3}$	
	Incorrect action	$1.1 \cdot 10^{-3}$	
	No depressurization	$2.2 \cdot 10^{-3}$	
ATOM 1A	No depressurization	$3.1 \cdot 10^{-3}$	$(9.1 \cdot 10^{-3})^a$
ATOM 2	No depressurization	$2.4 \cdot 10^{-3}$	
ATOM 2A	No depressurization	$3.4 \cdot 10^{-3}$	$(1.2 \cdot 10^{-2})^a$
ATOM 3	No depressurization	$1.9 \cdot 10^{-3}$	
ATOM 3A	No depressurization	$2.6 \cdot 10^{-3}$	$(6.9 \cdot 10^{-3})^a$
ATOM 4	Misdiagnosis	$3.0 \cdot 10^{-3}$	
	Incorrect action	$1.1 \cdot 10^{-3}$	
	No depressurization	$4.1 \cdot 10^{-3}$	
ATOM 4A	No depressurization	$5.0 \cdot 10^{-3}$	$(9.6 \cdot 10^{-3})^a$

[a]Mean values given within parentheses

Cases 2-4 should be regarded as sensitivity studies.



F_T = Total failure probability = $F_1 + F_2 + F_3 = A_1 \cdot A_2 \cdot A_3 +$

$+ a_1 \cdot B_1 \cdot B_2 + a_1 \cdot b_1 \cdot C_1 \cdot C_2 = A_1 \cdot A_2 \cdot A_3 + (1 - A_1) \cdot B_1 \cdot B_2$

$+ (1 - A_1) \cdot (1 - B_1) \cdot C_1 \cdot C_2$

The values given in the event tree are medians and the numbers within the parantheses are the corresponding error factors.

- A1: Failure of Control Room personnel to make the right initial diagnosis
- A2: Failure of RO to make the right recovery diagnosis
- A3: Failure of SE to make the right recovery diagnosis
- B1: Failure of RO to find the key
- B2: Failure of SE to find the key
- C1: Failure of RO to switch the key in the key-hole
- C2: Failure of SE to switch the key in the key-hole

Figure 3.4

ATOM's HRA event tree (ATOM 1/1A cases)

Table 3.4

Human error probabilities (ATOM 1/1A cases)

Event	HEP	Error Factor	Reference in the "Handbook"	Remarks
A1	0.04	10	fig 12-4 tab 20-3	The event is well-recognized and trained. However an average value of low and median is chosen due to a risk of hesitation in taking the decision to initiate manual depressurization.
A2	0.05	10	tab 20-23	Based on that 10 annunciators alarm when the L4-level is reached.
A3	0.53 $\frac{1 + 0.05}{2}$	3	tab 20-17 tab 20-21	
B1	0.016	3	tab 20-13 tab 20-16	No table available for this application. Analogy with errors for locally operated valves utilized. Tagging level not relevant.
B2	0.065 $\frac{1+19 \cdot 0.016}{2}$	3	tab 20-17 tab 20-21	
C1	0.0001	10	tab 20-12	
C2	0.5	2	tab 20-17 tab 20-21	

The basic principle of VTT's approach is that operators must have goals to behave in a rational way. The most probable course of events and possible errors made by operators can be foreseen by identification of these goals. In this approach the event tree (Figure 3.5) illustrating logical couplings between basic events is supported by a model called the most probable path diagram (Figure 3.6).

The time available for the operators was not explicitly modeled. However, the action probabilities implicitly include time factor. The probability evaluation was based on the absolute probability judgement; the numbers given in the event tree are the expected values of uncertainty distribution. According to VTT such an approach was motivated by the large uncertainties involved. The main goals of the operators are reflected by the head events of the event tree. The following results were obtained (case VTT 1A corresponds to the results generated by Monte Carlo based propagation of uncertainty distributions):

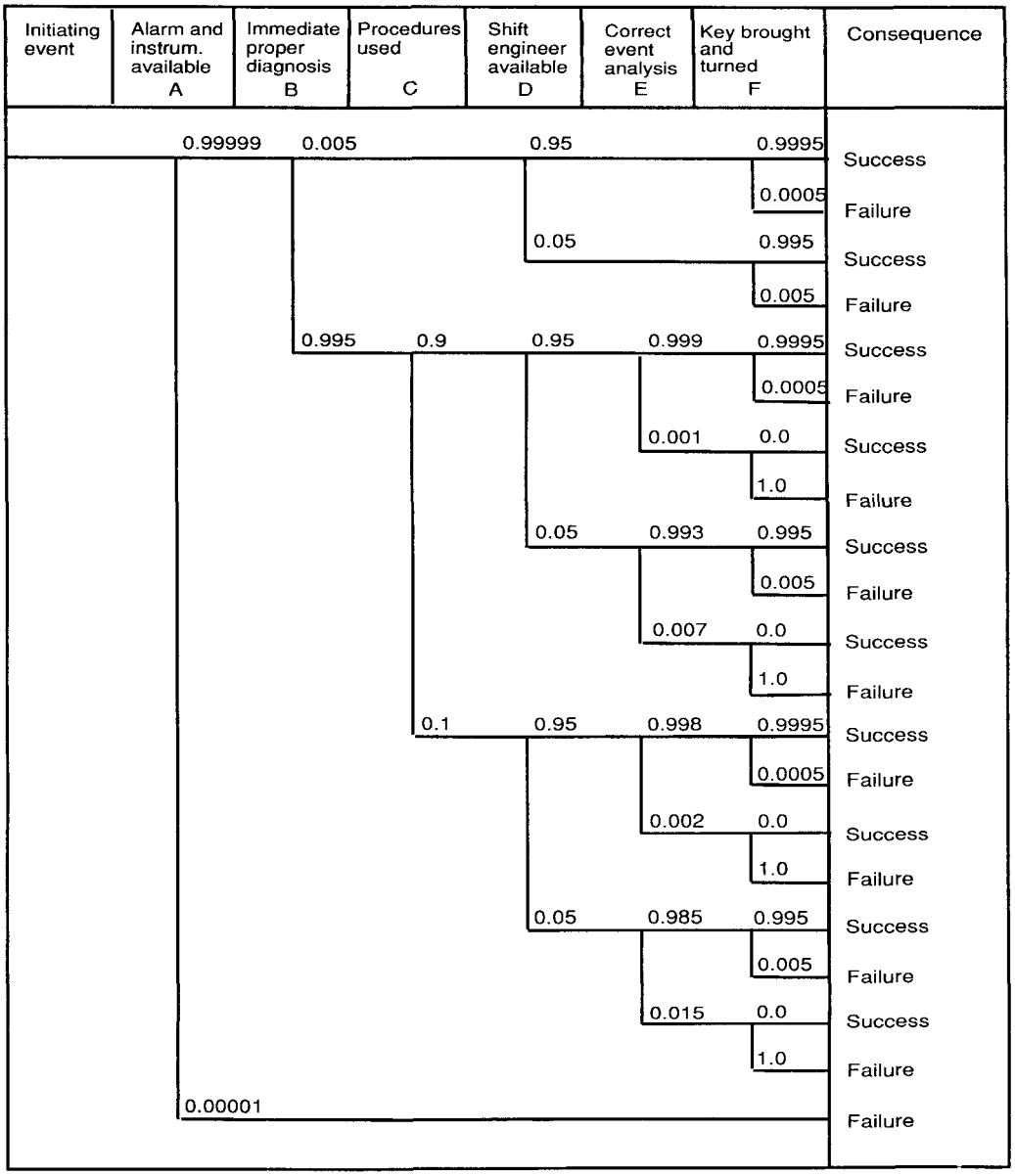


Figure 3.5

The Operator Action Tree (VTT's contribution)

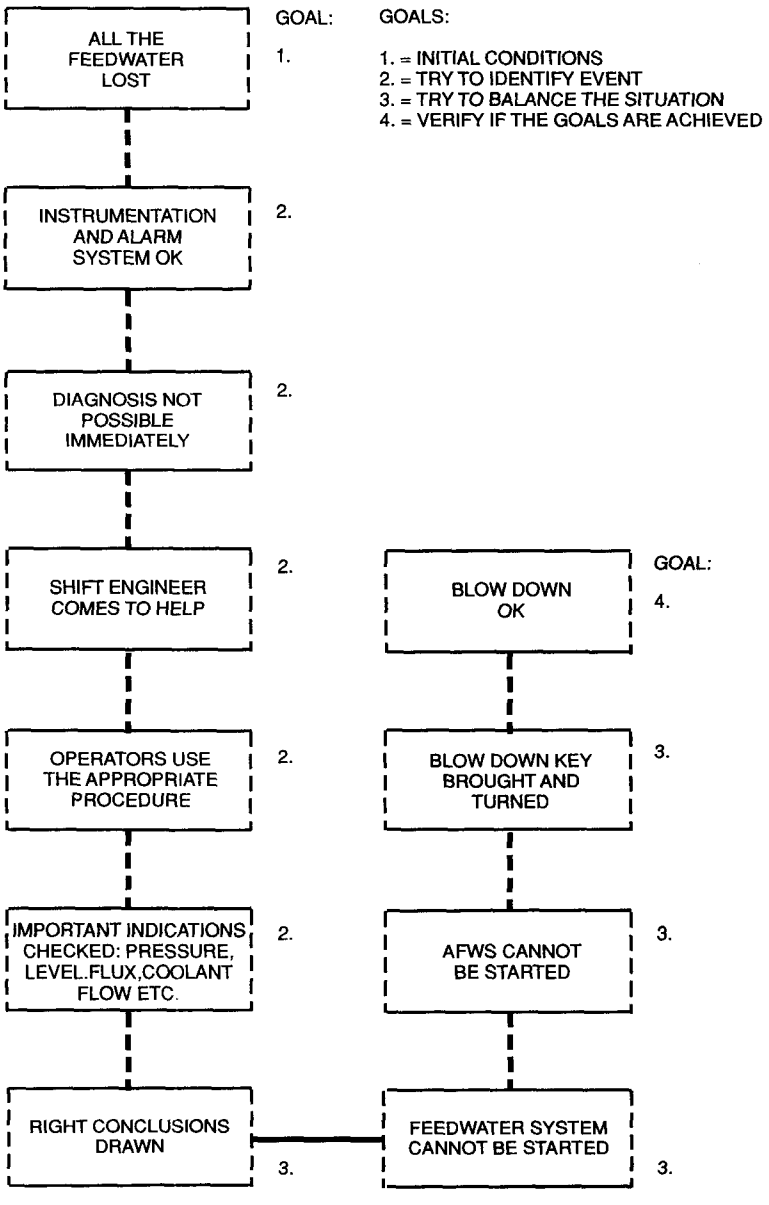


Figure 3.6

The most probable path diagram (VTT's contribution)

Case	Task	Probability (per demand)
VTT 1	Misdiagnosis	$1.5 \cdot 10^{-3}$
	Incorrect action	$7.2 \cdot 10^{-4}$
	No depressurization	$2.3 \cdot 10^{-3}$
VTT 1A	No depressurization	$1.9 \cdot 10^{-3}$ $(2.2 \cdot 10^{-3})^a$

[a]Mean value given within parentheses

Note that misdiagnosis includes all sequences with negative outcome where at the final stage no correct event analysis has been made.

3.2.4 Summary and conclusions

The numerical results of the reference study are shown in Table 3.5. Only the main results obtained by each group are given. Outcome of sensitivity studies is not included in the table. As pointed out all results are not directly comparable. For that reason the results are grouped in the table, i.e. comparisons within each group are possible.

Table 3.5

Main numerical results of the reference study (per demand failure probability of manual depressurization)

Case	Result	
ATOM 1	$2.2 \cdot 10^{-3}$	
STUDSVIK 1	$5.1 \cdot 10^{-3}$	
VTT 1	$2.3 \cdot 10^{-3}$	
ATOM 1A	$3.1 \cdot 10^{-3}$	$(9.1 \cdot 10^{-3})^a$
STUDSVIK 1A	$6.0 \cdot 10^{-3}$	$(1.9 \cdot 10^{-2})^a$
VTT 1A	$1.9 \cdot 10^{-3}$	$(2.2 \cdot 10^{-3})^a$
RISØ 2	$2.6 \cdot 10^{-1}$	$(5.5 \cdot 10^{-1})^b$
STUDSVIK 2	$1.5 \cdot 10^{-1}$	
STUDSVIK 2A	$1.6 \cdot 10^{-1}$	$(2.4 \cdot 10^{-1})^a$
RISØ 1	$7.5 \cdot 10^{-3}$	$(4.5 \cdot 10^{-3})^b$

[a]Mean values given within parentheses

[b]Results obtained using THERP- and HCR-methods, respectively

For comparison the point estimate value used in the Forsmark 3 PSA (ABB Atom AB, 1985) is 10^{-2} per demand.

Given similar boundary conditions the numerical agreement between the groups is quite satisfactory. Misdiagnosis dominates the probability of failure of manual depressurization according to all studies with exception of ATOM's contribution. The main causes for misdiagnosis could be:

- The relatively short time available for diagnosis and possible ambivalence in view of the consequences of the action
- Lack of obvious recovery cues combined with short time available for such a recovery.

These factors call for a serious consideration of substituting manual depressurization by automatic one.

In the context of carrying out the necessary actions given a proper diagnosis, ergonomical improvements can be made with respect to storage of the key; alternatively, the present arrangement could be substituted by a stationary control device. The instructions for manual depressurization and operator training should cover all steps including details regarding the key. Also improvements of the existing instructions could include a more clear definition of the criterion regarding when to initiate manual depressurization.

Three of the teams (ATOM, RISØ and STUDSVIK) used THERP-method combined with data from the Handbook of Human Reliability Analysis (Swain and Guttman, 1983). Thus, the numerical agreement in comparable cases should not be too surprising. The relatively small deviations in such cases may be attributed to differences in assigned timing schemes and to different assumptions concerning the stress level. The assignment of data in the VTT-analysis was purely subjective, at least with respect to absolute probability level.

The THERP- and HCR-based results obtained by RISØ are quite close as far as misdiagnosis is concerned. In this context the HCR-method resulted in higher values than THERP in cases where little time is available. However, the HCR-based predictions of failure probabilities to carry out the task given correct diagnosis are obviously not realistic.

The HCR-method is not well suited in cases where:

- the time required to perform a task is almost equal to the time available; in such cases the probability of failure is close to 1.
- the time required is very short in comparison to the time available; if a task requires 1 minute and some 15 hours are available, the estimated probability of failure would be unrealistically low (of the order of 10^{-40}).

Generally, the importance of clear specification of boundary conditions for the analysis of human interactions must be emphasized. This applies e.g. to the success criteria and to the timing conditions. All boundary conditions should be realistic. The choice of proper boundary conditions is less problematic in the context of a PSA-project.

Qualitative human interaction analyses and studies of related operating experiences should be applied more extensively within PSA-studies.

The simulator exercise proved to be very useful as a source of information concerning the activities in the control room, the working procedures of the crew members and their use of safety instructions. Thus, the operators used a symptom-oriented search and concentrated on parameter control and functional status instead of failure causes. They used primarily the information given on the safety panel in the control room, rather than the information presented on the screen. The reason was that they found it easier to get an overview, to check alternatives, and they felt closer to the equipment itself. Interpretation of the simulator exercise is, however, subject to limitations related to differences in conditions which would be experienced by operators in real accident conditions.

In addition, a simulator exercise must be planned with great care and preferably correspond as close as possible to the conditions being analysed if the findings are to be used directly in the analysis of a specific human interaction.

3.3 Retrospective Qualitative Analysis of Treatment of Human Interactions in Swedish PSAs

Similar to studies of dependencies analyses of human interactions in the Swedish PSAs contain a variety of models, data and assumptions. Thus, it is possible that modeling aspects could explain some of the differences in the results of different studies. This motivates the comparative studies carried out within the RAS-470 project and coordinated with the SUPER-ASAR project (Carlsson et al., 1988) aiming at an overall comparative review of the completed Swedish PSAs.

3.3.1 Scope of work

The scope of work in the present analysis is identical to that concerning retrospective qualitative analyses of dependencies as described in 2.3.1. Thus, the focus is on qualitative aspects while quantitative studies (sensitivity analyses) based on the input from the qualitative phase will be described separately (chapter 4).

The PSAs considered in the present work concern five ABB Atom BWRs (Ringhals 1, Swedish State Power Board, 1984; Barsebäck 1, Sydkraft, 1987; Forsmark 3, ABB Atom AB, 1985; Oskarshamn 3, OKG AB, 1986; and Oskarshamn 1, OKG AB, 1987) and one Westinghouse PWR plant (Ringhals 2, NUS-Corporation, 1984).

For details of the comparative review we refer to the main report (Bengtz and Hirschberg, 1987).

3.3.2 Categories of human interactions

A systematic classification of human interactions is helpful when carrying out the comparative studies. A method-oriented classification has been chosen. Thus, five categories of human interactions were defined (Hannaman and Spurgin, 1984):

Type 1
Before an initiating event, plant personnel can affect availability and safety either by inadvertently disabling equipment during testing or maintenance, or

they can improve the availability of systems by restoring failed equipment through testing and maintenance.

Type 2

By committing some error, plant personnel can initiate an accident.

Type 3

By following procedures during the course of an accident, plant personnel can operate standby equipment that will terminate the accident (errors of omission).

Type 4

Plant personnel, attempting to follow procedures, can make a mistake that aggravates the situation or fails to terminate the accident (errors of commission).

Type 5

By improvising, plant personnel can restore and operate initially unavailable equipment to terminate an accident (recovery actions).

3.3.3 Approaches to modeling of human interactions

The main observations concerning different types of human interactions are summarized in the following.

3.3.3.1 Type 1 interactions

Type 1 interactions concern routine human actions (also referred to as procedural or sequence independent interactions). Test and maintenance activities belong to this group. Routine human actions are normally considered in the systems analysis tasks. The following observations have been made:

1) Preventive maintenance has been modeled only for four-divisional plants (Forsmark 3 and Oskarshamn 3). This is correct with regard to Technical Specifications.

2) In Oskarshamn 3 PSA remedial maintenance for systems which are expected to be subject to preventive maintenance has been modeled separately, while in Forsmark 3 PSA both preventive and remedial maintenance are assumed to be covered by one contribution.

3) Preventive maintenance contributions are divided in different ways between the systems in Forsmark 3 and Oskarshamn 3 PSAs. Since the total contributions are equal this should not have a significant impact on the results from the numerical point of view.

4) Due to consideration of preventive maintenance the fault tree modeling of maintenance contributions is different in the Forsmark 3 and Oskarshamn 3 PSAs on the one hand, and in the other PSAs, on the other hand. While these contributions are modeled on the system train level in F3 and O3 PSAs, they are mainly incorporated on the component level in the other studies.

5) In the Ringhals 1 and 2 PSAs maintenance contributions for valves have been neglected in comparison with the corresponding contributions for pumps. The last mentioned contributions are two orders of magnitude larger in R1 and R2 PSAs when compared to Barsebäck 1 and Oskarshamn 1 PSAs. This implies significant differences between the plants, which may depend on the quality of maintenance or on different ways of calculating these contributions. The maintenance contributions for valves are in the B1 and O1 PSAs of the same order as those for pumps.

6) There are substantial differences in maintenance contributions for diesel generators. Much higher values have been used in the Ringhals 1 and 2 and Forsmark 3 PSAs than in the others.

7) Some inconsistencies have been observed in the maintenance contributions of the Forsmark 3 PSA. The data given in the fault trees do not agree with those present in the original version of the study and do not agree with those actually used in the calculations.

8) The origin of Barsebäck 1 and Oskarshamn 1 maintenance data is not totally clear. They seem to be plant-specific, but this should be verified.

9) Generally, since multiple maintenance outages have been disregarded, differences in quantification of maintenance unavailability contributions are not expected to have significant impact on the results of the Swedish PSAs.

10) In the Ringhals 1 PSA certain misconfigurations with dependency potential have been modeled. The other studies include explicitly several independent misconfigurations.

3.3.3.2 Type 2 interactions

Type 2 interactions are implicitly covered by component failure data and by initiating event (transient) statistics. They are usually in the context of PSA-work not specifically identified as causes of transients. According to a

detailed analysis of reactor scrams at Swedish BWR plants (Laakso, 1984), human errors account for 20 % of all the causes contributing to reactor scrams of Oskarshamn 1 during the period 1971-1982.

With respect to the treatment of Type 2 interactions no differences exist between the Swedish PSAs.

3.3.3.3 Type 3 interactions

Type 3 interactions are often referred to as dynamic human actions. They involve problem solving and are sequence dependent. The actions are taken during an event sequence, thus supplementing the automatic response of plant systems for event mitigation.

In some cases the boarder line between Type 3 and Type 5 interactions may not be totally clear. In the present report we consider intiation of equipment which is functionally unavailable (i.e. the equipment is not damaged but was not available due to failure of automatic signals or latent misconfiguration) as Type 3 interactions.

Table 3.6 shows identified Type 3 interactions in Ringhals 1 PSA (Swedish State Power Board, 1984), including assigned failure probabilities and the basis for the assignments. Similar surveys have been made for identified human interactions of all types in the PSAs being subject of the comparison.

The estimates are not directly comparable, in particular when dynamic interactions are being considered. The range of these values may be very different due to differences in the accident scenarios, available time for recovery (i.e. stress levels), human redundancy (i.e. number of control room operators involved in accident mitigation), potential for misdiagnosis, and other factors of influence (Svensson, 1987). However, given the relative similarity of the Swedish BWRs (mainly with respect to time frames for crucial operator actions and relative simplicity of the models), such comparisons may be made, but the results should not be misused. Figure 3.7 shows the simple basic time-reliability curves/relationships used in the Ringhals 2, Barsebäck 1, Forsmark 3 and Oskarshamn 1 PSAs.

Table 3.6

Type 3 interactions in the Ringhals 1 PSA

Operator action	Failure Probability (per demand)	Source
Failure to initiate system 321 within 4 hours	$1.0 \cdot 10^{-2}$	Situation-specific analysis and engineering judgement (SSA & EJ)
Failure to isolate not used heat exchanger in 322 given failure of 2 of 3 trains in 711 and 322	0.15	SSA & EJ
Failure to initiate 322 P2 given failure of 322 P1 or 322P3	$1.5 \cdot 10^{-4}$	Operator action tree (OAT), EJ & Handbook (Swain and Guttman, 1983)
Failure to open locally 711V25	$1.0 \cdot 10^{-2}$	OAT & EJ & Handbook (Swain and Guttman, 1983)
Failure to start 323 given no automatic start signal	$5.0 \cdot 10^{-3}$	-"-
Failure to partially block inadvertently activated 323-protections	$5.0 \cdot 10^{-3}$	-"-
Failure to manually open 329V4 given wrong central maneuver	$1.0 \cdot 10^{-2}$	SSA & EJ
Failure to start 329 with 342 as source of makeup water	$1.0 \cdot 10^{-2}$	SSA & EJ & Handbook (Swain and Guttman, 1983)
Failure to start 416 given no automatic start signal	$1.0 \cdot 10^{-3}$	-"-
Failure to restart 715 given inadvertent stop signal	$1.0 \cdot 10^{-2}$	OAT & EJ & Handbook (Swain and Guttman, 1983)
Failure to initiate manual reactor shutdown	$3.0 \cdot 10^{-3}$	-"-

Table 3.6 cont.

Operator action	Failure Probability (per demand)	Source
Failure to initiate back-flush operation[a]	$3.0 \cdot 10^{-4}$ (large LOCA)	SSA & EJ & Handbook (Swain and Guttman, 1983)
	$1.4 \cdot 10^{-4}$ (medium and small LOCA)	-"-
Failure to disconnect blocking protections (416)	$1.0 \cdot 10^{-3}$	-"-
Failure to discover indicated failure in system 356 (sequence dependent)	$1.0 \cdot 10^{-6} / 1.0 \cdot 10^{-4}$	SSA & EJ & Handbook (Swain and Guttman, 1983)
Failure to connect 130 kV net within 30 minutes given loss of 400 kV net and loss of more than one diesel generator	$5.0 \cdot 10^{-4}$	OAT & EJ & Handbook (Swain and Guttman, 1983)
Failure to stop feed-water pumps given repletion of reactor pressure vessel	0.33	Statistical evidence
As above plus reactor has been shutdown	0.1	EJ & Handbook (Swain and Guttman, 1983)
Failure to reclose pressure relief valve	$5.0 \cdot 10^{-2}$	OAT & EJ & Handbook (Swain and Guttman, 1983)

[a]Apart from failure to initiate this operation the possibility of errors of commission resulting in blockage of emergency core cooling, has been analysed.

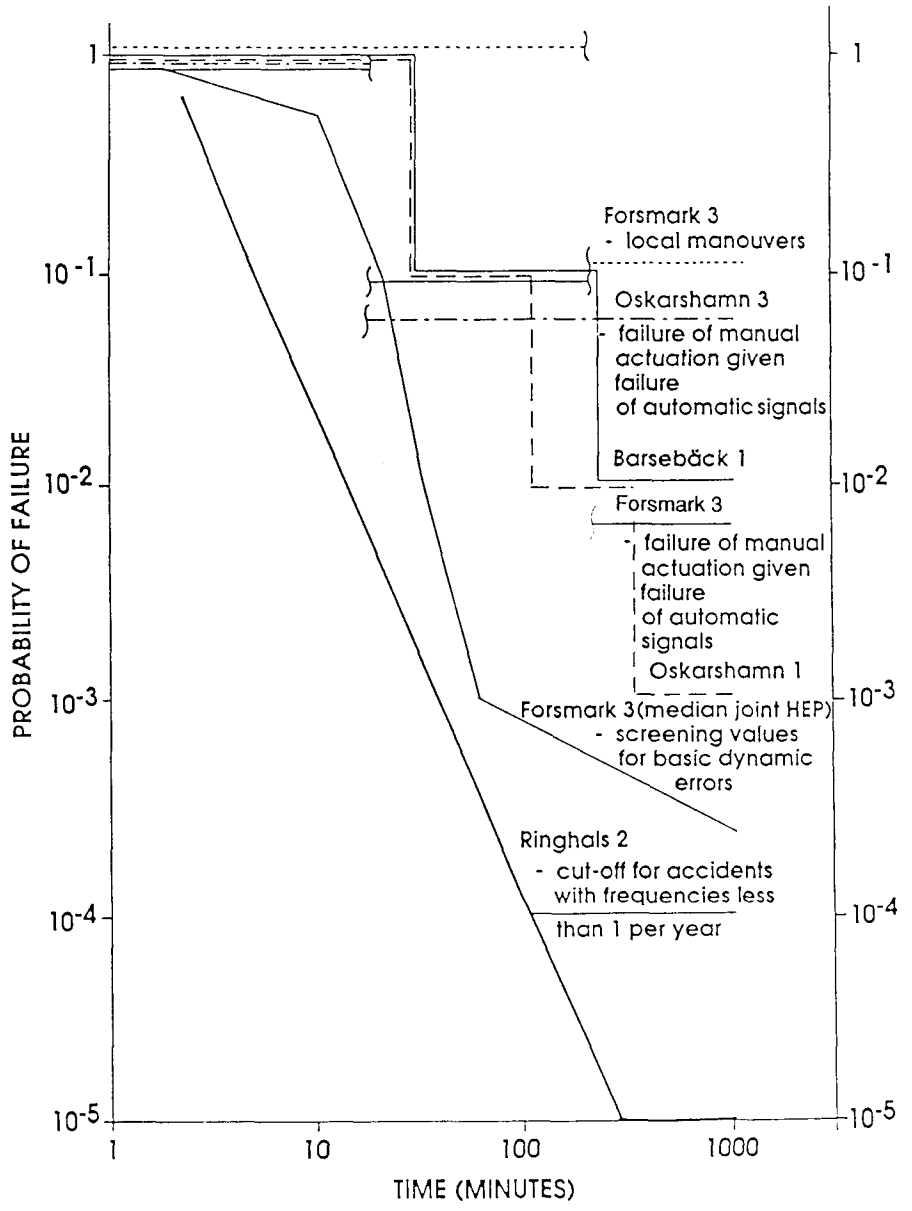


Figure 3.7

Basic time-reliability curves/relationships in some of the Swedish PSA; reservations and comments made in the text should be noted.

Note that:

1) Generally, for many dynamic errors other (usually lower) values have been used.

2) In Forsmark 3 PSA the median initial screening curve has been used as a starting point for a more situation-specific data assignment.

3) The Oskarshamn 3 time-independent model has been applied only to actuation of components from the central control room given no automatic signals. Thus, more situation-specific values have been used in other cases. The breaking point at about 20 minutes should not be interpreted literally. Basically, no operator actions are needed within 30 minutes after the initiating event (some exceptions exist, e.g. manual reactor shutdown given failure of automatic shutdown; for these cases other types of time-reliabiliy relationships are being used). Thus, for the makeup water safety functions at least 0.5 hour is available for operator actions. The reason that the breaking point has been placed at about 20 minutes in the figure is the need of pointing out that according to the relationship used, operator actions are credited for the makeup water safety functions. This is not the case in the Barsebäck 1 and Oskarshamn 1 PSAs.

4) For comparison also schematic relationships used in the Forsmark 3 PSA for local maneuvres, and for manual actuation of components from the central control room, given failure of automatic signals, are shown. The relationship concerning local maneuvres is essentially (for most components and taking into account how the relationships actually were used) identical to that used in the Barsebäck 1 PSA. The remarks given for Oskarshamn 3 and concerning the breaking point at 20 minutes apply here as well. The same kind of reasoning explains the other breaking point at about 230 minutes. In this case it has been taken into account that at least 4 hours are available to actuate residual heat removal systems.

5) The failure probability given in the diagram has sometimes been interpreted differently between the studies and also within the studies. In many cases there is no consequence in this context. Thus the probability may correspond to failure to diagnose the situation properly or to failure of the whole action to be performed (including observation of indications,diagnosis, realisation, and possibilities of recovery). The same reservation applies to the time variable whose meaning is in some cases related to time after an initiating event and in other applications to time after a compelling signal of an abnormal situation.

The span between the values used for similar interactions is very large. In several cases deviations from the prescribed model have not been motivated. Numerical consequences of such differences on the plant damage frequency level will be illustrated in chapter 4.

Some conclusions concerning treatment of Type 3 interactions may be drawn:

1)* "The failure rates for Ringhals 2 operator actions show very little variation between many of the sequences. This observation is not unique for this PSA. To some extent it reflects the difficulty in modelling and quantifying dynamic errors. Analysis efforts are concentrated on a few actions. In the Ringhals 2 PSA all the assessments are based on one time-reliability curve and with little variation in results the implication is that the available time for operator response before the onset of core damage does not vary significantly between the accident sequences. This is contradictory to the findings of other studies. Use of a time-reliability curve (TRC) indeed serves as an analytical aid, and under some conditions it can be a powerful tool. However, it also introduces problems. By reducing the HRA task to referencing error rates in a diagram, any basis for an assessment tends to become obscured, thus making a review process difficult to complete".

"The basis for the Ringhals 2 TRC are three reference points:

- with 10 minutes available for operator action, the operator error probability is estimated to be $1.0 \cdot 10^{-2}$.
- with 30 minutes available, the error probability is $1.4 \cdot 10^{-3}$.
- for a time of 100 minutes, it is $1.0 \cdot 10^{-4}$.

These data points, derived from using expert judgement, represent actions by a team of control room operators".

"A problem with the graph is that it does not provide any explicit information on operator actions that are required within a couple of minutes from the initiating event."

2) The Ringhals 1 analysis of dynamic errors is the most convincing at least from the qualitative point of wiew. All identified important human interactions of Type 3 have been subject to thorough situation-specific analyses based on the plant engineering knowledge. What is most important each case has been thoroughly documented. The documentation given in the study includes both OATs, outline of the data analysis and a survey of all Type 3 interaction data used in the quantification. With view to the failure rates used in the analysis, relatively low values have been assigned to manual reactor shutdown (at least for some of the initiating events) and to back-flush operation.

3) In the Barsebäck 1 PSA all data are based on engineering judgement. The basis and support for the data has not been given, except for a schematic time-reliability relationship which especially in view of the long and extremely positive operating experience of Barsebäck plants seems quite conservative. In several cases other values than that given by the relationship have been used without any explanation at all. In this context inconsequences have been observed, and in several cases information on data which have been used is missing. A survey of operator action data actually used would have helped to make the study more systematic and credible.

---

*With regard to the Ringhals 2 PSA comments given in (Lydell et al., 1984) are reproduced here.

4) The analysis of Forsmark 3 is relatively simple; in most cases credit for operator actions has been taken with caution since no operating experience was available at the time of the study. Screening values from NREP cognitive curve (median HEP) were used as guidance for assignment of Type 3 operator action failure rates in cases where procedures are available. Qualitative arguments have been given as a background to values chosen, but the analysis is relatively superficial and no OATs have been developed. Local maneuvers and actuation of components, given no automatic signals, have been credited in a way similar to Barsebäck 1 and Oskarshamn 1 analyses, the main difference being that credit has been taken for manual actuation also in sequences where time windows are of the order of 30 minutes. A survey of the approach and of the failure rates used, and motivation for their use has been given.

5) No particular time-reliability relationship has been used in the Oskarshamn 3 PSA. For manual actuations, given no automatic signal, a constant (time-independent) relation has been used; in addition the redundant trains have been considered as independent in the context of such manual operations. Both these approaches are contradictory to accepted praxis. The background to some data used is missing in several cases; some qualitative arguments have been given in other cases, but in parallel with the other PSAs (except Ringhals 1) no OATs or other types of detailed studies have been made. Failure probabilities for initiation of the reactor shutdown cooling system are remarkably high.

6) The remarks given for analysis of Type 3 interaction dependencies in the Barsebäck 1 PSA apply also to the Oskarshamn 1 analysis. Based on the documentation given it is difficult to see consistency in the approach. It is not clear to what degree the given time-relability relationship has actually been used when performing quantification. As a matter of fact the identified data only in few cases seem to origin from this relationship. In addition, no consequent distinction has been made between the probability of making wrong decision and the probability of failing to perform the tasks which follow the decision.

7) Only small differences exist between the PSAs for Swedish BWRs with respect to time frames chosen. In all studies it has been acknowledged that in the context of operator actions at least 30 minutes are available for assurance of makeup water safety function and at least 4 hours for assurance of residual heat removal. The conditions are, consequently, favourable from the point of view of manual actions.

8) The common feature of all studies (except Ringhals 1) is that detailed situation-specific analyses have not been performed. In some studies documentation is either missing or is far from complete. Also traceability is a major problem contributing to difficulties to verify the technical adequacy of these studies.

9) The main candidates selected for sensitivity analyses to be performed are:

   - initiation of reactor cooling shutdown system (321) for all plants
   - back-flush operation for Ringhals 1, Barsebäck 1 and Oskarshamn 1.

- manual depressurization for Forsmark 3 and Oskarshamn 3

and

- manual reactor shutdown for all plants.

3.3.3.4 Type 4 interactions

Type 4 interactions can lead to errors of commission which aggravate the situation. Operator mistakes may occur when a situation is misclassified or when inappropriate decisions and response selections are made in the operator action sequences. Methods for treatment of Type 4 interactions are presently being developed.

None of the Swedish PSAs addresses Type 4 interactions. In some cases they are referred to in the documentation of the studies, but they have not been analysed in detail.

3.3.3.5 Type 5 interactions

Crediting for Type 5 interactions affects directly frequencies of accident sequences. Data are usually presented as curves for probability of successful action as a function of time. Expert judgement and information from plant personnel are the basic sources of information. Recoveries are usually not credited for in case of accident sequences which already have low frequency. Given the preliminary results of a PSA it is often concluded that realistic modeling of the dominating accident sequences would require incorporation of recoveries in the model.

Relatively few recoveries have been credited for in the Swedish studies, although some of the Type 3 component-oriented interactions surveyed in the preceding chapter might have been classified as recoveries (manual actuation of components given failure or blockage of automatic signals, and local maneuvers given failure of maneuver power supply).

Table 3.7 summarizes the recoveries identified in different PSAs. Only these recoveries which directly involve manual operations are presented in the table.

Table 3.7

Identified recoveries in the Swedish PSAs

Type of recovery/PSA	Failure Probability (per demand)	Source
Manual restart of feedwater system[a]/		
Ringhals 1		
- within 30 minutes	0.2	QAT & Handbook (Swain and Guttman, 1983)
- within 2 hours	0.01	-"-
Barsebäck 1	0.1[b]	not clear
Forsmark 3		
- within 30 minutes	1.0	Detailed situation-specific analysis (SSA) and engineering judgement (EJ)
- within 4 hours		
- after loss of feedwater	0.5	-"-
- other transient	0.1	-"-
Oskarshamn 3		
- within 4 hours		
- after loss of offsite power	0.3	Engineering judgement (EJ)
- after loss of feedwater	0.1	-"-
Manual connection of system 711 to 321 pump given loss of 712-cooling/		
Ringhals 1	0.25	QAT & Handbook (Swain and Guttman, 1983)
Use of makeup water from fire system (to 323; within 4 hours)/		
Ringhals 1	0.01	SSA
Repair of containment cooling spray system (322)/		
Oskarshman 3 (within 4 hours)	0.05/0.1/0.5/0.9[c]	SSA

[a] Whenever appropriate given recovery of offsite power

[b] Time window not specified

[c] Sequence dependent

No recoveries with manual actions have been identified in the Oskarshamn 1 and Ringhals 2 PSAs. In the Oskarshamn 1 PSA, however, it has been shown that the boron injection system could be used as a source of makeup water after transients, if the system is started not later than 10 minutes after scram. This was not credited in the probabilistic analysis.

We may conclude that crediting for recoveries in the Swedish PSAs has not been a major issue. The comments in the preceeding section with regard to analysis of Type 3 interactions apply by and large also to the analysis of recoveries. One exception is the Forsmark 3 PSA, where a much more detailed (in comparison to the rather superficial analysis of Type 3 interactions in the same study) analysis of feedwater system recovery has been made.

Among recoveries the main candidate for sensitivity studies is repair of the containment cooling spray system. However, the possibilities of this recovery should be discussed in a more detailed way. Also the restart of feedwater system is of interest in this context since the numerical differences between the probabilities may in some cases have significant impact on the results of the studies.

3.3.3.6 Human interaction dependencies

Several human interaction dependencies have already been mentioned when accounting for Type 1, 3 and 5 interactions.

Four types of human interactions which may involve some potential for dependencies have been modeled in all examined PSAs:

1) Maintenance and test outages.
2) Manual actuation signals to objects in case of no automatic signal (only few cases occur in Ringhals 1 study).
3) Initiation of safety systems.
4) Misconfiguration of components in redundant trains.

In the Forsmark 3 PSA also local manual actuation of components has been modeled.

Below the main principles for treatment of the dependencies initiated by human interactions are summarized:

1) Test and maintenance activities are represented in the fault trees. The potential for simultaneous multiple failures in form of maintenance outages is judged to be low. Residual common cause failure contributions are considered to cover such errors.

2) Manual actuation of different components in different trains of the same system has been coded in the system fault trees as a common event (strong coupling). The only exception is the Oskarshamn 3 study where such events are treated as independent both between the trains and individual objects. This assumption is not realistic, but as indicated by a sensitivity study probably does not have a significant impact on the results of the study.

3) The essential operator actions have been modeled either in the event trees, in the fault trees or in both. Usually, operator actions considered as critical for propagation of accident sequences, i.e. operator actions which have impact on functional intersystem dependencies, are represented in event trees. In some studies (Ringhals 1, Ringhals 2) the manual initiation of safety systems and other complex operator actions during accident conditions have been divided into four (three for Ringhals 2) states: observation of indication, diagnosis of the nature of the event and identification of necessary responses, implementation of responses, recovery measures. These states have been modeled and analysed using the operator-action trees. In principle, a similar approach has been used in the Barsebäck 1 and Forsmark 3 studies, although no operator-action trees have been used and the level of detail in the analysis is rather superficial. Naturally, failure to diagnose the nature of the event is equivalent with no responses being carried out. The principles for treatment of dependency aspects of operator actions in the Oskarshamn 1 and Oskarshamn 3 PSAs are not accounted for in the available documentation.

4) None of the studies models explicitly systematic misconfiguration of redundant components (some MOVs in the Ringhals 2 PSA and two case studies in the Ringhals 1 PSA are exceptions). As shown in the sensitivity analysis in the Forsmark 3 PSA only marginal contributions are expected from such potential dependencies. This statement may not be relevant for plants characterized by lower level of redundancy and separation.

5) None of the PSAs systematically addresses errors of commission which obviously may introduce complex dependencies and may have critical impact on accident propagation. One case involving an error of commission in the context of back-flush operation has been considered in the Ringhals 1 PSA.

6) Systematic calibration errors are usually handled through residual CCF-contributions.

7) With the exception of Ringhals 1 and 2 PSAs none of the PSAs accounts for the question of dependencies between operators, which usually is one of the subjects of concern in U.S.-studies. In Ringhals 1 and 2 PSAs this issue is treated implicitly.

It may be concluded that human interaction dependencies are not treated in detail in the Swedish PSAs. Ringhals 1 PSA is an exception in this respect, since the basic human factors analysis in this study is rather comprehensive. However, even for Ringhals 1 PSA the need of supplementary analysis should be considered - in particular a study of errors of commission.

3.3.4 Impact of human interactions on dominant accident sequences

Table 3.8 provides an example of the impact of human interactions in one of the PSAs considered. Similar tables have been generated for the other PSAs by scrutiny of the cut-set lists.

Human interactions have relatively strong impact on the results of the studies. Thus, the contribution to the total core damage frequency from human errors (interactions of Type 1 and 3) is approximately 14% in the Ringhals 1 PSA, 46% in the Barsebäck 1 PSA, 60% in the Ringhals 2 PSA and 88% in the Forsmark 3 PSA. The discrepancy between the Ringhals 1 and Barsebäck 1 contributions is mainly due to large differences in data used for quantification of operator errors during back-flush operation. In the Oskarshamn 1 PSA it is claimed that the contribution from human errors is small. The picture would be different if pipe break probabilities from other studies had been used and if back-flush operations had been required. It is interesting to note that human interactions also have substantial impact on the results obtained for plants with high degree of redundancy and separation (Forsmark 3 and Oskarshamn 3). Naturally, the probability of systematic Type 1 failures leading to core damage is, however, quite insignificant for such plants. The dominating Type 3 interaction is failure of manual depressurization in loss of feedwater transient accident sequences. Modification of the actuation signal logic of the pressure relief system is presently being discussed. This could lead to substantial reduction of the total core damage frequency (see subchapter 4.2). A special feature of the Oskarshamn 3 PSA is that rather extensive credit has been taken for recoveries.

Table 3.8

Impact of human interactions (HIs) on dominant accident sequences of the Forsmark 3 PSA (ABB Atom AB, 1985).

Accident sequence	Sequence frequency (per year)	HIs represented in cut-set no.(among top ten)	Principal HI-contributor(s) and failure probability	Total importance of HIs (%)
T_fUX2	$4.3 \cdot 10^{-6}$	All	Manual depressurization; 0.01	100
Q_1W1W2	$6.2 \cdot 10^{-7}$	1,2,6,10	Maintenance 331; 0.002 Restart 331; 0.01 Start 321; 0.01	62
T_eQUX2	$6.0 \cdot 10^{-7}$	All	Manual depressurization; 0.01	100
T_fUV	$3.1 \cdot 10^{-7}$	1,3,6,7	Manual start 323 or 327; 0.1 and 0.1, respectively	86
$Q_1Q1UX23$	$2.8 \cdot 10^{-7}$	All	Manual depressurization; 0.001 ($t \geq 2h$)	100
R	$2.7 \cdot 10^{-7}$	-	-	0
Q_1Q1UV	$2.0 \cdot 10^{-7}$	1,3,6,7	Manual depressurization; 0.01	86
T_eQUV	$1.4 \cdot 10^{-7}$	2,3,4,6,7,10	Manual start 323 or 327; 0.1 and 0.1, respectively	31
$T_{ms}QUX2$	$6.0 \cdot 10^{-8}$	All	Manual depressurization; 0.01	100
T_tC3C4	$5.8 \cdot 10^{-8}$	-	-	0

3.3.5 Conclusions and recommendations

A wide spectrum of differences has been observed between human interaction analyses performed within the Swedish PSAs. These differences concern level of ambition, approach to modeling and quantification, and documentation of the studies. The attention given to human reliability analysis in the studies varies significantly with Ringhals 1 PSA being the only example of detailed treatment. This is in contrast with the relatively detailed modeling of dependencies and common cause failures in the Swedish PSAs.

Some possible reasons for not giving the highest priority to modeling of human interactions in the current Swedish PSAs may be as follows:

1) It was rather natural to concentrate on hardware functions, at least in the first generation of Swedish PSAs. Treatment of hardware reliability is not a controversial subject and is supported by the Swedish data base of high quality and by relatively long operating experience. The results concerning hardware performance are considered as more credible and have in several cases led to plant modifications.

2) For the Swedish BWRs there are rather few critical operator actions during accident conditions and plant operators have extensive experience from handling such situations in simulator exercises. Another important factor is the so called "30 minute's rule" valid for all ABB Atom BWRs. With few exceptions 30 minutes are available to the operators after an initiating event, before manual actions become necessary. For all Swedish BWRs at least 4 hours are available to assure proper function of the residual heat removal systems. Thus, the issue of time windows for operator actions is relatively simple.

3) The methods for efficient treatment of human interactions are presently being developed, are not well established, and the experience of their application is still very limited. All the Swedish PSAs have been generated in a relatively short period of time and there has been no time to incorporate the latest findings within the studies.

Thus, the limitations of the human interaction analyses have in most cases been prescribed by the intended scope of PSAs. On the other hand, the available documentation seldom reflects the constraints imposed by the limitations in scope. The human error studies rely heavily on subjective judgement which underlines the need of comprehensive documentation. Only in the Ringhals 1 PSA a systematic approach to dynamic operator interactions, which included consideration of applicable procedures, of available

instrumentation and alarms, of time available for operator response, and modeling of the assumed scenarios, has been consequently applied and documented.

The Ringhals 2 PSA refers frequently to a similar type of approach but no account for actual situation-specific modeling of human interactions is to be found in the study. The other PSAs apply rather superficial methodology to modeling of dynamic operator errors. The differences in these cases are in the first place related to the consistency in application of simple models, traceability of information and to presence or lack of arguments motivating choice of failure rates assigned to operator actions.

All studies (except Ringhals 1) use one or other form of time-reliability relationship. The span between the values used for very similar interactions is very large. In several cases deviations from the prescribed model have not been motivated. Apart from using the time-reliability curves more or less frequent references are made in all studies to the Handbook (Swain and Guttman, 1983), especially in the context of carrying out simple tasks given right decision.

Relatively small differences exist between the studies with respect to the treatment of Type 1 interactions. The approach is rather straight-forward and does not require any special models, at least as far as independent failures are concerned. The observed discrepancies mainly concern scope of the analysis. Potential dependencies are considered being covered by residual CCF-contributions.

Only few recoveries have been modeled in the studies. Relatively most credit for restoring unavailable safety system functions has been taken in the Oskarshamn 3 PSA.

The principal human interactions contributing to the dominating accident sequences in BWRs involve:

- failure to initiate depressurization of the reactor pressure vessel after transients with loss of ordinary and auxiliary feedwater systems (Forsmark 3, Oskarshamn 3)
- failure to carry out back-flushing of screens in the emergency core cooling system after large or medium LOCA (Barsebäck 1, Oskarshamn 1, Ringhals 1),

and for the only one PWR analysed (Ringhals 2), failure to depressurize and failure to switch to high-head recirculation after small LOCA (some other operator actions have, however, only a slightly smaller importance).

It is interesting to note that for BWRs the principal operator action contributing to core damage frequency occurs in two cases in transient sequences and in two cases in LOCA sequences. The back-flush operation has relatively larger impact in the Barsebäck 1 PSA than in Ringhals 1 PSA, which is mainly attributed to the differences in the assignment of failure data for that operation.

The characteristics of the HRAs of Swedish PSAs are also summarized in Table 3.9.

Based on the conclusions of this study some recommendations may be made, concerning:

1) Quantitative analyses (sensitivity studies)

2) Future research projects within the field of human interactions

3) Possible improvements of existing analyses.

The recommendations given here are to some degree overlapping with those given in the qualitative retrospective analysis of dependencies in the Swedish PSAs (subchapter 2.3). This is natural since dependency aspects of human interactions have the greatest potential to give significant impact on the results.

The sensitivity studies were proposed to address the following problems:

1) Miscalibration in the context of reactor protection function and reactor shutdown function.

2) Systematic component misconfiguration; it is only partially true that the residual CCF-contributions cover such dependency since CCFs have been modeled only for selected component types and not for manual valves.

3) Type 3 interactions such as:

- connection of reactor cooling shutdown system (321) for all BWR-plants
- back-flush operation for Ringhals 1, Barsebäck 1 and Oskarshamn 1

Table 3.9

Treatment of human interactions in Swedish PSAs

Topic	PSA						Comment
	RINGHALS 1	RINGHALS 2	BARSEBÄCK 1	FORSMARK 3	OSKARSHAMN 3	OSKARSHAMN 1	
DEGREE OF COVERAGE (ANALYSED TYPES OF INTERACTIONS)							
TYPE 1							
	Covered by fault trees (FT)	Covered by FT	Covered by FT	Covered by FT	Covered by FT	Covered by FT	For more details see 3.3.3
- Maintenance	Remedial	Remedial	Remedial	Preventive and remedial	Preventive and remedial	Remedial	Test contributions usually negligible.
o Components considered	Only for pumps and diesel generators	Pumps, diesel generators and system 416	Major components	Safety function trains	Safety function trains	Major components/systems	Some inconsistencies discovered in Forsmark 3 PSA.
o Source of data	Mainly Ringhals 1 (R1)	Mainly Ringhals 2 (R2)	Mainly Barsebäck 1 (B1)	TS & ATV	Mainly TS	Oskarshamn 1 (O1)	The origin of B1 & O1 data not totally clear
- Procedural Errors							
o Miscalibration	Modeled	Modeled	Modeled	Only systematic	Modeled	Modeled	
o Source of data	ATV (R1 & R2),	ATV (R1 & R2) Handbook	Handbook	Handbook	Handbook	Engineering judgement	
o Misconfiguration	Valves	Only systematic	Valves	Manual valves	Valves	Valves	
o Source of data	Basically U.S.-generic	Engineering judgement	Handbook and engineering judgement	Handbook and engineering judgement	Engineering judgement and Seabrook PSA	Engineering judgement	
- Systematic	Covered by residual CCFs	CCFs	CCFs	CCFs	CCFs	CCFs	Low potential for multiple maintenance outages.

Table 3.9 cont.

Topic	PSA						Comment
	RINGHALS 1	RINGHALS 2	BARSEBÄCK 1	FORSMARK 3	OSKARSHAMN 3	OSKARSHAMN 1	
TYPE 2	Covered by transients statistics	Covered by transients statistics	Covered by transients statistics	Covered by transients statistics	Covered by transients statistics	Covered by transients statistics	
TYPE 3	Covered by fault trees (FT) and event trees (ET)	FT & ET	FT & ET	FT & ET	FT & ET	FT & ET	For more details see 3.3.3
- Basic Approach	Operator action trees (OAT)	OAT-principles (no OATs accounted for)	Case-by-case	OAT-principles (no OATs developed)	Case-by-case	Case-by-case	
- Source of data	Situation-specific analysis, Handbook, engineering judgement	Time-reliability curve (TRC; NUS control room team)	Time reliability relationship (assumed), Handbook, engineering judgement	NREP cognitive error screening curve, time reliability relationship (assumed) Ringhals 1 PSA, engineering judgement	Engineering judgement, time independent probability (in some cases)	Time-reliability relationship (assumed), engineering judgement	Inconsistencies discovered in Barsebäck 1, Oskarshamn 1 and Oskarshamn 3 PSAs
TYPE 4	Not covered	Not covered	Not covered	Not covered	Not covered	Not covered	Inadvertent signals sometimes modelled
TYPE 5	Covered	Not identified	Covered	Covered	Covered	Not identified (except a deterministic study of a special case)	For more details see 3.3.3
- Basic Approach	See Type 3 interactions	-	See Type 3 interactions	Detailed qualitative analysis	Engineering judgement	-	Very few recoveries have been modeled

Table 3.9 cont.

Topic	PSA						Comment
	RINGHALS 1	RINGHALS 2	BARSEBÄCK 1	FORSMARK 3	OSKARSHAMN 3	OSKARSHAMN 1	
SENSITIVITY STUDY	No	Yes, impact of different assumptions about TRC	One case analysed (non-dominant)	Yes, principal contributor, main recovery and manual scram analysed	Yes, principal contributor and main recovery analysed	One case analysed	
IMPACT OF OPERATOR ERRORS							
- Global (on core melt frequency)	14%	60%	46%	88%	High (not specified)	Relatively small (not specified)	
- Principal Contributors	Back-flush operation	Failure to depressurize and failure to switch to high-head recirculation	Back-flush operation	Manual depressurization	Manual depressurization	Not apparent	Given similar assumptions for the analysis, back-flush operation would be a principal contributor also for Oskarshamn 1
DOCUMENTATION	Detailed and informative	Detailed with regard to approach; no applications included	Very brief and not clear	Systematic description of approach, data and detailed account for credited recoveries	Brief, data given in sequence descriptions	Very brief, background not given	

- impact of not taking credit for manual reactor shutdown
- manual depressurization in view of the findings of reference study performed within this project.

4) Type 5 interactions such as:

- repair of the containment cooling spray system including support for such recovery
- restart of feedwater system.

It is natural that after implementation of hardware improvements more attention is presently being given to the man-machine interactions. Possible areas of interest for Nordic research projects could be:

1) Study of errors of commission including a theoretical part and application to one of the plants (preferably Ringhals 1).

2) Comparisons with international experience; this would give a better perspective on the approach used in the Swedish studies.

3) Consequent application of SHARP-methodology in a pilot study.

4) Model studies aiming at systematic use and interpretation of simulator experiments.

5) Systematic search for human errors based on Swedish operational experience.

6) Systematic studies of possible non-credited recoveries and their impact on PSA-results.

7) Integration of reliability models, engineering judgement and operating experience with cognitive psychology.

It is expected that future projects will benefit from the experience of plant personnel and specialists in control room design. Hopefully, a more constructive dialogue will be initiated between the technical experts and behavioural scientists.

Basically all aspects of human interaction analysis in the Swedish PSAs can be improved. Main improvements would involve:

1) Situation-specific studies of identified principal contributors.

2) More systematic documentation of analyses performed.

3) Use of methods and data which better reflect state-of-the-art.

3.4 Retrospective Qualitative Comparisons of Treatment of Human Interactions in Foreign PSAs

3.4.1 General remarks

For the qualitative comparisons of foreign PSAs, five studies were selected. The studies are: Oconee (Electric Power Research Institute, 1984), Seabrook (Pickard, Lowe and Garrick Inc., 1983), Calvert Cliffs (U.S. Nuclear Regulatory Commission, 1984), Sizewell B (Westinghouse Electric Corporation, 1982) and Biblis B (Electric Power Research Institute, 1981) PSAs. In each study, the overall framework is quite similar. Event trees are used to model accident sequences and fault trees to represent system failures of interest as identified in the event trees. The extent to which these models are used varies. The goal of human error analysis is usually to enhance the completeness of plant models. In the Oconee and Seabrook cases the flow chart of the analysis is well documented. The flow diagram of the Oconee analysis is shown in Figure 3.8.

As shown in the figure, the principal objective is to assess human contribution to core damage frequency by synthesizing system analysis, human factors and operating experiences. The phases are described further in the following. The Oconee analysis mainly follows the ideas presented in the Systematic Human Action Reliability Procedure (SHARP; Hannaman and Spurgin, 1984).

The objective of the Seabrook human actions analysis was to make the event sequence diagrams more complete. Routine human interactions are treated in the system analysis, dynamic actions are analysed in the human actions analysis and residual human contribution is taken implicitly into account in initiating event frequencies, component failure rates and common cause failure parameters.

The level of the documentation of human actions analysis varies significantly from one study to another. Here, the Oconnee and Seabrook documents are the most detailed ones when compared with the other studies. Also the Calvert Cliffs material included some detailed information on the incorporation of human errors. In the remaining two PSAs only a very limited amount of information could be found.

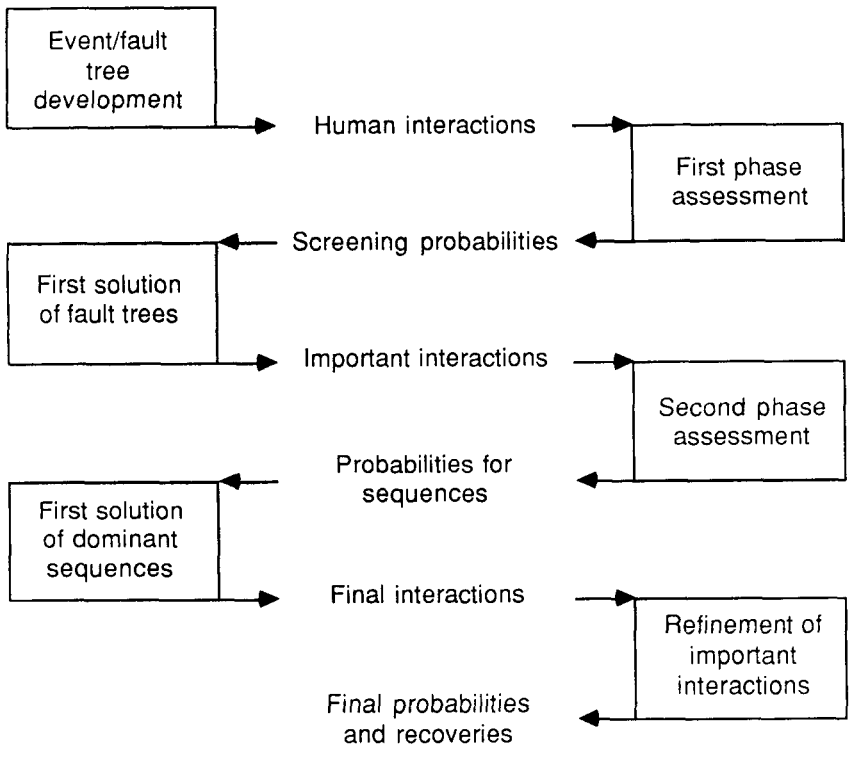


Figure 3.8.
Process diagram for the Oconee human reliability analysis

Lack of comprehensive documentation induces difficulties into the retrospective analysis and affects the quality of the comparisons. Despite the deficient reporting follwing areas were investigated:

- Scope and limitation of the studies
- Treatment of psychological aspects
- Identification of significant human activities
- Classification of human errors
- Modeling of man-machine interface
- Sources of human error data
- The impact of human behaviour on core damage frequencies
- Uncertainties.

Detailed comparison of human error probability estimates is left outside the consideration since the estimates are normally subjective and the quality of documentation would introduce bias in the results.

3.4.2 Scopes of the studies

The scopes of the studies are important when the results are interpreted. In the German Risk Study errors of omission were included but errors of commission excluded.

In Calvert Cliffs PSA, errors of commission were also included in a limited way. For components found to require active manipulation such errors were taken under closer investigation. Here, operating procedures were utilized. Errors of omission were included in the models. As for test and maintenance, only restoration errors were modeled explicitly in the fault trees.

In Seabrook PSA, most of the limitations concern the review of event sequence diagrams and the evaluation of the impact of psychological factors. Here, simulator runs were used extensively, but the operators participating were only prospective Seabrook operators, who had not received any plant-specific simulator training until then. Besides, all the operating instructions were drafts and the simulator was not yet perfect especially with respect to the steam generator part.

The Oconee Risk Assessment clearly declares all the limitations, e.g. simplicity of taxonomies and lack of data concerning human reliability. This can be seen as a positive exception. The difficulties are attempted to be solved by use of special models for dynamic accident situations, but problems related to the data cannot be put aside. Furthermore, it is pointed out that the validation of current models would require an appreciable amount of investment and would take years to complete.

Scopes of each investigated PSAs are illustrated by Table 3.10. In addition to the limitations mentioned here, it should be pointed out that no PSA has taken improper management and supervisor performance into account.

Table 3.10

Documented scopes of the studies investigated

Study \ Error Type	1.	2.	3.	a)	b)	c)
Oconee	++	+	++	++	++	++
Biblis	+	-	+	++	-	-
Sizewell	No accurate information exists					
Calvert Cliffs	++	-	+	++	+	-
Seabrook	++	+	++	++	++	++

1. = Maintenance errors
2. = Human event initiators
3. = Dynamic operator actions
   a) errors of omission
   b) errors of commission
   c) diagnostic errors

++ = included extensively
+ = included partially
- = not included

3.4.3 Identification and classification of human errors

The main identification source for the important human errors is system analysts' knowledge. It has been mentioned to form the basis of the identification in Oconee and Seabrook studies. In addition, insights from simulator runs and operator judgement were utilized.

Operating manuals were the main source of information in German Risk Study and in Calvert Cliffs PSA, but the latter was supplemented by reviewing maintenance and emergency procedures.

General features concerning the identification task are covered by Table 3.11.

Table 3.1i

Identification of human interactions

Plant	Basis of identification
Oconee	System analysts, event and fault tree development
Seabrook	System analysts, event tree development, verification via simulator exercises
Calvert Cliffs	Fault tree development, procedures reviewed
Biblis	Operating procedures investigated
Sizewell	No detailed information available

The question of classification is also coupled to identification and sorting out human errors. Swain's classification (Swain and Guttman, 1983) has been utilized in Calvert Cliffs and Biblis PSAs. Oconee and Seabrook PSAs generated their own taxonomies, but the ideas of modern cognitive models, e.g. three state division (Rasmussen, 1981), were clearly taken into account.

Psychological factors are normally treated in the form of performance shaping factors (PSFs). In Sizewell PSA stress was seen to be the most important PSF; this is also valid for Seabrook, where stress levels were seen to affect the simulator run results. In Calvert Cliffs PSA, discussions with the staff were carried out and photographs of panels were taken to evaluate the importance of PSFs. German Risk Study and Oconee PSA used many PSFs according to Swain's schemes, but the Oconee study includes also dependencies between e.g. actions with the same goal or between actions dependent on the same diagnosis.

3.4.4 Modeling of human errors

General reliability models i.e. fault trees (FTS) and event trees (ETS), with their extensions such as HRA-tree and OAT, are normally used to model human actions. Also confusion misdiagnosis matrix may be used. Different PSAs used different models in the following manner:

- In Sizewell PSA, OAT was used besides standard FTs and ETs.
- In German Risk Study, HRA-tree was used according to the Handbook of Human Reliability.
- Calvert Cliffs study utilized HRA-tree for the most important human interactions besides ETs and FTs.
- In Seabrook PSA, OAT-models represent the most important interactions and confusion matrix demonstrates misdiagnosis possibilities.
- In Oconee PSA, human error fault trees were drawn to aid in the quantification.

Cognitive models were used only to support the quantification.

3.4.5 Data sources

The assignment of human error data is based on procedures, drawings, control room reviews, interviews, simulator runs, engineering judgement and Swain's Handbook. The last two are the most often used. In the Seabrook study, also the Bayesian treatment of the high pressure injection sequence in the light of operating experience was applied. The human error probabilities varied generally from 10^{-5} for certain inhibition errors to 10^{-1} or even higher for extremely stressful dynamic activities.

In Table 3.12, the comparison of the data sources of the PSA is shown.

Table 3.12

The data sources used in the PSAs

Plant	Data source
Oconee	Handbook for routine actions, plant documentation reviews, simulator runs and expert opinion for dynamic errors
Seabrook	Handbook for routine actions, expert opinion for dynamic actions, Bayesian treatment of the TMI scenario
Calvert Cliffs	Handbook, interviews, maintenance procedures
Biblis	Expert opinion
Sizewell	Estimations and possibly Handbook

3.4.6 Impact of human activities on core damage frequencies

The impact of human activities on the core damage frequencies is significant. This means that the frequency can be affected even by an order of magnitude. The way in which errors and recovery actions are taken into account should be considered when interpreting the results.

- In Calvert Cliffs PSA, recovery actions are taken into account. Two important scenarios dominate the human impact.
- In Sizewell PSA, the human impact is relatively low. This may be due to design features but also new analyses are being carried out.
- In the German Risk Study, human errors have a remarkable effect on the final result. The role of recovery is somewhat unclear.
- In Seabrook PSA, the human influence was not apparent but had to be calculated from the sequences.
- In Oconee PSA, recovery actions influenced the final result substantially. Two sequences including human errors contribute significantly to the overall risk.

In Table 3.13 human contributions are presented. It should be noted that in most cases the human contribution could not be directly seen from the PSA summary. Therefore, the table should be used carefully to avoid misunderstandings.

Table 3.13

Human contributions to core damage frequencies

Plant	Core Damage Frequency	Impact of Human Errors	Impact of Recovery
Oconee	$2.5 \cdot 10^{-4}$ (mean; modified plant)	4 %	75 %
Seabrook	$2.3 \cdot 10^{-4}$ (mean for a single unit)	30-50 % (estimate)	not clear, evidently significant
Calvert Cliffs	$1.3 \cdot 10^{-4}$ (mean)	12 %	90 % (order of magnitude)
Biblis	$9.0 \cdot 10^{-5}$ (mean)	63-69 % (with other failures)	not documented
Sizewell	$1.0 \cdot 10^{-6}$ (median)	1.4 %	not documented

3.4.7 Conclusions

The material for this retrospective analysis was vast and its thorough investigation would have required more resources. Therefore, we have to focus on these parts of PSAs, which were devoted to human reliability analysis. The human actions analysed implicitly in other sections are thus not considered here. Since in some cases the written documentation on the human reliability analysis was quite concise, it may be suspected that this part of the analysis is quite large.

With respect to the PSA documentation, it should be pointed out that better quality is needed in the future. This means also that different analysis steps should be easy to find and references to other relevant parts of the study should be given. Seabrook and partly Oconee studies are positive exceptions in this context.

With respect to the scopes of the PSAs, they basically consider only human actions directly related to operation and maintenance. This is generally reasonable, since management and supervisory activities are reflected via increase or decrease in error or recovery probabilities.

Commission type errors if taken into account, may change the event sequence by affecting the reactions of plant staff (e.g. som actions forbidden by shift supervisors; Suokas and Pyy, 1988). This can be seen to be the most hazardous part of human interactions; the operators may not have adequate information on the situation or at least the information is not completely utilized. Such misleading situations cannot be identified by using procedures only, but operating experience, simulators and comprehensive analysis effort are required. Among the studies, only Seabrook and Oconee PSAs tried to investigate this part of the problem.

Nowadays the identification of significant human interactions relies on the abilities of system analysts. Referring to the earlier conclusions, verification based on simulator runs and interviews with plant staff should be encouraged. In some cases, also application of hazard identification methods used in the process industries could be reasonable.

The modeling of human interactions is mainly based on event tree models such as the THERP-tree and OAT, which are used to support quantification by decomposing human behaviour. The quantified actions are then included in system fault trees or event trees depending on their importance. A matrix model for misdiagnosis events was utilized in Seabrook and Oconee to define corresponding probabilities for OAT or HRA-fault trees (Oconee). Simple logical models are suitable for procedural activities mostly analysed.

The main source of reliability data is expert opinion. The comparison of probability estimates is not covered here, but the importance of the subject becomes manifested thinking about the impact of human activities on total core damage frequencies. It is, however, clear that experts can assess probabilities with accuracy of an order of magnitude or in some cases even better.

The main differences in the studies came through the inclusion of recovery. This means that the core damage probabilities are highly sensitive to human actions - erroneous or corrective - and in some cases would be about an order of magnitude higher if recovery possibility was not included. The erroneous actions increase the possibility of accident, but by proper accident management (recovery) the control can be restored. However, the numbers tell us that human behaviour is frequently the key factor to safe plant operation. Completely another question is how large the impact of recovery should be, i.e. how much the operating staff could be relied on.

In the retrospective study, it became clear that all the PSAs are made with care and are based on good engineering judgement. The purpose of the study is only to point out some aspects for discussion. It is evident that a PSA with an extensive psychological program and detailed investigation of every possible event sequence branchings would take years to complete. Thus, we have to compromise but the limitations and the uncertainties should be expressed in a transparent way.

3.5 References

ABB Atom AB (1985)
Forsmark 3 Safety Study (in Swedish), February 1985.

Aid, H. (1987)
Reference Study on Human Interaction Concerning Manual Depressurization at Forsmark 3. Report RAS-470(87)17 (Studsvik Report NP-87/135), November 1987.

Aid, H. and Pörn, K. (1988)
Addendum to Report NP-87/135, Studsvik, February 1988.

Bengtz, M. and Hirschberg, S. (1987)
Retrospective Analysis of Human Interactions in the Swedish Probabilistic Safety Studies. Phase 1: Qualitative Overview. Report RAS-470(87)5 (ABB Atom Report RPC 87-54), July 1987.

Carlsson, L., Hirschberg, S., Johanson, G., Pörn, K. and Wilson, D. (1988)
Can different PSAs be Compared and Used in Nationwide Decision Making? Status of and Experience from the Swedish ASAR-program. OECD/CSNI Worskhop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Electric Power Research Institute (1981)
German Risk Study - Main Report: A Study of the Risk Due to Accidents in Nuclear Power Plants (Translation from German). Report EPRI NP-1804-SR, April 1981.

Electric Power Research Institute (1984)
Probabilistic Risk Assessment of Oconee Unit 3 Vol. 1-4. Report NSAC-60, June 1984.

Hannaman, G.W., Spurgin, A.J. (1984)
Systematic Human Action Reliability Procedure (SHARP). Report EPRI NP-3583, Electric Power Research Insitute, June 1984.

Hannaman, G.W., Spurgin, A.J. and Lukic, Y. (1985)
A Model for Assessing Human Cognitive Reliability in PRA Studies. 1985 IEEE Third Conference on Human Factors and Power Plants, Monterey, California, U.S.A.

Hirschberg, S., ed. (1989)
NKA-project "Risk Analysis" (RAS-470); Summary Report on Reference Study of Human Interactions. Report RAS-470(89)17 (ABB Atom Report RPC 89-112), December 1989.

Hirschberg, S. and Bengtz, M. (1987)
Retrospective Analysis of Dependencies and Human Interactions in Swedish PSA-studies. Scandinavian Reliability Engineers Symposium, Helsingør, Denmark, October 5-7, 1987.

Hirschberg, S., Björe, S. and Jacobsson, P. (1989a)
Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA'89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S., Jacobsson, P., Petersen, K.E., Pulkkinen, U. and Pörn, K. (1989b)
Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Hirschberg, S., Jacobsson, P., Pulkkinen, U. and Pörn, K. (1989c)
Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A. April 2-7, 1989.

Jacobsson, P. (1988a)
Reference Study on Human Interaction Concerning Manual Depressurization at Forsmark 3. Report RAS-470(88)13 (ABB Atom Report RPC 88-78), May 1988.

Jacobsson, P. (1988b)
Sensitivity Study on Manual Depressurization and Manual Reclosure of 314-valve in Swedish PSAs. Report RAS-470(88)26 (ABB Atom Report RPC 88-113), August 1988.

Laakso, K. (1984)
A Systematic Feedback of Plant Disturbance Experience in Nuclear Power Plants. Ph.D. Thesis (in Swedish), Helsinki University of Technology, December 1984.

Lydell, B.O.Y., et al.
Human Reliability Analysis in Contemporary Probabilistic Risk Assessment Studies. Report PLG-0349, prepared for the Swedish Nuclear Power Inspectorate, March 1984.

NUS-Corporation (1984)
Ringhals 2 Safety Study. Report NUS-4365, May 1983 (Revised February 1984).

OKG AB (1986)
Oskarshamn 3 Safety Study (in Swedish), 1986.

OKG AB (1987)
Oskarshamn 1 Safety Study (in Swedish), 1987.

Petersen, K.E. (1988)
Reference Study on Human Interactions. Report RAS-470(87)16, Risø, September 1988.

Petersen, K.E. and Aid, H. (1988)
Use of Operator Training Simulators in Analysis of Human Interventions in Complex Industrial Systems. Scandinavian Reliability Engineers Symposium, Västerås, Sweden, October 10-12, 1988.

Pickard, Lowe and Garrick Inc. (1983)
Seabrook Station Probabilistic Safety Assessment. Report PLG-03300, 1983.

Poucet, A., ed. (1989)
HF-RBE, Human Factors Reliability Benchmark Exercise. Synthesis Report EUR 12222 EN, Ispra Establishment, August 1989.

Pyy, P. and Pulkkinen, U. (1988)
Human Reliability in Probabilistic Risk Assessment. A Retrospective Study. Report RAS-470(87)10 (VTT Research Notes 908), November 1988.

Rasmussen, J. (1981)
Human Factors in High Risk Technology. Report Risø N-2-81, 1981.

Suokas, J. and Pyy, P. (1988)
Evaluation of the Validity of Four Identification Methods of Safety Analysis with Event Descriptions. VTT Research Report 516, January 1988.

Svenson, O. (1987)
Cognitive Psychology for Safety Analyses in the Processing Industry with Emphasis on Nuclear Power Plant Applications. University of Stockholm, April 1987.

Svensson, I. (1977)
Safety Study Forsmark 3: Loss of water make-up (in Swedish). ABB Atom Report RCC 77-180, November 1977.

Swain, A.D., Guttman, H.E. (1983)
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report NUREG/CR-1278, U.S. Nuclear Regulatory Commission, August 1983.

Swedish State Power Board (1984)
Ringhals 1 Safety Study (in Swedish), October 1983 (Revised August 1984).

Sydkraft (1987),
Barsebäck 1 Safety Study (in Swedish), January 1985 (Revised January 1987).

U.S. Nuclear Regulatory Commission (1984)
Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant, 1984.

Westinghouse Electric Corporation (1982)
Sizewell B Probabilistic Safety Study. Report WCAP 9991, 1982.

4. UNCERTAINTY AND SENSITIVITY ANALYSIS

This chapter provides a review of RAS-470 activities within the area of sensitivity and uncertainty analysis. Present state-of-the-art is shortly accounted for. This is followed by summaries of the Nordic Reference Study on Uncertainty and Sensitivity Analysis (Hirschberg et al., 1989b,c), and of retrospective sensitivity studies of CCFs and human interactions in Swedish PSAs (Hirschberg et al., 1989a). Limitations of PSA are discussed and some reflections on decision making in view of uncertainties (Pulkkinen and Pörn, 1989), are given.

4.1 Status

All modeling of physical phenomena is associated with uncertainty. It will never be possible to claim that a model is perfect. Instead a model may be more or less valid with respect to its capacity to predict the phenomena of concern.

These general statements are also valid in case of PSA. The purpose of PSA is to provide basis or support for decision making in safety related matters. Then, of course, it is not enough for the risk analyst to present an estimated point value of the risk variable of concern - as a result of point values for input quantities. Instead of this the analyst has to express his/her uncertainty about the quantity of interest in the form of a probability distribution which includes both the a priori engineering knowledge and the statistical evidence. The analyst must also keep track of all known uncertainties and integrate them in a consistent way into the final decision variable. This approach presupposes the concept of subjective probability and the use of Bayesian methodology.

The analysis of uncertainties is not possible if the uncertain modeling assumptions, the uncertaties about the modeling parameters and the model structure are not identified, admitted and documented by the analyst. Thus the uncertainty analyses require a critical attitude with regard to the modeling work. Some of the uncertainties are not quantifiable - by the technique available today - but they have to be documented carefully and described for the decision makers.

When a risk analysis is started it is always necessary to confine the problem areas within certain boundaries. Then a nonquantifiable uncertainty is introduced with regard to the impact such boundaries will have on the results of the analysis. This source of uncertainty could be characterized as **completeness uncertainty.**

All quantitative analyses need models. The models are always parametric. The choice of a specific model is based on some basic assumptions, the validity of which is uncertain. This **modeling uncertainty** is usually analysed by conventional sensitivity analysis, where point value estimations are repeated for varying modeling assumptions.

In the light of the model chosen the available statistical evidence is interpreted and treated in order to determine the appropriate parameters. Not seldom it is difficult to decide whether existing data are adequate for the application considered. Further, the statistical data are scarce, which means a substantial statistical uncertainty. All uncertainties connected to the determination of model parameters, conditioned by a given model, can be classified as **parametric uncertanties.** A good basis for handling of this type of uncertainty in PSA is e.g. provided by the Reliability Data Book for components in Swedish nuclear power plants (Bento et al., 1985). Using this data base and existing computer programs for uncertainty propagation the parametric uncertainty can be treated for a whole PSA (Pörn, 1988), Figure 4.1.

Above several sources of uncertainty have been identified. However, even if the sources of uncertainty are different the uncertainties as such are similar. As a matter of fact, there is no difference between the uncertainty about some parameter value and the uncertainty with regard to the validity of alternative models. This means that all uncertainties, in principle, can be expressed by the use of a common measure, the concept of subjective probability. It is, however, much more difficult to assess the uncertainties about the validity of models compared with the numerical values of parameters.

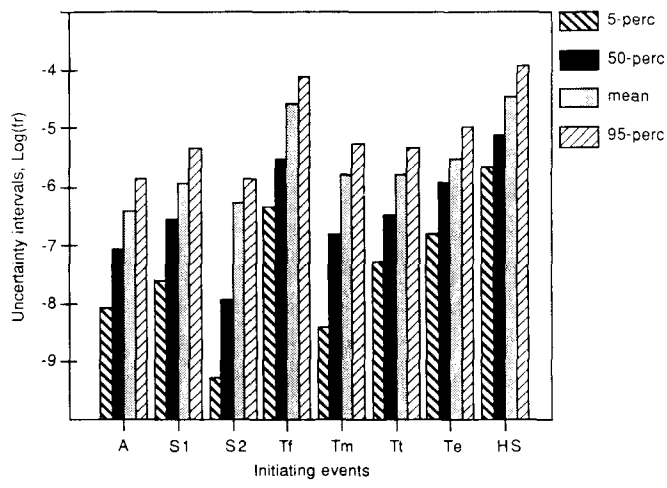


Figure 4.1

Uncertainty intervals of core damage frequency and its contributors corresponding to the different initiating events (Pörn, 1988)

The issue of probability as a measure of uncertainty in PSA is widely discussed in the literature. A good summary together with a comprehensive reference list is given in (Apostolakis, 1989). As this reference points out some authors wish to make a very clear distinction between statistical or stochastic uncertainties and "state-of-knowledge" uncertainties. To illustrate this distinction let us consider the failure time T of a certain component. The distribution of this time is $F(t|\lambda)$, conditioned by the failure rate λ. The uncertainty about the numerical value of λ is expressed by the pdf $p(\lambda)$.

Then, the distinction stands between $F(t|\lambda)$, representing the 'frequency' or stochastic uncertainty, and $p(\lambda)$, expressing the 'probability' or state-of-knowledge uncertainty. As also stated in (Apostolakis, 1989), this distinction is simply for convenience. Another interesting reference in this context is (Apostolakis, ed., 1988), which is entirely devoted to the theme: "The interpretation of probability in probabilistic safety assessment".

In this project one has chosen to study a risk dominating accident sequence (T_fUX2) from the uncertainty point of view (subchapter 4.2). The main parameter of interest in the study is the frequency (intensity) of core damage as a consequence of loss of feedwater accompanied by the loss of the auxiliary feedwater flow.

In this specific analysis it is easy to recognize the various sources of uncertainty desribed above. Completeness uncertainty was introduced to some extent by starting the analysis from a given list of minimal cut-sets. Certainly other more basic boundaries were stated already when the Forsmark 3 PSA (ABB Atom AB, 1985) was carried out. As modeling uncertainty contributors the binary event and fault tree models can be mentioned as well as the assumption of constant failure rates for the components. Even larger uncertainties can be ascribed to the modeling of common cause failures and human errors. The interpretation of existing data for initiating events and common cause failures is probably the most significant source of parametric uncertainty.

As previoulsy mentioned PSA or other more specific studies are performed in order to generate a basis for decision. An interesting item for decision making, actualized in the uncertainty analysis of this project, is the choice between manual or automatic depressurization.

In order to support the decision maker it is essential for the analyst to fulfil some basic documentation requirements. It is to clearly and systematically summarize the results obtained and to describe all presumptions, limitations and simplifications (completeness uncertainty) that have been made in the analysis. As regards other uncertainty aspects, which cannot be quantified, it is equally important to qualitatively identify all the uncertainty sources the analyst is aware of.

Some basic features of uncertainty analysis and decision making under uncertainty are treated in subchapter 4.5.

4.2 Reference Study on Uncertainty and Sensitivity Analysis

4.2.1 Background

The Benchmark Exercise on common cause failure (CCF) data for motor-operated valves (MOVs), described in subchapter 2.2, resulted in findings concerning recommendations on suitable procedures for search of CCFs, suggestions for improvements of the current failure reporting system, identification of merits and drawbacks of classification systems, evaluation of

parametric models and direct assessment, and identification of most sensitive elements in the process of CCF-quantification (Hirschberg, ed., 1987).

The human interaction reference study (Hirschberg, ed., 1989), summarized in subchapter 3.2, concerns manual depressurization following loss of main and auxiliary feedwater systems at the Forsmark 3 plant. The main purpose of this study was to compare different approaches to the problem, to identify factors which have decisive impact on quantitative results and to investigate the importance of assumptions behind the boundary conditions.

The Swedish PSAs available at the time of initiation of the activities described in this subchapter, are limited to point estimates of accident sequence frequencies. With the exception of Forsmark 3 PSA (ABB Atom AB, 1985 and Hirschberg and Knochenhauer, 1986) no comprehensive sensitivity studies have been performed.

The reference study on uncertainty and sensitivity analysis was undertaken in order to combine experiences from the previous phases of the RAS-470 project mentioned above, and to demonstrate the impact of modeling and parameter uncertainties on the accident sequence level.

In the following the results of the reference study are summarized. For details we refer to the reports written by each working group (Hirschberg and Jacobsson, 1988; Pulkkinen et al., 1988; Pörn and Fahlén, 1988; Hirschberg and Jacobsson, 1989; Petersen, 1990; Pörn and Fahlén, 1989; Pulkkinen et al., 1989).

4.2.2 Objectives and scope

The main objectives of the reference study are:

- To demonstrate the impact of uncertainties, in particular these associated with treatment of CCFs and human interactions on the uncertainty of the investigated accident sequence.
- To present alternative approaches to the treatment of uncertainties and interpret the obtained results.
- To evaluate and compare the available methods and computer codes for uncertainty analysis.

The first phase of the study (Hirschberg et al., 1989c) concerned generation of uncertainty distribution for the investigated accident sequence. In this context the participants have been given great freedom with regard to choice of methods and data for quantification of the CCF- and human interaction contributions. The second phase (Hirschberg et al., 1989b) concentrated on comparisons of different computer codes for uncertainty analysis. It is based on use of a common model and data for all types of events involved. Finally, in the third phase (Hirschberg et al., 1989b) the participants used the experiences from preceding stages choosing a final solution (models, data and computer codes) which they regard as "optimal" (with due regard to practical limitations).

4.2.3 Problem description

As a first activity within the project a set of boundary conditions had been proposed by ABB Atom (Hirschberg, 1988) and was accepted by the project participants.

T_fUX2, the most dominant sequence from the Forsmark 3 PSA (ABB Atom AB, 1985) is the object of the study (T_f = loss of feedwater transient; U = loss of auxiliary feedwater; X2 = failure to initiate manual depressurization). Forsmark 3 is a BWR plant designed by ABB Atom. The plant is characterized by a strict division of safety systems into four redundant trains which are consequently separated from the physical and functional point of view.

The selected sequence is dominated by residual CCF-contributions for motor-operated valves (previously studied within the CCF-data Benchmark Exercise (Hirschberg, ed., 1987)) and by operator failure to initiate manual depressurization (previously studied within the reference study (Hirschberg, ed. 1989)). It should be observed that the selected sequence is not typical for the Swedish PSAs. Due to the involvement of CCF-contributions with high failure multiplicities, combined with an operator action, the associated uncertainties are expected to be large. The particular sequence is, however, considered as ideal for the present project since it represents a challenge to the analysts.

The background material distributed by ABB Atom to all participants in the reference study included:

1) Basis for evaluation of the frequency of the initiating event T_f (loss of feedwater transient).

2) Description of the system analysis for system 327 (auxiliary feedwater system), including fault trees and failure data; event U corresponds to loss of this system function.

3) Event tree for initiating event T_f, sequence description and dominating minimal cut-sets (MCS) for sequence T_fUX2 (88 cut-sets).

4) Description of the approach to CCF-treatment as applied in the Forsmark 3 PSA. This includes incorporation of CCF-contributions in the fault tree model, CCF-data and quantification of CCF-contributions.

5) Description of the approach to human interactions, used in the Forsmark 3 PSA.

6) Coding system used in the Forsmark 3 PSA.

Consequently, the reference study did not contain construction of the fault tree model which was accepted as it was. The available fault trees and the cut-set list from the Forsmark 3 PSA served as the basis of the reference study. All dominating cut-sets include the manual depressurization (event X2) and CCF-contributions corresponding to different failure multiplicities. Thus, most of the important failure probabilities have been assigned, based on models and engineering judgement. In the first and third phases the participants were free to choose their own approach to quantification of CCF-contributions and manual interaction(s). However, the approach chosen had to be consistent with the logical structure of the cut-set list supplied. Whenever applicable the Swedish Reliability Data Book, version 2 (T-book; Bento et al., 1985) was to be used as a basis for specification of uncertainty distributions. Each group could choose an approach to uncertainty propagation which they considered as best among those practically available. The results were to be supplemented by a sensitivity study.

4.2.4 Common assumptions

Due to the special nature of the analysed sequence the main uncertainties are expected to be associated with the treatments of the initiating event, manual depressurization and CCFs. Thus, the analysis effort was concentrated on study of these problem areas. Also in the following description the main emphasis will be on these critical elements.

The sequence frequency has been represented by all groups as a polynomial function of the initiating event frequency and basic event probabilities. This function also determines how the uncertainty of the output is related to the uncertainties of the inputs. When the function is established there are four major steps in the uncertainty and sensitivity analysis:

1) Characterization of the uncertainties in the inputs.

2) Propagation of these uncertainties through the system model represented by the polynomial function.

3) Performance of sensitivity studies concerning elements (models, data, assumptions) which may have significant impact on the results.

4) Identification of the significant sources of uncertainty with respect to the sequence results.

All groups based the uncertainty analysis on the list of 88 most dominating MCS as they are presented in the safety study (ABB Atom AB, 1985). The impact of deleted MCS has not been evaluated. Initially, the conservative rare event approximation was consequently applied. However, in phases two and three some groups attempted to evaluate the degreee of conservatism associated with this approximation (see Section 4.2.7).

4.2.5 Principles for propagation of uncertainties and analysis tools

Propagation of uncertainties through sequence model has been carried out by all groups using Monte Carlo technique. This technique was deemed to be the most flexible and precise among those available. All groups took into account "state-of-knowledge" dependences (Apostolakis and Kaplan, 1981) by assignment of the same uncertainty distribution to components or events belonging to the same category. Table 4.1 shows the computer programs used by different groups for the purpose of uncertainty and sensitivity analysis.

Table 4.1

Computer tools used by different groups for the purpose of uncertainty propagation and sensitivity analysis

Group	Uncertainty propagation	Sensitivity analysis
ATOM	SAMPLE[a] and SPASM[b]	SAMPLE[a], SPASM[b] and SENS[a]
RISØ	MOCARE[c]	MOCARE[c]
STUDSVIK	SPASM[b]	SPASM[b]
VTT	MONTEC[d]	MONTEC[d] and RELVEC[d]

[a]SAMPLE and SENS are parts of ABB Atom's integrated code package for reliability and risk analysis (SUPER-NET). SPASM was used by ATOM only in phase 3.
[b]Version extended by STUDSVIK.
[c]Code developed by RISØ primarily for systems reliability analysis.
[d]Codes developed by VTT.

4.2.6 Initial (phase 1) analysis

Phase 1 approach and data used will be described in a rather detailed way since they constituted a basis for evolution of the results of the subsequent phases.

4.2.6.1 Input uncertainty distributions and sensitivity aspects

The cut-set list for sequence T_fUX2 contains 45 basic events corresponding to single component failures, human errors and CCFs. The results obtained for the distributions of the most important variables are summarized below. Whenever applicable this includes also cases for sensitivity analysis. For each of the groups the most representative set of parameters later to be used in quantification of the reference case on the sequence level, will be given first. Generally, in ABB Atom analysis although different distributions have been used as a starting point, they were consequently approximated by log-normal distributions before propagation of uncertainties was carried out.

1) Initiating event. According to the operational experience 3.5 events classified as loss of feedwater transients relevant for the Forsmark 3 design and operation have occurred during 16 reactor-years at Swedish

BWRs included in the background material. Note that the estimated number of transients is based on assignment of weighting factors to events which occurred during the first year of operation. Table 4.2 summarizes the results.

An interesting feature of the approach employed by VTT is use of weighting factors in order to take into account the possible nonrelevance of data sources. A methodology for this approach has been developed earlier within the RAS-470 project (Pulkkinen et al., 1987).

As may be seen the discrepancies between the groups are rather small from practical point of view.

2) Common cause failures. In the Forsmark 3 PSA the Multiple Greek Letter (MGL) method (Fleming and Kalinowski, 1983) has been used for estimation of CCF-contributions. The contributions have been incorporated into the fault tree model on the system train level. This means that all relevant CCF-combinations for components which may be affected by CCFs, have been taken into account. The contributions corresponding to different failure multiplicities are obtained as a sum of calculated contributions on the component level. Due to the symmetry of redundant trains this simplified and compact representation is exact. The CCF-contribution for the auxiliary feedwater system includes contributions from two sets of MOVs, two sets of check valves and one set of piston pumps (each set consists of four redundant components).

Within the present study ATOM used the alpha-factor method (Mosleh and Siu, 1987;reference case) and the MGL-model (sensitivity analysis) for quantification of CCF-contributions. The quantification of CCF-contributions has been made by a Monte-Carlo simulation of beta-distributed (approximated by log-normal distribution) parameters of the models. The evaluation of these parameters was based on data from the T-book (Bento et al., 1985), ABB Atom's contribution to the CCF-data Benchmark Exercise (Hirschberg, ed., 1987) and the Forsmark 3 PSA.

STUDSVIK chose the direct assessment employing the Bayesian method based on a noninformative prior distribution (Pörn, 1989). Both the prior and posterior distributions are of Dirichlet type. This approach which was earlier used by STUDSVIK in the context of CCF-data Benchmark Exercise (Hirschberg, ed., 1987) is directly based on knowledge of the number of system demands/tests and the number of double, triple and quadruple failures.

VTT used in the reference case the MGL-method and the parameter estimates given in the Forsmark 3 PSA. The MGL-parameters were used as the expected values of maximum entropy distributions. For the purpose of sensitivity analysis the direct estimation based on Dirichlet distribution was applied for MOVs, which totally dominate the CCF-contributions; for other components the same approach as in the reference case was used. In an additional sensitivity study the MGL-model for CCFs was combined with beta distributions for single failure probabilities. The latter distributions were based on uniform prior distributions and the statistical evidence of the T-book.

Table 4.2

Distribution parameters for initiating event frequency (phase 1)

Group	Distribution	Mean (per year)	Stand.dev. (per year)	Median (per year)	5-per-centile (per year)	95-per-centile (per year)
ATOM	Discrete Poisson[a]	0.23	0.16	0.19	0.07	0.53
STUDSVIK	Gamma[b]	0.25	0.13	0.23	0.09	0.48
VTT[c]	Mixture of gamma[b]	0.27	0.14	0.25	0.09	0.55
	"-	0.32	0.20	0.28	0.10	0.70

[a]Approximated by a log-normal distribution
[b]Based on noninformative prior distribution
[c]Different interpretations of the original data

Table 4.3 summarizes the estimates of quadruple CCF-contributions in the auxiliary feedwater systems (these have the most significant impact on the accident sequence frequency). For the contributions corresponding to lower failure multiplicities we refer to the original reports (Hirschberg and Jacobsson, 1988; Pulkkinen et al., 1988; Pörn and Fahlén, 1988). It is important to note that the selected sequence involves a phased mission operation of the auxiliary feedwater system. During the mission time the MOVs are operated about 50 times. All groups took this fact into account when estimating single failure probability for MOVs by introduction of a reduction factor of 0.1 for the actuations following upon the first demand. Two groups (ATOM, VTT) used the same approach to this problem in the CCF-context, while STUDSVIK neglected the CCF-contributions associated with the subsequent demands. Since these two extreme approaches may be regarded as excessively pessimistic and optimistic, respectively, and the models used are rough, this aspect will be subject to refined analysis in the second phase of the project.

Given the nature of the problem the discrepancies between the results obtained by different groups are not too dramatic and originate from specific differences in treatment of data (e.g. use of design-oriented screening, use of extension schemes, treatment of potential CCFs) and in choice of quantification methods and distributions. Notably ATOM's and VTT's uncertainty intervals are much broader than STUDSVIK's.

3) Manual depressurization. Based on thermal-hydraulic calculations for the sequence in question, the available time for initiation of manual depressurization is approximately 25 minutes. The analysis of this operator action was preceded by a simulator exercise which, however, did not correspond exactly to the situation to be analysed.

Two of the groups (ATOM and STUDSVIK) used a similar approach to the problem. The THERP method was combined with data from the Handbook of Human Reliability Analysis (Swain and Guttman, 1983). Available time for carrying out of the manual depressurization (i.e. for diagnosis, performance of necessary operation and possible recovery) was regarded by all groups as a critical factor in the context of quantification. The third group (VTT) used the most probable path diagram as a support to the operator action tree approach. The diagram illustrates time-dependent course of events and operator goals in different stages of the event sequence. The estimates of operator error probabilities were in VTT's analysis based on subjective judgement and the uncertainty distributions were obtained by using the maximum entropy principle.

Table 4.4 shows characteristics of the uncertainty distributions for manual depressurization error probability, according to different groups.

The discrepance between ATOM's and STUDSVIK's results is primarily due to different assumptions concerning time window for the operator action. The fact that VTT's analysis leads to significantly lower estimates is not attributed to methodological differences but mainly to the approach to data assignment.

Table 4.3

Distribution parameters for quadruple CCF probability in the auxiliary feedwater system (phase 1)

Group	Distribution	Mean (per demand)[a]	Stand.dev. (per demand)[a]	Median (per demand)[a]	5-per-centile (per demand)[a]	95-per-centile (per demand)[a]
ATOM	Alpha-factor[b]	$8.5 \cdot 10^{-3}$	$2.0 \cdot 10^{-2}$	$3.8 \cdot 10^{-3}$	$6.1 \cdot 10^{-4}$	$2.8 \cdot 10^{-2}$
	MGL[b]	$2.3 \cdot 10^{-3}$	$5.5 \cdot 10^{-3}$	$9.3 \cdot 10^{-4}$	$1.2 \cdot 10^{-4}$	$8.4 \cdot 10^{-3}$
STUDSVIK	Direct assessment[c]	$4.0 \cdot 10^{-3}$	$2.3 \cdot 10^{-3}$	$3.5 \cdot 10^{-3}$	$1.2 \cdot 10^{-3}$	$8.4 \cdot 10^{-3}$
VTT	MGL[d]	$1.6 \cdot 10^{-3}$	$6.5 \cdot 10^{-3}$	$2.7 \cdot 10^{-4}$	$7.0 \cdot 10^{-6}$	$6.9 \cdot 10^{-3}$
	Direct assessment[e]	$1.3 \cdot 10^{-3}$	$2.8 \cdot 10^{-3}$	$4.2 \cdot 10^{-4}$	$1.5 \cdot 10^{-5}$	$5.7 \cdot 10^{-3}$
	MGL[f]	$1.5 \cdot 10^{-3}$	$3.6 \cdot 10^{-3}$	$4.3 \cdot 10^{-4}$	$1.3 \cdot 10^{-5}$	$5.6 \cdot 10^{-3}$

[a] In ATOM's and VTT's analysis the contributions correspond to approximately 50 demands anticipated in the course of this sequence

[b] Based on beta distribution approximated by log-normal

[c] Based on Dirichlet distribution

[d] Based on maximum entropy distribution

[e] Direct assessment based on Dirichlet distribution used only for MOVs; otherwise MGL and maximum entropy distribution

[f] Based on beta distribution for single failures

Table 4.4

Distribution parameters for failure of manual depressurization (phase 1)

Group	Basic Distribution	Mean (per demand)	Stand.dev. (per demand)	Median (per demand)	5-per-centile (per demand)	95-per-centile (per demand)
ATOM[a]	Log-normal	$9.1 \cdot 10^{-3}$	$2.9 \cdot 10^{-2}$	$3.1 \cdot 10^{-3}$	$6.4 \cdot 10^{-4}$	$3.1 \cdot 10^{-2}$
	"	$9.6 \cdot 10^{-3}$	$1.6 \cdot 10^{-2}$	$5.0 \cdot 10^{-3}$	$1.2 \cdot 10^{-3}$	$3.3 \cdot 10^{-2}$
STUDSVIK	Log-normal	$1.9 \cdot 10^{-2}$	$6.5 \cdot 10^{-2}$	$5.8 \cdot 10^{-3}$	$1.0 \cdot 10^{-3}$	$7.3 \cdot 10^{-2}$
VTT	Max. entropy	$2.2 \cdot 10^{-3}$	$1.3 \cdot 10^{-3}$	$1.9 \cdot 10^{-3}$	$6.3 \cdot 10^{-4}$	$4.5 \cdot 10^{-3}$

[a]Two cases corresponding to alternative modeling assumptions (different time windows) analysed

4.2.6.2 Results on accident sequence level

1) Reference case. The results of analyses performed by different groups for their reference cases are presented in Table 4.5. Note that the results correspond to treatment of the critical elements shown in Tables 4.2, 4.3, 4.4 according to the first alternative (if several) given for each group, respectively.

Table 4.5

Results on sequence level (reference case; phase 1)

Group	Mean (per year)	Stand.dev. (per year)	Median (per year)	5-per-centile (per year)	95-per-centile (per year)
ATOM	$8.3 \cdot 10^{-5}$	$1.8 \cdot 10^{-3}$	$2.9 \cdot 10^{-6}$	$1.2 \cdot 10^{-7}$	$1.1 \cdot 10^{-4}$
STUDSVIK	$6.4 \cdot 10^{-5}$	$5.6 \cdot 10^{-4}$	$6.7 \cdot 10^{-6}$	$6.4 \cdot 10^{-7}$	$1.7 \cdot 10^{-4}$
VTT	$4.7 \cdot 10^{-6}$	$3.1 \cdot 10^{-5}$	$2.3 \cdot 10^{-7}$	$6.8 \cdot 10^{-9}$	$1.2 \cdot 10^{-5}$

The estimates of central characteristics of uncertainty distributions obtained by ATOM and STUDSVIK are quite close. VTT's results are in this respect significantly lower which is mainly attributed to use of much lower probabilities for quadruple CCFs and for failure of manual depressurization. The overall uncertainty interval attained by all groups covers more than two decades. Notable is also that the ratio between mean and median values, considered as a measure of skewness of the distributions, is extremely large (between 9.6 and 28.6).

2) Sensitivity Analyses. As stated earlier all groups performed sensitivity analyses. Some cases have been mentioned earlier (Tables 4.2, 4.3, 4.4); for all these cases uncertainty propagation on the sequence level has been performed. The results will be shortly summarized in the following.

ATOM examined the impact of "state-of-knowledge" dependences by using an uncorrelated sequence function. This was done partly for the reference case and partly with alpha-factor method substituted by the MGL-model. As expected both cases lead to substantial reduction of the mean values. In both correlated and uncorrelated cases the use of alpha-factor method results in higher mean values, median values and broader confidence intervals than those obtained using the MGL-model. Also this result is consistent with expectations (Mosleh and Siu, 1987). Use of an alternative model for manual depressurization did not lead to any dramatic changes in comparison with the reference case. The code SENS was applied when studying two additional sources of modeling uncertainties. This includes impact of an alternative extension scheme in the context of design- and application-oriented screening of common cause failure events (very small effect for the sequence studied) and use of recently published data (Knochenhauer, 1988) for relationship between

MOV-failure probability and test interval length (strong reduction of the accident sequence frequency). The last mentioned case is regarded by ATOM as a much more realistic representation of the phased mission situation and will be fully integrated into the uncertainty analyses to be performed in the next phase of the project. It should be noted that the SENS code provides point estimates based on mean values for the basic events included in the cut-set list. Thus, these results can only be directly compared with uncertainty analyses based on the use of an uncorrelated sequence function.

STUDSVIK's sensitivity analysis concentrated on identification of those basic events which contribute most to the overall uncertainty. In order to calculate the uncertainty contribution of a specific basic event i, the corresponding variable x(i) was kept constant while all the other variables varied according to their distributions. The variance obtained in this way is smaller than the overall variance. Thus, the reduction of the variance is a quantitative measure of the uncertainty contribution from the variable i. Somewhat surprisingly the greatest deviation from the mean value and the greatest reduction in standard deviation was obtained for the intermittently operated MOVs, followed by manual depressurization and initiating event. The influence of the uncertainty of quadruple CCF is negligible in this context. This might be a consequence of uncertainty distribution and modeling assumptions used by STUDSVIK.

In VTT's analysis the distribution is broadest and the mean is highest in the reference case. This is due to the use of maximum entropy distribution. The two other cases involving application of Dirichlet distributed CCF-probabilities for MOVs on the one hand, and component failure probability distributions based on uniform beta prior, MGL-model and T-book failure data (Bento et al., 1985) on the other hand, are rather near to each other. In all three cases the manual depressurization model has been the same and thus its effect on uncertainty distributions is similar in all cases.

Similarly, the important parameter linking together the single failure probabilities for MOVs in the repeated action model has been the same in all cases. In addition to the three cases described, VTT varied arbitrarily reliability data for MOVs and for corresponding CCF-probabilities. As expected, the impact on the accident sequence frequency was strong. Finally, using the MONTEC code a sensitivity study based on fractiles of the model parameter distributions was performed. In all three cases mentioned above the parameters describing the quadruple failure probability and the repeated activation parameter are the most important. This conclusion is partly consistent with the results of sensitivity analysis performed by STUDSVIK. Although the accident sequence frequency is proportional to the depressurization failure probability, according to VTT-analysis the sensitivity to individual parameters in VTT's model of human interaction is weak.

Figure 4.2 shows the results obtained by different groups. From STUDSVIK's sensitivity analysis in the form of reduced variances only these cases which have led to the most significant variance reductions in comparison with the reference case, are displayed. The distributions generated for the reference case are displayed in Figure 4.3.

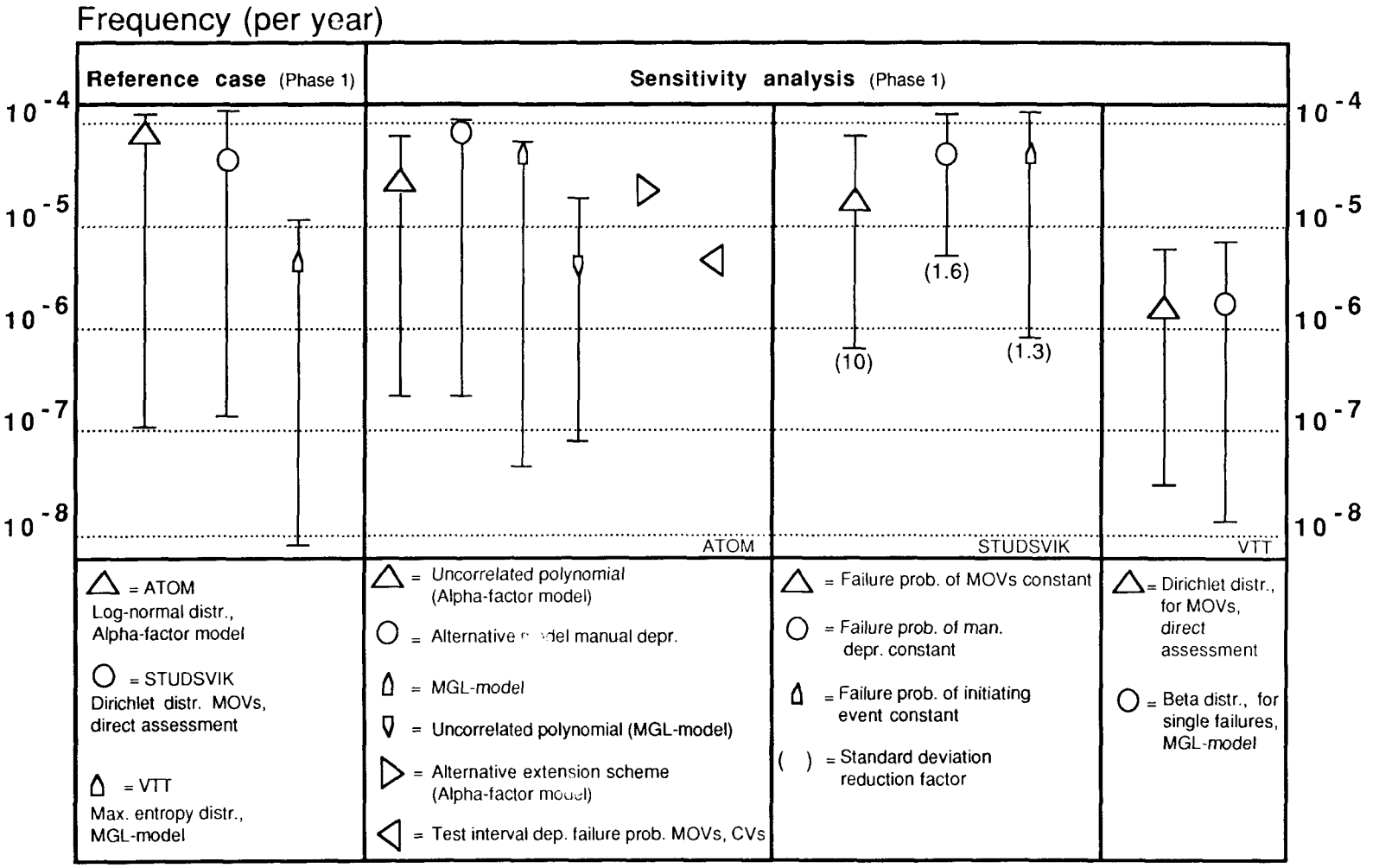


Figure 4.2

Initial (phase 1) results on uncertainty and sensitivity analysis for sequence T_fUX2

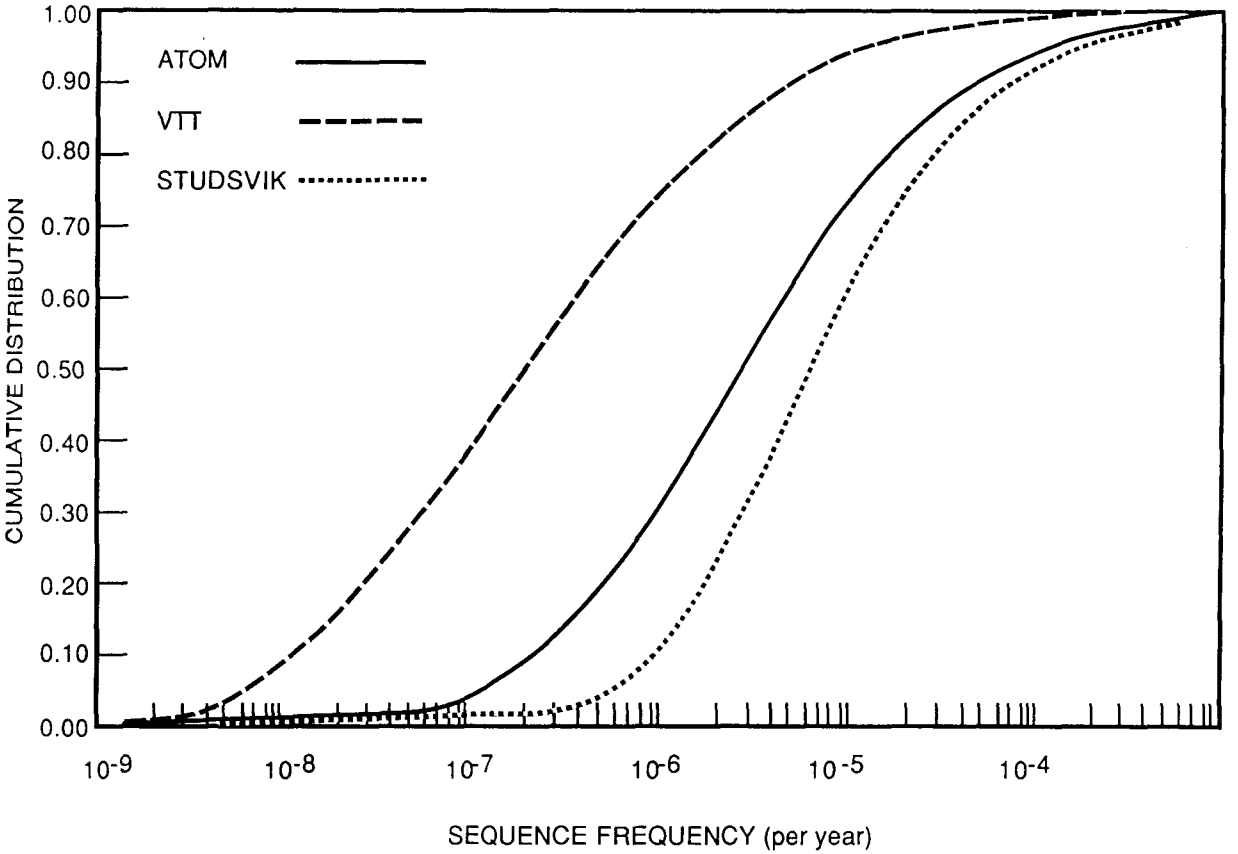


Figure 4.3

Cumulative distribution function for the frequency of sequence T_fUX2 according to different groups (phase 1)

The statistical uncertainties are apparently large. This was expected since the analysed sequence involves critical human interaction combined with common cause failure of a system with high level of redundancy. The uncertainty associated with manual depressurization is substantial according to all groups. This is natural since no empirical evidence exists for such operator action. The estimates of the mean value of failure probability of this operator action differ by a factor of 8.6 at most. The corresponding factor for the quadruple CCF is 5.3. This factor could be significantly larger if the same model had been used in the CCF-context for the repeated activation of MOVs. However, in this case while two groups arrived at a very broad uncertainty interval, that is not the case for the third group (STUDSVIK). The reasons for these discrepancies are to be found primarily in the interpretation of data. This conclusion is consistent with findings of the Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987) Design-oriented screening was only used by ATOM in the process of CCF-estimation. In evaluation of the frequency of the initiating event relatively small discrepancies have been observed between the groups since the same operating experience has been used. One of the groups (VTT) applied in this context a data combination procedure, thus taking into account relevance of the material available for the particular application.

On the sequence level the mean values estimated by the groups for the reference case differ at most by a factor of 17.7. The overall uncertainty interval (90%) covers more than two decades (STUDSVIK) and three decades (ATOM, VTT). The ratio between mean values and median values is very large for all groups, i.e. 9.6 (STUDSVIK), 20.4 (VTT) and 28.6 (ATOM). These results may be explained by the above mentioned observations concerning the most important elements and by the large impact of "state-of-knowledge" dependence. As expected the use of maximum entropy distribution results in the broadest confidence intervals.

Several types of sensitivity analyses have been performed. Among the modeling uncertainties which have been investigated we may mention: use of different CCF-quantification models (direct assessment, alpha-factor method, MGL-model), use of different extension schemes in the context of handling of CCF-data, time windows for operator actions and time dependences in phased mission operation. The use of recently published (Knochenhauer, 1988) results on failure probability of MOVs leads to a significant reduction of the frequency of the analysed accident sequence. This is due to the fact that the failure probability is dominated by the time-dependent part which, however, gives a relatively small contribution during the relatively short phased mission time period. It was confirmed and reflected by the results on the sequence level that the alpha-factor method leads to significantly larger uncertainty intervals than the MGL-model.

The parametric uncertainties have been studied by evaluating the impact of "state-of-knowledge" dependences and by ranking the dominating uncertainty contributors. The goal of such ranking is to identify the points where the reduction of uncertainty (improving the state-of-knowledge) could lead to upgrading of our decision making capability. In this context STUDSVIK has introduced reduction of the variance as a quantitative measure of the uncertainty contribution from a particular

variable. According to STUDSVIK's analysis the ranking of dominating uncertainty contributors is in the present case different from the ranking of dominating frequency contributors. The failure frequency of MOVs in intermittent operation is the main uncertainty contributor according to the analyses carried out by all teams. This is even more pronounced when parametric CCF-models are used; quadruple and triple CCFs constitute very important uncertainty contributors in ATOM's and VTT's analyses. This is not the case in STUDSVIK's study, which may be explained by the fact that uncertainties associated with CCF-treatment are relatively small in their analyses and CCFs of MOVs have not been considered in connection to subsequent demands.

Naturally, the sensitivity studies do not cover all modeling uncertainties. The logical model of the plant, the cut-set list and a comprehensive set of data were provided as a basis for this study and have not been questioned. For the estimate of the initiating event frequency the data base could be expanded by using the operational experience from a significantly larger number of reactor-years. The substantial uncertainties associated with the process of CCF-data screening have not been analysed. The simplified model for representing the operator interactions does not take into account e.g. the possibility of errors of commission. From the point of view of the time available for manual depressurization it has been assumed that the CCF in four trains of the auxiliary feedwater system occurs immediately after the initiating event. On the other hand, the CCF-contributions have been calculated on the basis of 24 hours' mission time. Naturally, conditions governing the performance of operators would be more favorable if the CCF occurred later in time and if not all redundant trains failed simultaneously. In such situation recoveries could also be possible, which would result in reductions of the accident sequence frequency.

As a result of phase 1 it has been recommended that the subsequent activities of the Nordic reference study on uncertainty and sensitivity analysis should concentrate on problems identified as important but treated superficially in phase 1. This includes modeling of intermittent operation of MOVs, which according to the results of one of the sensitivity analyses is not realistic in any of the reference cases. One of the groups (ATOM) anticipated that improved modeling of phased mission operation combined with use of a more realistic uncertainty distribution for MOVs would decrease the sequence frequency by a factor of 5-10. Other problems of interest for subsequent phases concern e.g. convergence of simulation codes, effect of log-normal approximation, and interpretation and impact of uncertainties in the context of decision making.

4.2.7 Comparison of computer codes for uncertainty analysis (phase 2)

The objective of this phase was to compare the simulation codes applied by different working groups participating in the project. In the first phase a

sample size of 5000 realizations was considered sufficient to achieve adequate precision in the calculations. In order to compare the codes and to evaluate the effect of using the log-normal approximation, it was agreed that two common cases will be analysed using different sample sizes (1000, 2000, 4000, 8000 and 16 000).

Both cases consist of the frequency model originally applied by STUDSVIK in phase 1. However, in the second case considered in phase 2 the original uncertainty distributions were approximated by log-normal ones. In the approximation process mean values and standard deviations of the original distributions were kept fixed.

The results obtained by different groups are displayed in Figure 4.4. Due to the limitations of the SAMPLE-code with respect to choice of distributions, ATOM's contribution to phase 2 does not include use of STUDSVIK's original distributions.

In addition to mean and standard deviation values shown in the figure also 0.5, 5, 50, 95 and 99.5 percentiles were calculated. These distribution characteristics are according to all groups quite insensitive to the sample size. While 3000-4000 realizations seem to be sufficient for percentiles, the mean value and standard deviation can change quite substantially even for much greater sample sizes. This is even more apparent from supplementary calculations for sample sizes within the interval 1000-16 000. A plausible explanation to the leap-like behaviour could be the presence of rare extreme values for the sequence frequency, the probability of which increases with increasing sample sizes. However, the results obtained indicate that for the actual problem reasonably reliable estimates may be obtained using 5000-10 000 simulations. MOCARE-results deviate from the others when original distributions are used. This might be attributed to the approximation of Dirichlet distribution, used by RISØ. When the approximation was substituted by direct generation of the distribution, results similar to those of the other groups were obtained. The conclusion to be drawn from the calculations performed is that if more precise mean value estimates are desired, development of analytical approach may be necessary.

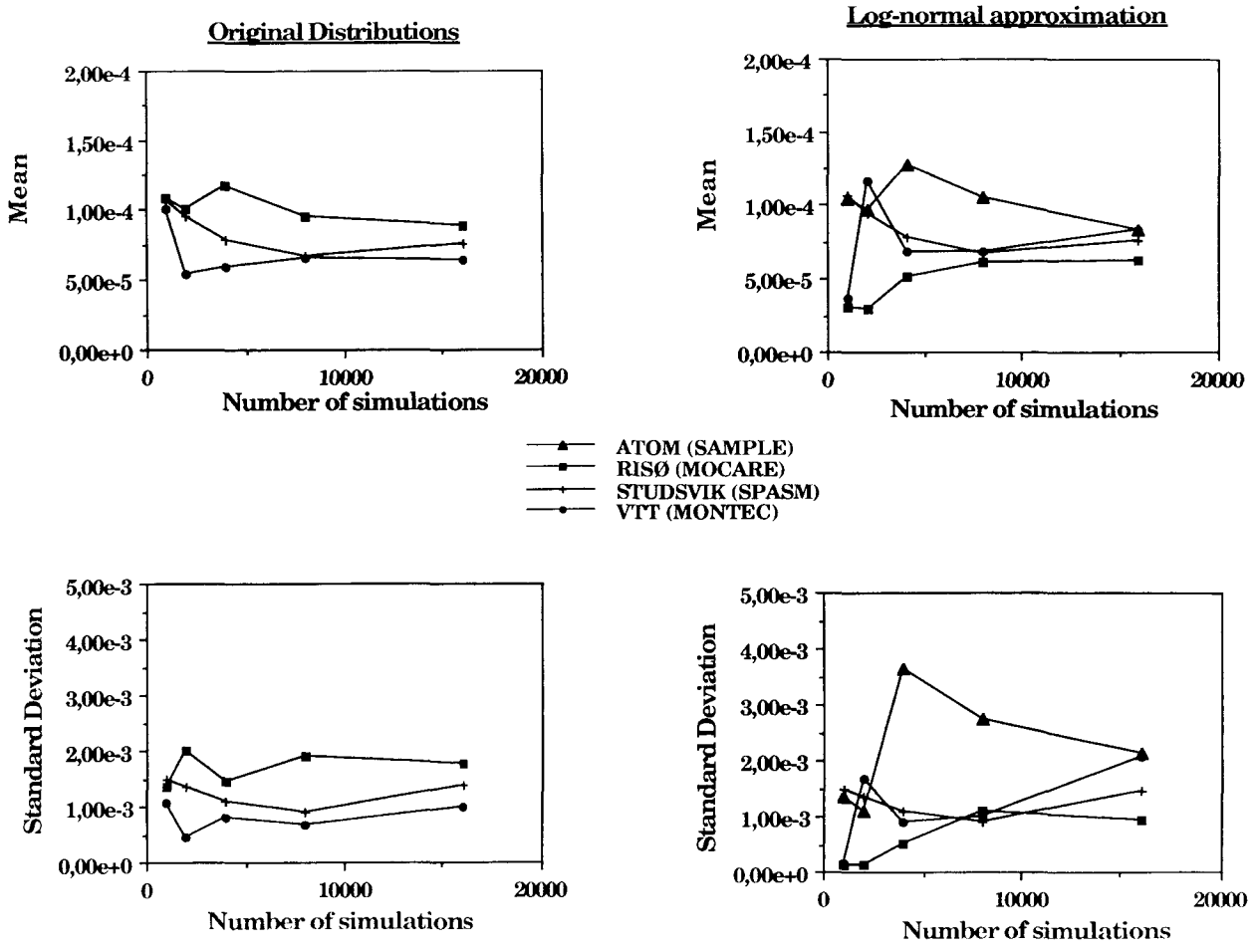


Figure 4.4

Mean and standard deviation values obtained by different groups in phase 2

There are only small differences between the estimates obtained using original distributions and log-normal approximation, respectively. In STUDSVIK's and VTT's case the mean value and standard deviation become slightly larger when log-normal approximation is being used. Similar results were obtained when SPASM was applied on ATOM's phase 1 polynomial using both log-normal and original distributions. The agreement between SPASM and SAMPLE was excellent in the log-normal case.

Finally, ATOM, and RISØ investigated the impact of terms of higher order integrated into the uncertainty polynomial (which originally was based on the first moment approximation). In both cases use of a more exact representation of the problem leads to a rather dramatic reduction of the mean and the standard deviation while the percentiles are not affected in such a drastic way. The strong reduction of the mean value (by a factor of 2.7 and 3.1, respectively), may be attributed to high degree of dependency between the cut-sets and large uncertainty (according to T-book data) associated with MOVs.

While some of the observations made as a result of phase 2 comparison should be generally valid, the numerical significance is definitely problem dependent.

4.2.8 Evolution of best estimate results (phase 3)

Best estimate results have been generated by each group using experiences from the preceding phases of the reference study. The input uncertainty distributions for the most important elements (failure probability of a MOV in phased mission operation, initiating event, quadruple CCF in the auxiliary feedwater system and manual depressurization) are shortly summarized below and contrasted with those used in phase 1. This is followed by a summary of results for the selected sequence.

4.2.8.1 Input uncertainty distributions

Table 4.6 summarizes characteristics of the analyses carried out in phase 1 and 3. Only reference cases are reflected in the table. In addition, sensitivity analyses have been carried out, including alternative approaches.

Table 4.6

Analysis characteristics (phase 1/phase 3)

Element	Group	Method	Distribution[a]
Initiating event	ATOM	-	Discrete Poisson[b]/ Discrete Poisson[b]
	STUDSVIK	-	Gamma/Gamma
	VTT	-	Mixture of Gamma/ Mixture of Gamma
MOV-failure in phased mission operation	ATOM	Time-dep.(eng. judgement)/ Time-dep.(linear standby failure model)	Beta[b]/Log-normal
	STUDSVIK	-"-	Beta/Beta prior for q, Gamma prior for λ
	VTT	-"-	Maximum entropy/ Uniform prior and discretized posterior for q
Common cause failures	ATOM	Alpha-factor/ Alpha-factor	Beta[b]/Beta
	STUDSVIK	Direct assessment/ Alpha-factor	Dirichlet/Dirichlet
	VTT	Multiple Greek Letter/ Direct assessment	Maximum entropy/ Dirichlet
Manual depressurization	ATOM	THERP, HRA Handbook/ THERP, HRA Handbook	Log-normal/ Log-normal
	STUDSVIK	THERP, HRA Handbook/ Mixed[c]	Log-normal/ Mixed (tabular, log-normal)
	VTT	Operator action tree, subjective judgement/ Human cognitive reliability, subjective judgement	Maximum entropy/ Mixed (Uniform, Weibull, Beta)

[a]Concerns either final distribution for the element considered or distribution for parameters involved

[b]Approximated by a log-normal distribution

[c]Phase 1 distributions from all groups weighted equally

Below follow some comments concerning numerical values for distribution parameters of the most critical elements, as obtained in phase 1 and 3, respectively. Some distribution characteristics obtained in phase 3 are shown in Table 4.7.

1) Initiating event. No changes of phase 1 parameters have been made by any of the groups. The discrepancies between the groups are rather small from practical point of view.

2) MOV-failure in phased mission operation. The model and data used for this event are of central importance since MOVs are represented in a large number of cut-sets (implicitly in 85 out of 88 cut-sets). In the first phase all groups used a simplified approach to this problem and time-dependent data were based on judgement. The phase 3 approach is, on the other hand, based on a linear standby failure model and on data which clearly reflect the strong correlation between MOV-failure probability and test interval length (Knochenhauer, 1988) ATOM and STUDSVIK used the same comprehensive database in this context, which explains the good agreement between these groups. As expected, the more realistic approach leads to significantly lower estimates of the mean and standard deviation. VTT, on the other hand, used a more exclusive set of data (statistical evidence only for MOVs in auxiliary feedwater systems, data from four plants).

3) Common cause failures. Both STUDSVIK and VTT changed their approaches to CCF-quantification as compared to phase 1, while ATOM used the same model combined with more realistic time-dependent data for MOV-failure probability. The best estimates of quadruple CCF-probabilities are very close to each other, while the mean values differed by at most a factor of 5.3 in phase 1.

   The discrepancies in phase 3 would have been relatively large given use of the same model in the CCF-context for the repeated activation of MOVs. Two groups (ATOM, STUDSVIK) applied the same approach to this problem, while VTT considered the contributions associated with subsequent demands as negligible. In addition, differences between the groups, identified in the Nordic CCF-data Benchmark Exercise still prevail (e.g. use of design-oriented screening, use of extension schemes, treatment of potential CCFs). Thus, the numerical agreement is more a result of coincidence rather than a proof of consensus.

4) Manual depressurization. Also in this case the numerical agreement is much better than in phase 1. The original estimates of the mean value for the operator failure probability differed by a factor of 8.6 at most. STUDSVIK decided in view of the uncertainties involved to use all the distributions earlier generated by the working groups and to assign to them equal weights. Naturally, the resulting mixed distribution is - with respect to the mean value - somewhere between the most narrow and the broadest of the original ones, while the spread of the distribution tends to increase compared to the original spreads. VTT changed both the model and data which led to a significant increase of the operator failure probability. This increase is mainly attributed to subjectively assigned parameter values.

Table 4.7

Distribution parameters for critical elements (phase 3)

Group	Element	Mean	Stand.dev.	Median	5-per-centile	95-per-centile
ATOM	Initiating event	0.23	0.16	0.19	0.07	0.53
STUDSVIK	(per year)	0.25	0.13	0.23	0.09	0.48
VTT		0.27	0.14	0.25	0.09	0.55
ATOM	MOV-failure in pha-	$1.2 \cdot 10^{-2}$	$1.3 \cdot 10^{-2}$	$7.7 \cdot 10^{-3}$	$2.4 \cdot 10^{-3}$	$3.5 \cdot 10^{-2}$
STUDSVIK	sed mission opera-	$1.4 \cdot 10^{-2}$	$1.0 \cdot 10^{-3}$	$1.2 \cdot 10^{-2}$	$1.8 \cdot 10^{-3}$	$3.3 \cdot 10^{-2}$
VTT	tion (per demand)	$4.1 \cdot 10^{-2}$	$2.9 \cdot 10^{-2}$	$3.5 \cdot 10^{-2}$	$7.6 \cdot 10^{-3}$	$9.5 \cdot 10^{-2}$
ATOM	Quadruple CCF	$3.5 \cdot 10^{-3}$	$1.9 \cdot 10^{-2}$	$1.2 \cdot 10^{-3}$	$1.3 \cdot 10^{-4}$	$8.6 \cdot 10^{-3}$
STUDSVIK	(per demand)	$3.6 \cdot 10^{-3}$	$4.6 \cdot 10^{-3}$	$2.4 \cdot 10^{-3}$	$3.2 \cdot 10^{-4}$	$1.1 \cdot 10^{-2}$
VTT		$2.6 \cdot 10^{-3}$	$2.2 \cdot 10^{-3}$	$2.1 \cdot 10^{-3}$	$3.6 \cdot 10^{-4}$	$6.8 \cdot 10^{-3}$
ATOM	Manual depressuri-	$9.1 \cdot 10^{-3}$	$2.9 \cdot 10^{-2}$	$3.1 \cdot 10^{-3}$	$6.4 \cdot 10^{-4}$	$3.1 \cdot 10^{-2}$
STUDSVIK	zation (per demand)	$1.3 \cdot 10^{-2}$	$3.2 \cdot 10^{-2}$	$3.6 \cdot 10^{-3}$	$6.0 \cdot 10^{-4}$	$5.1 \cdot 10^{-2}$
VTT		$1.2 \cdot 10^{-2}$	$1.3 \cdot 10^{-2}$	$6.3 \cdot 10^{-3}$	$1.1 \cdot 10^{-3}$	$3.9 \cdot 10^{-2}$

4.2.8.2 Results on accident sequence level

The results of analyses performed by different groups for their reference cases in phase 1 and 3, are presented in Table 4.8. Cumulative distribution function obtained in phase 3 by different groups is shown in Figure 4.5.

Table 4.8
Results on sequence level (reference case; phase 1/phase 3)

Group (per year)	Mean (per year)	Stand. dev. (per year)	Median (per year)	5-percentile (per year)	95-percentile (per year
ATOM	$8.3 \cdot 10^{-5}$/ $1.2 \cdot 10^{-5}$	$1.8 \cdot 10^{-3}$/ $3.3 \cdot 10^{-4}$	$2.9 \cdot 10^{-6}$/ $8.6 \cdot 10^{-7}$	$1.2 \cdot 10^{-7}$/ $5.6 \cdot 10^{-8}$	$1.1 \cdot 10^{-4}$/ $2.1 \cdot 10^{-5}$
STUDSVIK	$6.4 \cdot 10^{-5}$/ $1.2 \cdot 10^{-5}$	$5.6 \cdot 10^{-4}$/ $6.7 \cdot 10^{-5}$	$6.7 \cdot 10^{-6}$/ $2.0 \cdot 10^{-6}$	$6.4 \cdot 10^{-7}$/ $1.2 \cdot 10^{-7}$	$1.7 \cdot 10^{-4}$/ $4.5 \cdot 10^{-5}$
VTT	$4.7 \cdot 10^{-6}$/ $1.1 \cdot 10^{-5}$	$3.1 \cdot 10^{-5}$/ $2.4 \cdot 10^{-5}$	$2.3 \cdot 10^{-7}$/ $4.8 \cdot 10^{-6}$	$6.8 \cdot 10^{-9}$/ $4.4 \cdot 10^{-7}$	$1.2 \cdot 10^{-5}$/ $4.2 \cdot 10^{-5}$

Note that the results obtained by ATOM in phase 3 are based on an extended uncertainty polynomial including higher order terms up to the third order, as opposed to first moment approximation used by the other groups. However, it has been shown in a sensitivity study that the impact of such an approximation is negligible in this particular case.

This contrasts with the results from phase 2, where use of extended "common" polynomial resulted in a very strong reduction of the mean and standard deviation. The observed difference may probably be attributed to the fact that the failure probability of MOVs (which constitute the main source of dependency between the cut-sets) is both much smaller and characterized by a more narrow uncertainty distribution in ATOM's best estimate.

The agreement between the results obtained by the three groups was much improved in phase 3. Thus, the estimates of the mean for accident sequence frequency are almost identical, while they differed in phase 1 by a factor of 17.7 at most. Also the overall uncertainty interval, although large, is quite similar according to all groups. The main reasons for the better agreement are: similar modeling of MOV-phased mission operation (all groups), use of the same original data for MOVs (ATOM, STUDSVIK), which also affects

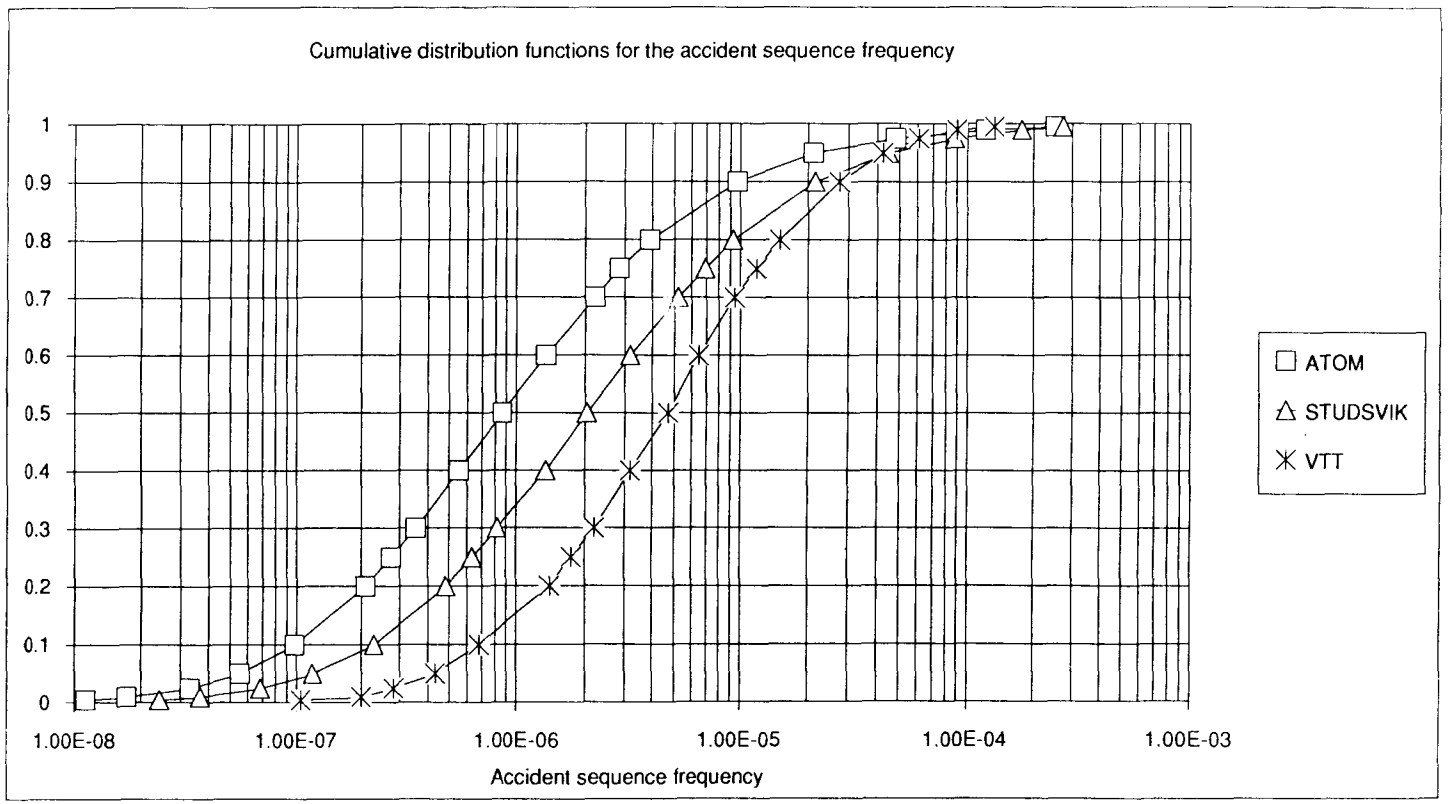


Figure 4.5

Cumulative distribution function for the frequency of sequence T_fUX2 according to different groups (phase 3)

CCF-quantification since both these groups use a parametric model (alpha-factor), and significantly modified approach to the treatment of manual depressurization (STUDSVIK, VTT).

In addition to the reference case analyses, a number of sensitivity analyses have been carried out. Thus, ATOM performed uncertainty propagation using also SAMPLE and log-normal approximation of the original distributions. In addition, impact of use of an alternative distribution for the initiating event, of more pessimistic assumptions in modeling of manual depressurization, of introduction of automatic depressurization and of "state-of-knowledge" dependences, have been studied by ATOM. The findings of main interest are: relatively good agreement between the results obtained using original distributions and log-normal approximation, significant impact of "state-of-knowledge" dependences and a dramatic reduction of the mean of the sequence frequency (by a factor of 20) due to automatic depressurization.

VTT's sensitivity analyses include use of maximum entropy distributions for independent failure probabilities and impact of taking into account the possibility of CCF-occurrence during repeated MOV-activations. While the impact of application of an alternative distribution is very small, the contribution of additional CCFs is quite large. However, in this context the aspect of time-dependence has not been taken into account.

STUDSVIK's sensitivity analyses concern ranking of uncertainty contributors, and use of more comprehensive statistical material for estimation of initiating event frequency. The concept of uncertainty contributors was introduced already in phase 1. According to the results obtained in phase 3 the three most dominating uncertainty contributors are the manual depressurization, quadruple CCF in the auxiliary feedwater system and the reciprocating pumps in this system. The surprisingly large contribution from these pumps can be explained by the alpha-factor modeling of CCFs, by which the uncertainty of single failure frequency strongly propagates to all levels of CCFs.

Figure 4.6 shows the survey of reference case results of phase 1 and 3. Phase 3 results of sensitivity analyses as compared to those of the reference case are illustrated by Figure 4.7.

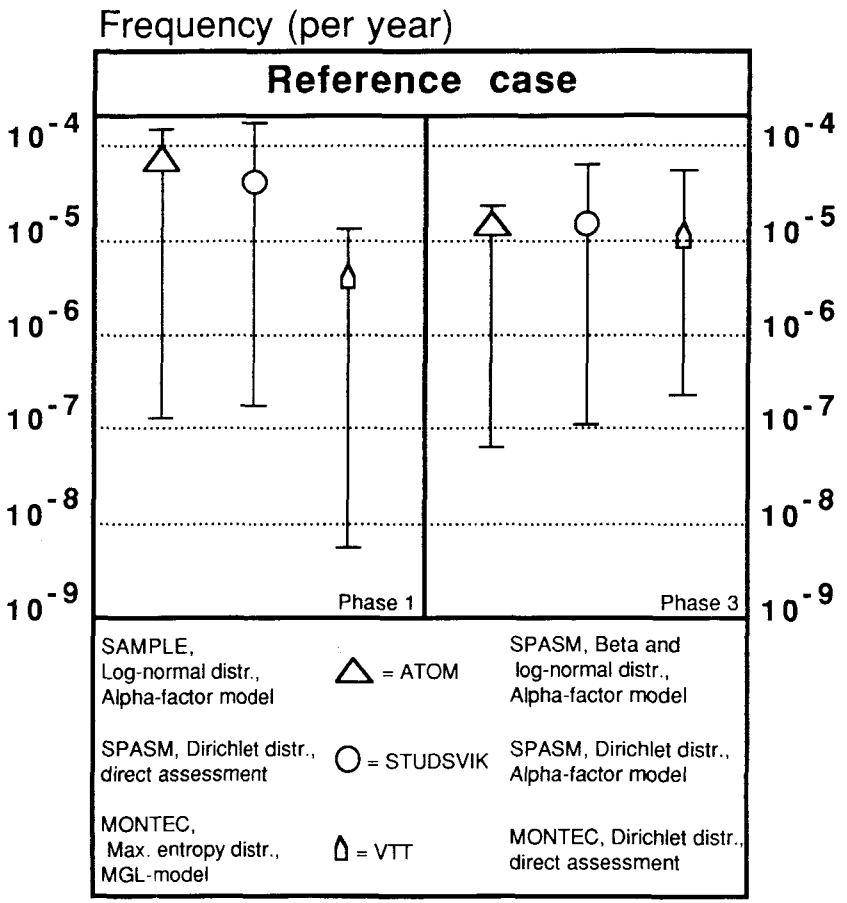


Figure 4.6

Reference case (phase 1 and phase 3) results of uncertainty analysis for sequence T_fUX2

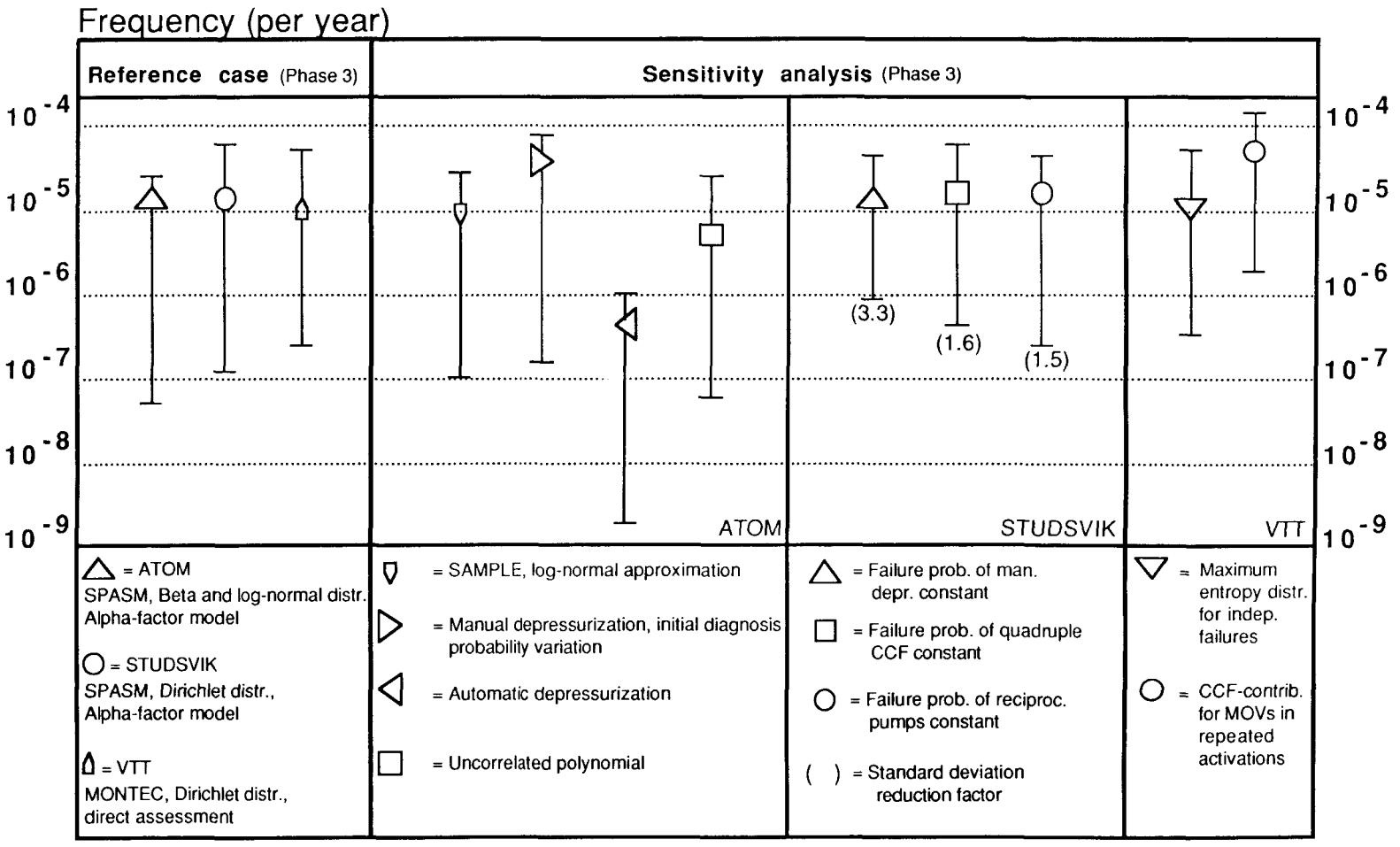


Figure 4.7

Reference case (phase 3) and sensitivity analysis (phase 3) results for sequence T_fUX2

4.2.9 Conclusions

The parametric uncertainties associated with the frequency of the analysed accident sequence are apparently large. This was expected since the sequence involves a critical human interaction combined with common cause failure of a system with high level of redundancy.

As a result of modification of the approaches to modeling of some of the critical elements, used in the initial analysis, the numerical agreement between the groups has been drastically improved in the best estimate phase. The main reasons for that are: a more realistic representation of the phased-mission operation, use of new time-dependent data for MOVs and extensive changes of the modeling of manual depressurization. However, although a certain degree of consensus has been reached with respect to some modeling aspects, the numerical agreement is to some extent coincidental. The CCF-contributions for example have been assessed using different approaches to treatment of data and the scope of CCF-analysis is varying. These differences appear to take out each other, leading to comparable numerical values.

The overall uncertainty interval (90%) for the accident sequence covers more than two decades in the best estimate case. In this context the uncertainties associated with initiating event frequency are relatively small due to availability of operating experience. This is definitely not the case for the CCFs with high failure multiplicity and for the operator action involved.

The ratio between mean and median values of the sequence frequency is substantial i.e. 14.0 (ATOM), 6.0 (STUDSVIK) and 2.3 (VTT), but has generally been lowered compared with phase 1 results (28.6, 9.6 and 20.4, respectively). These results may be explained by the features of distributions used for the critical elements and by the impact of "state-of-knowledge" dependences. In VTT's case the most important change, which probably can explain the drastic reduction of the ratio above, is attributed to use of Dirichlet distributions instead of maximum entropy for CCFs involved. The distributions used by VTT for CCFs in the best estimate phase are much more narrow than those of phase 1.

The main methodological insights are as follows:

1) Direct assessment and alpha-factor method constitute two acceptable approaches to quantification of CCF-contributions. Use of Multiple Greek Letter (MGL) model may result in underestimation of the mean value and the uncertainty interval. The approach to treatment of raw data (identification, screening, extension, weighting) is still of most critical importance.

2) Assumptions concerning boundary conditions for modeling of human interactions have decisive impact on the analysis results. Independently of which model is used subjective judgement plays a central role when assigning failure probabilities to operator interactions. However, the numerical consequences of changes in state-of-knowledge can be quite different when applying various models. This issue needs further investigations.

3) Although the validity of the linear standby failure model has been generally demonstrated (Knochenauer, 1988), its applicability in the case of phased mission operation has not been analysed. However, the model has proved to be very useful in the sequence analysis of this project.

4) Use of log-normal approximation for the original distributions involved gives satisfactory results. This conclusion is, however, problem dependent.

5) Use of higher order terms in the uncertainty polynomial as opposed to first moment approximation represents the preferred approach, eventhough the actual impact depends on the degree of dependency between the cut-sets and on the absolute level of failure probabilities involved. The numerical importance of this aspect may be negligible when generating point estimates and large when uncertainty distributions are properly propagated.

6) "State-of-knowledge" dependences may have a surprisingly large impact on the quantitative results and must be taken into account in order to avoid underestimation.

7) Reduction of the variance may be used as a practical and simple measure of the uncertainty contribution from a particular variable. In this way the principal uncertainty contributors may be ranked.

8) Progress has been made in applications of the Bayesian approach including development of Bayesian procedures to estimate the model parameters and experience of Monte Carlo simulation from multidimensional distributions.

From practical point of view the quantification of the impact of automatic depressurization instead of the manual one, is of major interest. The frequency of the selected sequence, which is by far the most dominant contributor to the total damage frequency of Forsmark 3 PSA (ABB Atom AB, 1985) would be reduced by a factor of 20 as a result

of such design modification. The effect is overwhelming, although large uncertainties are associated with the estimate of the reliability of automatic depressurization (determined by a 3-out-of-8 failure of pressure relief valves).

The comparison of computer codes for uncertainty propagation (MONTEC, MOCARE, SAMPLE, SPASM) shows good agreement. In some cases improvements of the codes were implemented in the course of the project. The precision of mean and standard deviation generated by Monte Carlo technique is much more dependent on the sample size than the precision of percentiles. Substantial changes in mean and standard deviation have been observed for sample sizes greater than 10000, while the percentiles become stable at 2000-4000 simulations. Still, reasonably reliable estimates of the mean and standard deviation have been obtained using 5000-10000 realizations. If more precise estimates are required development of an analytical approach might be necessary.

Generally, the present study has shown that uncertainty analysis based on the current Swedish PSAs and data is feasible, requires reasonable resources, and may be carried out using the available computer codes. Improvements with respect to more realistic uncertainty distributions for certain component types and with respect to increased flexibility of the codes, are possible, and in some cases are already being implemented.

4.3 Sensitivity Studies of Common Cause Failures and Human Interactions in Swedish PSAs

4.3.1 Background

Systematic qualitative retrospective analyses of the treatment of dependencies (Hirschberg, 1987a) and human interactions (Bengtz and Hirschberg, 1987) in Swedish PSAs, described in subchapters 2.3 and 3.3, have lead to identification of a wide spectrum of discrepancies. These differences may concern level of ambition, degree of detail, scope, approach to modeling and quantification, and documentation of the studies.

Recommendations from the qualitative phase comprise a list of specific cases to be analysed in sensitivity studies, proposals for future Nordic research

projects and suggestions for improvements or supplements to existing analyses. In the following the main results of sensitivity studies will be covered. The analysis is based on the PSAs for Ringhals 1 (R1), Barsebäck 1 (B1), Forsmark 3 (F3), Oskarshamn 3 (O3) and Oskarshamn 1 (O1); references (Swedish State Power Board, 1984; Sydkraft, 1987; ABB Atom AB, 1985; OKG AB, 1986 and OKG AB, 1987). Ringhals 2 (R2) PSA (NUS-Corporation, 1984) has not been included in the sensitivity studies.

Table 4.9 shows a fragment of a survey of some of the features of CCF-analyses in these PSAs.

A corresponding comparison concerning the treatment of human interactions of type 3 (by following procedures during the course of an accident, plant personnel can operate standby equipment which will terminate the accident; classification according to (Hannaman and Spurgin, 1984)) is given in Table 4.10.

4.3.2 Common cause failures

Table 4.11 shows contribution of CCFs to core damage frequency for different plants according to the PSAs. It should be noted that other failures (independent, human interactions) must occur after an initiating event in combination with CCFs, in order to cause core damage. Thus, the numbers given in Table 4.11 correspond to risk reduction which would be achieved if all CCFs accounted for had negligible probabilities.

Table 4.11
CCF-contributions to core damage frequency

PSA	Contribution (%)
O1	20
B1	19
R1	44
F3	90
O3	75
R2	15

Table 4.9

Selected features of CCF-analyses in Swedish PSAs

Feature	Oskars-hamn 1	Barse-bäck 1	Ring-hals 1	Fors-mark 3	Oskars-hamn 3	Ring-hals 2
CCF-represen-tation in fault trees	Component tree level (CTL)	CTL	Function tree level (FTL)	System train level (STL)	CTL	FTL
Method for CCF-quantifi-cation	Multiple Greek Letter (MGL) model	Beta-factor model	C-factor model (extended)	MGL	MGL	C-factor model
Source of CCF-data	Engineering judgement	Engineering judgement	US-experi-ence	Swedish/ Finnish experience	US-experi-ence	US-experi-ence

Table 4.10

Selected features of type 3 human interaction analyses in Swedish PSAs

Feature	Oskars-hamn 1	Barse-bäck 1	Ring-hals 1	Fors-mark 3	Oskars-hamn 3	Ring-hals 2
Representation	Covered by fault trees (FT) and event trees (ET)	FT & ET	FT & ET	FT & ET	FT & ET	FT & ET
Basic approach	Case-by-case	Case-by case	Operator action trees (OAT)	OAT-principles	Case-by-case	OAT-principles
Source of data	Time-reliability curve (TRC; assumed), engineering judgement	TRC (assumed), Handbook, engineering judgement	Situation-specific analysis, Handbook, engineering judgement	NREP cognitive error screening curve, TRC (assumed), Ringhals 1 PSA, engineering judgement	Engineering judgement, time independent probability (in some cases)	TRC (NUS-control room team)

The relative CCF-contributions are high for four-divisional plants (F3 and O3), characterized by consequent physical and functional separation of redundant equipment.

This is natural since such a design efficiently reduces potential for serious outcome of combinations of independent failure events. Other advantages of this design philosophy include minimization of the impact of common cause initiators (CCIs) and possibilities to introduce a more flexible and efficient strategy with respect to maintenance activities (Hirschberg and Knochenhauer, 1987).

The impact of CCFs on the PSA-results motivates performance of sensitivity studies. In the qualitative part of the project large discrepancies in numerical results have been observed (e.g. for diesel generator systems), which are not always motivated by actual differences in design and operation of the plants considered. On the other hand, the existing differences are frequently not reflected in data used. The survey of the impact of intercomponent CCFs on the dominant accident sequences according to different PSAs showed (Hirschberg, 1987a) that motor-operated valves (MOVs) and pumps are the principal CCF-contributors. Thus, the future efforts should be concentrated on supplying better estimates of CCF-contributions for these component types. Other important components in this context are diesel generators, gas turbines, scram valves, pressure relief valves and reactor protection system (RPS)-logic channels.

4.3.2.1 Impact of lower failure multiplicities (Bengtz and Hirschberg, 1988)

The C-factor model (Parry, 1984) used in R1 and R2 PSAs, and the beta-factor model (Fleming, 1975) used in B1 PSA do not distinguish between the different failure multiplicities. The consequence of using these models is that only one (the highest) failure multiplicity is taken into account and the lower failure multiplicities are neglected in systems with three or four redundant trains. This assumption could lead to underestimation which, however, probably is compensated by the overestimation of the highest failure multiplicity, an intrinsic feature of methods based on only one CCF-parameter. On the other hand, the MGL-model (Fleming and Kalinowski, 1983) used in the O1, O3 and F3 PSAs provides the possibility to distinguish between the different failure multiplicities.

The impact of lower failure multiplicities has been directly assessed for F3 and O3 PSAs. On the core damage level the total contribution of double and triple CCFs is 7.1 % in the case of F3 PSA and 1.2 % in the case of O3 PSA. Thus, given a reasonable choice of higher-order parameters the contributions to core damage frequency from lower failure multiplicities are small for plants with high level of redundancy. This conclusion is important when assessing the impact of neglected contributions in case of studies using simple CCF-models (B1 and R1). The lower failure multiplicities are not expected to contribute significantly to the core damage frequency for these plants due to the lower degree of redundancy and due to prevailing success criteria. Nevertheless, it is clear that neglect of these contributions results in underestimation of the frequencies of accident sequences. Consequently, it is recommended that whenever applicable the simple models of some of the studies should be replaced by models which properly take into account all relevant failure multiplicities.

4.3.2.2 Plant-specific CCF-parameters for motor-operated valves (Bengtz and Hirschberg, 1988)

A number of CCFs for MOVs have been identified within the Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987). This material is based on the Swedish operating experience and in spite of its limitations from the statistical point of view, is regarded as more relevant for applications concerning Swedish plants than alternative use of US-experience. Following the generation of plant-specific parameters, the four PSAs (B1, R1, F3, O3) were requantified using the new sets of parameters and the available cut-set lists. In this context some engineering approximations have been used. However, the applied approach is based on consequent application to all plants of similar assumptions concerning treatment of CCF-data. In this way plant-specific issues are emphasized, but at the same time the available PSAs become more comparable (at least with respect to treatment of CCF-contributions for MOVs).

Seven CCF-events from the Nordic Benchmark Exercise (Hirschberg, ed., 1987) constitute the basis for the analysis. Two different approaches to mapping up of the impact vectors, namely the approach according to (Mosleh et al., 1988) and one used by ABB Atom in the F3 PSA (ABB Atom AB, 1985)

have been applied. The ABB Atom's approach relies exclusively on engineering judgement as opposed to that of (Mosleh et al., 1988) which is based on a more formal mathematical frame.

From practical point of view the main difference in situations encountered concerns extension from size "2" system to a system of size "4". More specifically the elements of the impact vector, corresponding to double and triple failures, are reversed in these two approaches. For both mapping up schemes one of three values (0,0.5 or 1) has been assigned to the conditional probability of each component failure given a shock.

For mapping down, which in our analysis is applicable only in one case (B1 plant), the approach of reference (Mosleh et al., 1988) is more prescriptive and deterministic, while ABB Atom used engineering judgement.

Table 4.12 shows the estimated CCF-parameters of MGL-method compared with those originally used in each PSA. Maximum-likelihood method (MLM) has been used in this context. The discrepancies between the higher-order parameters estimated using the two approaches to adjustments for system size differences are significant. The approach based on F3 PSA (ABB Atom AB, 1985) results in expected relation between the higher-order parameters (delta > gamma), which is not the case for the other approach. Naturally, this might be due to statistical limitations of the database used in the present report. The estimated plant-specific beta-factors for MOVs at O3 and R1 plants are significantly higher than the parameter values used in these PSAs.

The PSAs considered have been requantified using the generated plant-specific CCF-parameters for MOVs, the MGL-method (for plants where models which do not distinguish between different failure multiplicities were used, the original CCF-estimate was substituted by the highest applicable MGL-estimate) and two different approaches to adjustments for system size. Table 4.13 illustrates changes in the results of PSAs considered.

Table 4.12

Estimated CCF-parameters for MOVs

Plant	CCF-parameters								
	Beta			Gamma			Delta		
	PSA	Used in present work		PSA	Used in present work		PSA	Used in present work	
		Alt.1[a]	Alt.2[b]		Alt.1[a]	Alt.2[b]		Alt.1[a]	Alt.2[b]
F3	0.07	0.084	0.096	0.4	0.37	0.72	0.6	0.57	0.27
O3	0.022	0.084	0.096	0.3	0.37	0.72	0.9	0.57	0.27
R1	-[c]	0.135	0.146	-[c]	0.63	0.83	-[c]	0.85	0.61
B1	0.05-0.10[d]	0.097	0.078	-[e]	-[e]	-[e]	-[e]	-[e]	-[e]

[a]Mapping up according to F3 PSA (ABB Atom AB, 1985), mapping down based on engineering judgement.

[b]Mapping up and mapping down according to reference (Mosleh et al., 1988).

[c]C-factor of 0.042 used in the R1 PSA; reduction by a factor of 2 in systems of size three or four.

[d]The beta-factors of the B1 PSA are based on engineering judgement and are not component type-specific, but rather situation-specific. In most cases a value of 0.10 has been used.

[e]All the affected systems are of size two.

Table 4.13

Changes (relatively PSA results) in estimated core damage frequency due to use of plant-specific CCF-parameter for MOVs, MGL-method and different extension schemes

PSA	Relative changes (%)	
	Alt. 1[a]	Alt. 2[b]
B1	negligible	negligible
R1	+36	+36
F3	+ 3	+24
O3	+56	+78

[a]Mapping up according to F3 PSA(ABB Atom AB, 1985); mapping down based on engineering judgement.

[b]Mapping up and mapping down according to reference(Mosleh et al., 1988).

As may be seen the impact of using different extension schemes is significant in the case of F3 and O3 PSAs. Use of higher plant-specific CCF-parameters generated in the present work leads to substantial increases of the estimated core damage frequencies for Ringhals 1 and Oskarshamn 3. These PSAs originally used in a somewhat arbitrary way CCF-parameters originating from the US-experience.

4.3.2.3 Comparison of MGL-method and alpha-factor method (Jacobsson, 1988a)

Deviations between the MGL- and alpha-factor methods (Fleming and Kalinowski, 1983 and Mosleh and Siu, 1987, respectively) have been indicated in subchapter 4.2. The difference between the parameters of the alpha-factor model and the MGL-model is that the former are event based (as opposed to component failure based) and are easier to estimate in a statistically proper way. In the present work (Jacobsson, 1988a) quantification of CCF-contributions for a set of four redundant MOVs has been made, using the basic data provided in the Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987) and the two methods. Based on a beta distribution a Monte-Carlo simulation has been used to obtain the contributions corresponding to different failure multiplicities, in form of mean and median values and associated uncertainty intervals (Table 4.14).

Table 4.14

Contributions corresponding to different failure multiplicities for a set of redundant MOVs[a]

P_i[b]	Uncertainty Distribution Parameter							
	Mean		Median		5-percentile		95-percentile	
	MGL	Alpha	MGL	Alpha	MGL	Alpha	MGL	Alpha
P_1	$4.3 \cdot 10^{-2}$	$3.8 \cdot 10^{-2}$	$3.0 \cdot 10^{-2}$	$3.0 \cdot 10^{-2}$	$2.1 \cdot 10^{-3}$	$1.9 \cdot 10^{-3}$	$1.2 \cdot 10^{-1}$	$1.1 \cdot 10^{-1}$
P_2	$9.0 \cdot 10^{-4}$	$1.2 \cdot 10^{-3}$	$5.7 \cdot 10^{-4}$	$7.0 \cdot 10^{-4}$	$3.5 \cdot 10^{-5}$	$4.1 \cdot 10^{-5}$	$3.0 \cdot 10^{-3}$	$3.8 \cdot 10^{-3}$
P_3	$3.0 \cdot 10^{-4}$	$8.7 \cdot 10^{-4}$	$1.4 \cdot 10^{-4}$	$4.1 \cdot 10^{-4}$	$7.1 \cdot 10^{-6}$	$1.5 \cdot 10^{-5}$	$1.1 \cdot 10^{-3}$	$3.0 \cdot 10^{-3}$
P_4	$9.7 \cdot 10^{-4}$	$3.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-4}$	$2.0 \cdot 10^{-3}$	$2.7 \cdot 10^{-5}$	$5.9 \cdot 10^{-5}$	$3.7 \cdot 10^{-3}$	$1.1 \cdot 10^{-2}$

[a]The MOVs chosen for comparison operate in a special mode which explains relatively high failure probabilities.

[b]P_i is the probability of observing excatly i (i = 1, 2, 3, 4) failures per demand.

Apparently, the alpha-factor method results in larger values of CCF-contributions and in a larger uncertainty interval. Underestimation of uncertainties is avoided when using the alpha-factor method which provides a more correct representation of statistical uncertainties.

In view of the results given above use of alpha-factor method in the context of Swedish PSAs has been recommended (Jacobsson, 1988a). However, if point estimates based on maximum likelihood method (MLM) are used to quantify the parameters of the two models the resulting CCF-contributions will be identical. Relations between the parameters of the two models are also provided in (Jacobsson, 1988a). This is of practical importance in case the present MGL-model used in several Swedish PSAs is to be substituted by the alpha-factor model.

4.3.2.4 Data variation for pumps and diesel generators (Jacobsson, 1988d)

Since relevant plant-specific CCF-data for these components are not available for all analysed plants, the choice of representative parameter sets for the purpose of sensitivity studies is based on engineering judgement. In this context plant-specific features considered as important for reduction of CCF-potential (e.g. degree of separation) are taken into account. In the case of diesel generators the impact of the new values on the core damage level is small, except for the O3 PSA which originally used extremely low beta-factors. Generally, the contributions from loss of offsite power sequences to the total core damage frequency are low according to available PSAs for Swedish BWRs. On the other hand, relative changes obtained within sensitivity analysis are in some cases substantial (very large for O3 PSA) on the sequence level.

A similar study concerning pumps shows that the impact of parameter variation on the core melt frequency of some plants is significant.

4.3.2.5 Systematic misconfiguration of redundant components (Björe, 1988d)

With few exceptions dependent aspects of this type of interaction have been disregarded in the Swedish PSAs or are considered to be covered by modeled residual CCF-contributions (which do not include manual valves). Earlier

sensitivity analysis for Forsmark 3 shows (Hirschberg and Knochenhauer, 1986) that only marginal contributions are expected from a postulated case with systematic misconfiguration of MOVs. This is due to the consequently applied physical separation and due to the chosen approach to maintenance and testing. The impact of this type of dependency might be different for other plants.

The approach to this problem within the present sensitivity studies comprises identification of groups of redundant components for which a postulated CCF of the type in question could significantly contribute to dominant core melt frequency. The Multiple-sequential Failure (MSF) model (Samanta et al., 1985) is then applied to quantification of CCF-contributions to be used in sensitivity studies. The MSF-model which requires as input the probability of first component failing and dependency factor, has been developed for estimation of multiple human failure probabilities. Application of this method to the Swedish plants confirms that the impact of postulated CCFs on core damage frequency is small in case of latest generation of Swedish BWRs. For older plants the impact is more pronounced and becomes quite substantial for dependency factors of the order of 0.1.

4.3.2.6 Test arrangements (Björe and Hirschberg, 1989)

The practical arrangement of tests of redundant components and policy applied with respect to identification of CCF-events by testing has impact on the choice of suitable CCF-model (Parry, 1984). C-factor (Parry, 1984) and beta-factor (Fleming, 1975) methods, respectively, correspond to two extremely different testing policies). Use of MGL- and alpha-factor methods is consistent with the origin of Swedish CCF-data, i.e. the presently available Swedish CCF-experience originates almost exclusively from plants where redundant components are tested simultaneously.

4.3.2.7 CCF-contributions in systems with non-standard level of redundancy

The presently available methods and data are (and will probably remain) inadequate for proper modeling of this issue. Cases of interest comprise (Hirschberg, 1987a) e.g. pressure relief valves (most important), control rods and fine motion drives, scram modules and frequency converters. As a first

step in the treatment of these problems a survey has been made with the purpose to clarify the approaches (i.e. assumptions, data, quantification methods) used in the Swedish PSAs. Incorrect extrapolations of simple parametric methods have been observed in several cases. Application of an extended Common Load (CL) model (Mankamo, 1988) has been recently proposed as a solution of this problem.

The model is defined in terms of subgroup probabilities, which means that simple, exact and consistent expressions for different success criteria can be derived. The underlying physical stress-strength model provides understandable interpretations for the model parameters. Future plans (Mankamo, 1989) involve detailed data analyses and performance of sensitivity studies based on applications of extended alpha-factor and CL-methods. It must be emphasized that the initial handling of data may in practice have a much stronger impact on the end result than the choice of quantification model.

4.3.3 Human interactions

Table 4.15 shows the contributions of human failures to the core damage frequency for different plants. In parallel to the consequences of CCFs also human errors lead to core damage only in combination with other failures (CCFs, independent). The numbers in the table should be interpreted as risk reduction which would be achieved if the modeled human errors had negligible probability.

Table 4.15
Impact of human errors on core damage frequency

PSA	Contribution (%)
O1	Relatively small
B1	46
R1	14
F3	88
O3	High
R2	60

High contributions obtained for F3 and O3 plants are due to manual depressurization which is a critical operator action necessary in scenarios involving a transient followed by loss of ordinary and auxiliary feedwater systems. This operator action is of secondary importance for plants belonging to older generations of Swedish BWRs since depressurization is automatically initiated in corresponding situations.

The qualitative analyses (Bengtz and Hirschberg, 1987) have shown that the differences between the approaches used in different studies are large. In case of simple time-reliability curves which frequently have been employed the discrepancies are sometimes on the level of orders of magnitude, although this is hardly motivated by the performance shaping factors for specific situations. In this context it should be pointed out that the Swedish BWRs are similar with respect to time windows for crucial operator actions.

The sensitivity studies of human interactions are different in nature from most of the corresponding analyses concerning CCFs. Since in several Swedish PSAs a rather simplified approach to human interaction analysis has been applied, the assignment of data for sensitivity analysis must be made in a more arbitrary manner.

The sensitivity studies performed concentrate on type 3 (errors of omission) and type 5 (recoveries) interactions (categorization of human interactions according to reference (Hannaman and Spurgin, 1984), which are of primary interest according to the recommendations of qualitative analysis (Bengtz and Hirschberg, 1987).

The sensitivity studies have led to recommendations concerning treatment of the investigated human interactions within the reference PSAs generated within the current SUPER-ASAR project (Carlsson et al., 1988). The recommendations serve in the first place as a basis for consequent treatment of operator actions in this context and are only relevant for such a purpose. The present work does not contain a detailed analysis of human interactions. Carrying out plant-specific studies, based on agreed common assumptions, is recommended.

4.3.3.1 Manual reactor shutdown (Björe, 1988a)

The dominant accident scenario with need of manual reactor shutdown involves according to all Swedish PSAs an arbitrary initiating event (transient or LOCA) and a CCF in reactor protection system (RPS). The assigned failure probabilities for manual reactor shutdown are in the interval 0.003-1.0. In one of the PSAs (F3) rather strong differentiation has been made with respect to the initiating event.

The available time for operator actions is for all analysed plants of the order of 5 minutes in case of loss of feedwater or small LOCA, roughly 10 minutes for loss of offsite power or loss of turbine condenser and extremely short for medium or large LOCA.

On the basis of the available analyses low (0.003 per demand), medium (0.1 and 0.5) and high (1.0; no credit for operator action) failure probabilities have been selected for the purpose of sensitivity analysis of manual reactor shutdown. Figure 4.8 shows the results obtained for the total core damage frequency. For comparison the values used in each PSA, respectively, are indicated.

Apparently core damage frequency for two of the plants is sensitive to the assigned probability of this operator action. Note that the impact of the considered accident sequence on the total core damage frequency is also dependent on the total frequency of initiating events involved (ranging between 0.99 and 4.83 per year for the plants analysed) and the probability of CCF in RPS (ranging between $5.0 \cdot 10^{-8}$ and $1.0 \cdot 10^{-5}$ per demand). The differences between plants with respect to control room design and display of process information have not been judged to be of such importance that they would have a decisive impact on this particular operator action.

It has been concluded (Björe, 1988a) that the diagnosis and not carrying out the manual action will be the most crucial step. Since the available time for decision-making is of central importance, different failure probabilities should be used depending on type of initiating event. Thus, taking credit for manual reactor shutdown in the case of large and medium LOCA is not recommended. Reasonable failure probabilities for this operator action in case of other initiating events considered, are judged to be in the interval 0.01-0.04 per demand.

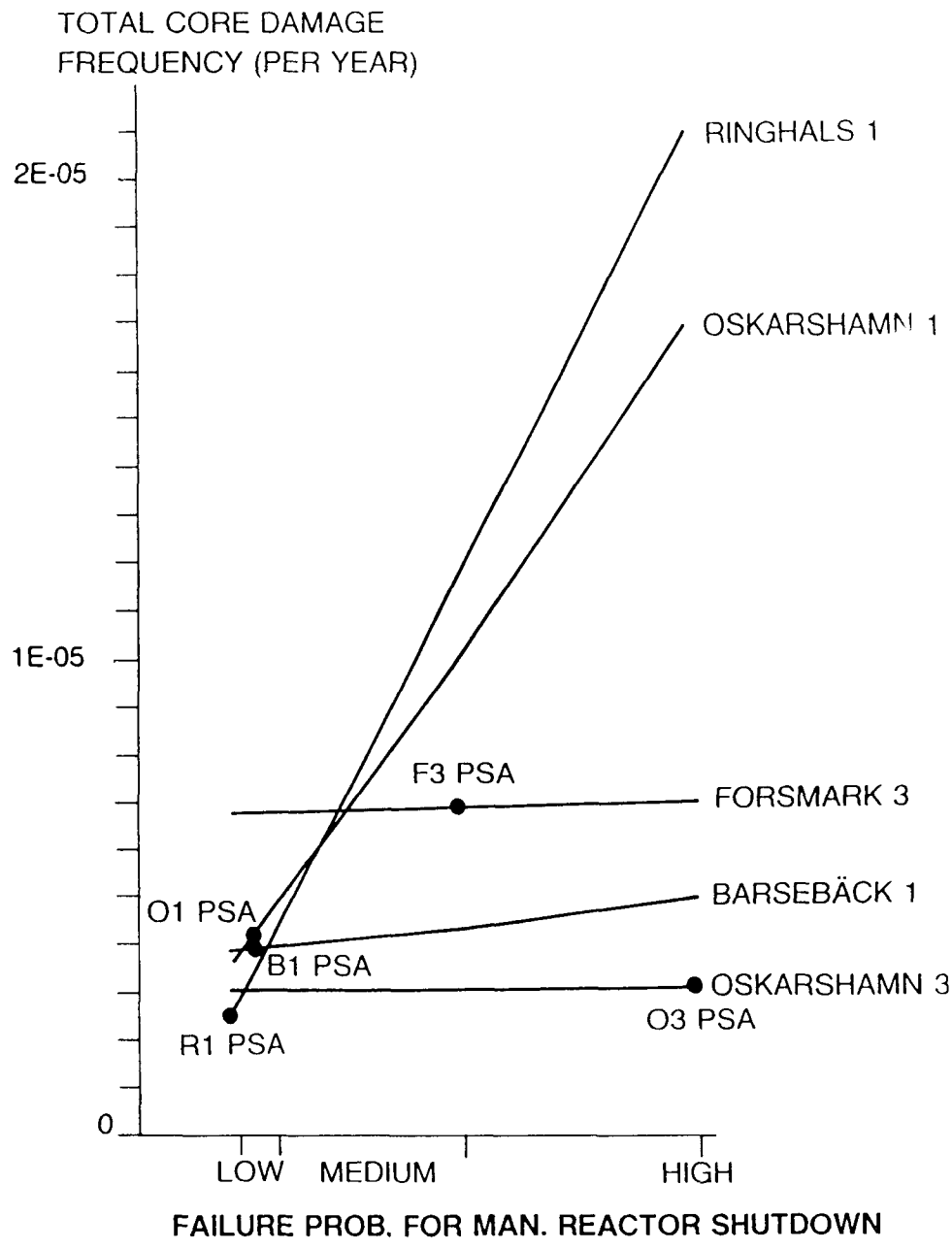


Figure 4.8
Sensitivity analysis of manual reactor shutdown

4.3.3.2 Manual depressurization (Jacobsson, 1988b)

Following any transient initiating event and given that the ordinary and auxiliary feedwater systems are unavailable depressurization would be necessary before the low pressure emergency core cooling system can be activated. In O1, B1 and R1 plants automatical depressurization would take place in such a situation, while for F3 and O3 plants the action must be initiated manually from the central control room.

The sensitivity study has been carried out for these two plants, based on the results obtained by ABB Atom within the recently completed Nordic reference study on human interactions (Hirschberg, ed., 1989). This study, carried out for the F3-plant, contains a thorough analysis of manual depressurization following a loss of feedwater transient and unavailability of the auxiliary feedwater system. For the purpose of the present sensitivity analysis the median ($3.1 \cdot 10^{-3}$ per demand), the mean ($9.1 \cdot 10^{-3}$) and the 95-percentile ($3.1 \cdot 10^{-2}$) have been used as the low, medium and high values for probability of failure of manual depressurization. Table 4.16 summarizes the results; within parantheses relative contributions of accident sequences involving manual depressurization to the total core damage frequency, are given.

Table 4.16

Sensitivity analysis of manual depressurization

Failure probability (per demand)	Core damage frequency (per year)	
	F3 PSA	O3 PSA
PSA-value ($1.0 \cdot 10^{-2}$)	$7.0 \cdot 10^{-6}$(75%)	$3.2 \cdot 10^{-6}$(29%)
Low ($3.1 \cdot 10^{-3}$)	$3.3 \cdot 10^{-6}$(52%)	$2.6 \cdot 10^{-6}$(11%)
Medium ($9.1 \cdot 10^{-3}$)	$6.6 \cdot 10^{-6}$(73%)	$3.1 \cdot 10^{-6}$(27%)
High ($3.1 \cdot 10^{-2}$)	$1.9 \cdot 10^{-5}$(90%)	$5.1 \cdot 10^{-6}$(55%)

The results shown reconfirm the crucial importance of manual depressurization for F3 and O3 plants. Introduction of automatical depressurization in order to eliminate this relatively difficult operator action should be seriously considered. The observed discrepancies between the impacts on the results of the two PSAs are mainly due to different operation modes of the auxiliary feedwater system and different treatment of CCFs. The failure probability (10^{-2} per demand) which was used in the PSAs is consistent with the results obtained within the much more detailed analysis of the Nordic reference study (Hirschberg, ed., 1989).

4.3.3.3 Manual reclosure of pressure relief valve (Jacobsson, 1988b)

According to the present sensitivity study the probability assigned to failure of manual reclosure of pressure relief valve has negligible impact on the total core damage frequency. This statement is valid for all plants. The action is characterized by a relatively high stress-level and a failure probability of $5.0 \cdot 10^{-2}$ per demand, used in R1 PSA and supported by a detailed analysis, is regarded as most representative.

4.3.3.4 Manual back-flush operation (Jacobsson, 1988c)

After a LOCA debris such as piping insulation may drop into the condensation pool and the suction strainers of some cooling systems may be clogged. Thus, manual back-flush operation (BFO) may be necessary for O1, B1 and R1 plants. For F3 and O3 plants the BFO is not necessary due to different containment design and use of different pipe insulation. The analyses of BFO have been carried out within the B1 and R1 PSAs and later supplemented by additional studies (a more detailed one for B1(Moricz, 1988) and an independent for R1 (Lydell et al., 1986)). BFO has not been modelled within the O1 PSA, since the action was not considered as necessary.

Large differences between the PSAs regarding the modeling of BFO exist. The discrepancies include different modeling of the need of BFO, different modeling of the associated manual actions, different core damage definitions and different frequencies for the concerned initiating events (large and medium LOCA). The most significant parts that contribute to the discrepancies in results are:

- Different assumptions made regarding the probability for the need of BFO (in O1 PSA no need at all of BFO, in R1 PSA a certain probability of the need of BFO after both medium and large LOCA, in B1 PSA always need of BFO after large LOCA).

- Different assumptions made regarding the point of time for initiation of BFO (varies between 30 minutes and 10 hours), which has influence on stress conditions.

- Different assumptions made regarding the time window (varies between 6.5 minutes and 30 minutes).

Figure 4.9 shows the results of sensitivity analysis based on use of different values of BFO failure probability. The values correspond to those used in O1 PSA (0 per demand), R1 PSA ($3.0 \cdot 10^{-4}$), B1 PSA ($1.0 \cdot 10^{-2}$) and those estimated in supplementary studies for B1 ($5.1 \cdot 10^{-3}$) and for R1 ($3.2 \cdot 10^{-1}$). In this sensitivity study BFO has been considered for medium and large LOCA for R1 and only for large LOCA for the other plants. New, recently generated plant-specific values for the frequency of LOCA (Sandstedt, 1988) have been used. Otherwise the models originally used within the PSAs have not been modified or extended when carrying out the sensitivity analysis.

For all PSAs considered the same tendency with respect to core damage dependency on assigned failure probability for BFO has been observed. Thus, the total core damage frequency increases by a factor of 16, 22 and 109 for B1, O1 and R1, respectively, if extreme failure probabilities for BFO are used.

The present analysis does not contain a plant-specific analysis of BFO. The level of detail is not sufficient to assure that the plant-specific aspects do not have a decisive impact on the BFO failure probability. However, no such critical differences have been identified. Based on the available PSAs, on supplementary studies and on the outcome of sensitivity studies, $1.0 \cdot 10^{-2}$ per demand and affected system is regarded as a representative value (for the purpose of generating reference PSAs) for the failure probability of BFO.

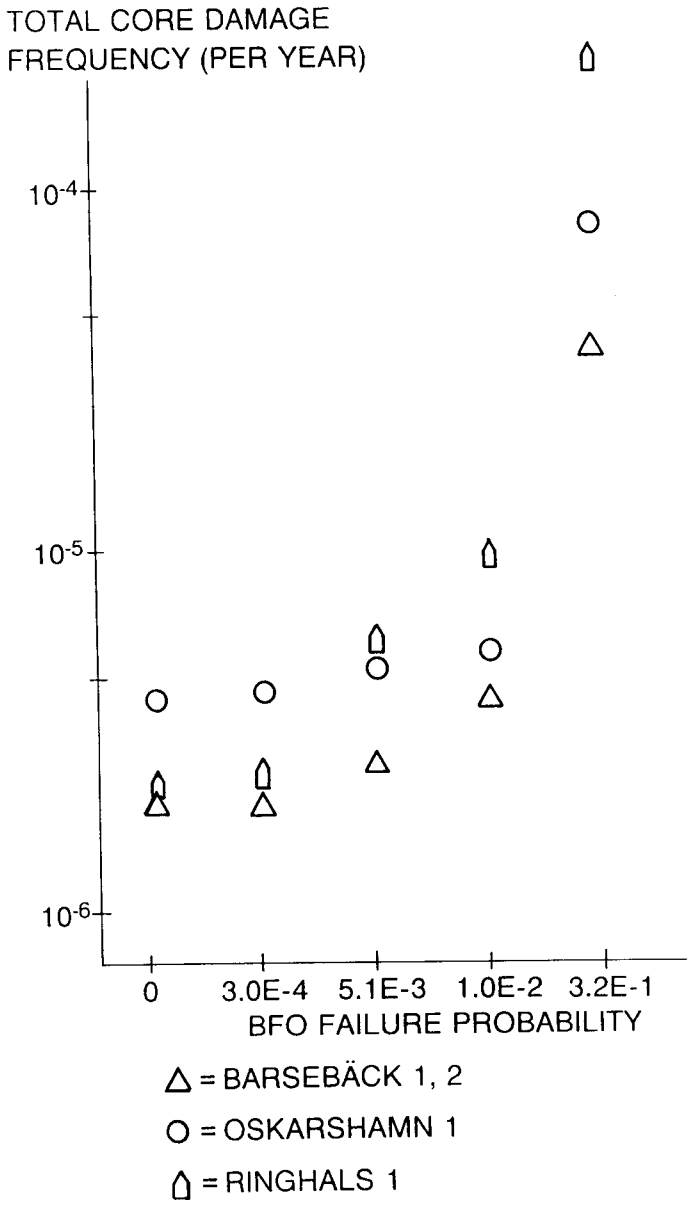


Figure 4.9
Sensitivity analysis of back-flush operation

4.3.3.5 Manual initiation of reactor shutdown cooling system (RSCS); (Björe,1988b)

This study has been limited to O3, F3 and R1 PSAs. Cut-sets including manual initiation of RSCS are not to be found in B1 PSA; loss of residual heat removal (RHR) function does not lead to core damage according to O1 PSA. The assumptions of different PSAs, concerning prerequisites for core damage are a subject of a separate study being in progress. The minimum available time for manual initiation of RSCS is for Swedish BWRs approximately four hours.

Figure 4.10 illustrates the results of sensitivity study. It is anticipated that due to design similarities B1 would follow approximately the same trend for core damage frequency versus failure probability for initiation of RSCS as R1. Low (10^{-3} per demand), medium (10^{-2}), high (0.1 and 0.5) and very high (1.0) values, have been used in this context.

Apparently the results of R1, F3 and O3 PSAs are sensitive to the assigned probabilities. Dominant contributors in the analyses performed are decision to connect RSCS in loss of offsite power sequences for R1 and decision to restart high pressure pump in loss of feedwater sequences for F3 and O3.

The decision failure probability of 10^{-2} per demand, which also has been used in several PSAs, is judged as reasonable.

4.3.3.6 Manual Restart of Feedwater System (Björe, 1988c)

Relatively few recoveries which directly involve manual operations have been modeled and credited for in the Swedish PSAs. Among identified recoveries manual restart of feedwater system may have significant impact on the results of the studies. The initiating events of interest are the loss of feedwater and loss of offsite power transients. Two main categories of accident sequences which are affected by a possible recovery may occur following these transients:

- sequences involving loss of makeup water to the reactor core; the available time for restart of feedwater system is approximately 30 minutes,
- sequences involving loss of the residual heat removal function; the available time is at least 4 hours in these cases.

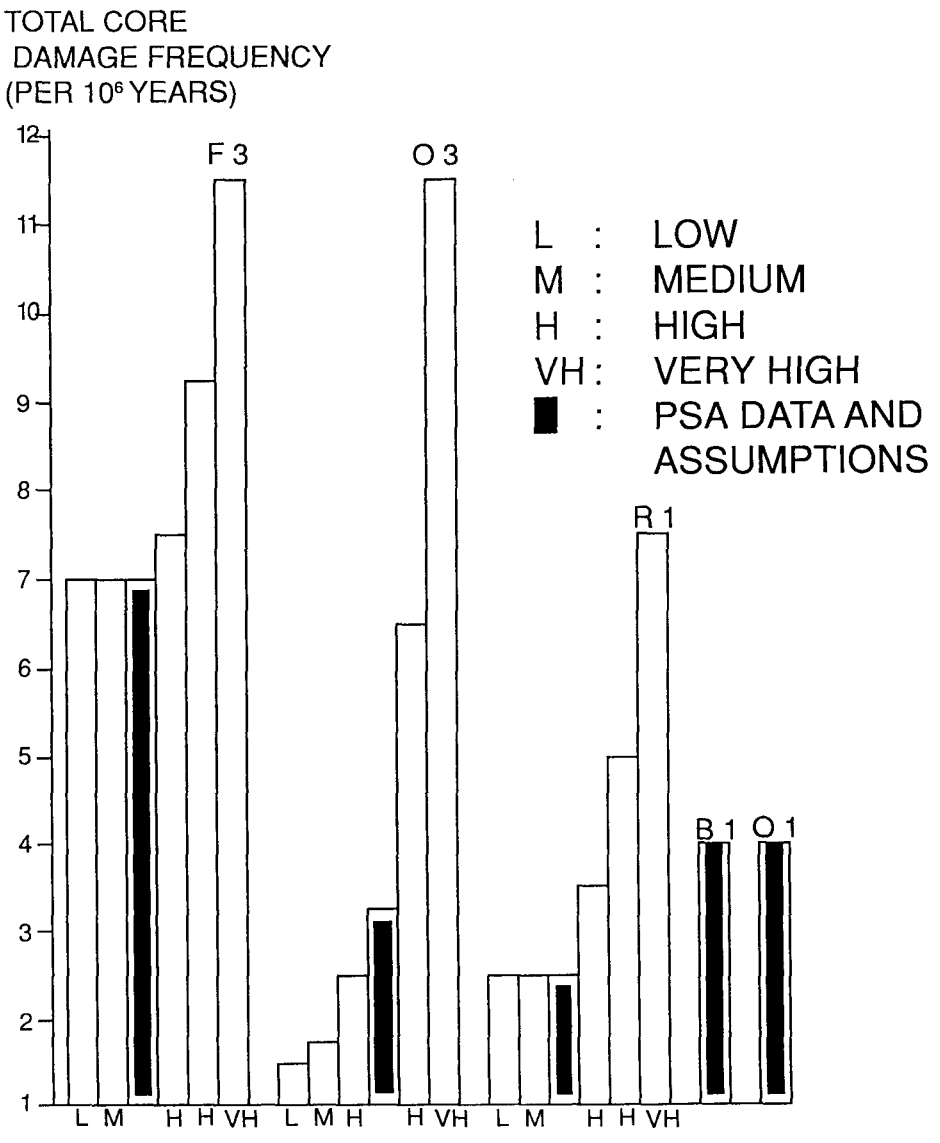


Figure 4.10

Sensitivity analysis of manual initiation of reactor shutdown cooling system

The two relevant initiating events and two categories of accident sequences have been considered in the sensitivity study. In this context two sets of failure probabilities for restart of feedwater system have been used. No recalculations have been carried out for O1 since no credit for recovery has been taken in the PSA and due to the nature of dominant accident sequences the impact of more optimistic modeling is expected to be insignificant. The results are shown in Figure 4.11. As can be seen also results for R1 PSA are quite insensitive to the assigned probabilities for failure to restart feedwater system.

The study of typical fixed and variable restoration times shows that within 30 minutes no credit can be taken for the restart if the initiating event is loss of feedwater and only weak credit is motivated in case of loss of offsite power. For residual heat removal sequences (available time at least 4 hours) corresponding failure probabilities have been judged to be of the order of 0.5 and 0.05, respectively.

4.3.3.7 Repair of containment cooling spray system (CCSS); (Tuvesson, 1988)

The repair has been credited only in O3 PSA, which results in a reduction of the estimated core damage frequency by a factor of ten. Significant reductions, although not so large, would also result for B1, R1 and F3 plants if corresponding credit had been taken.

The dominant failure modes in affected sequences concern pumps and valves. A study of repair times has been made, based on failure reports involving these components at all Swedish plants. A corresponding analysis has been made for CCSS. The studies indicate that if total repair time including disclosure and tracing of failure in the central control room, time for assemblying the repair force, preparation for repair, actual repair and system restart, is considered, any crediting of CCSS repair is questionable for most of the accident sequences of interest. For large LOCA taking any credit is not possible at all since the CCSS is needed in short time perspective for water level measurement (cooling of reference water column).

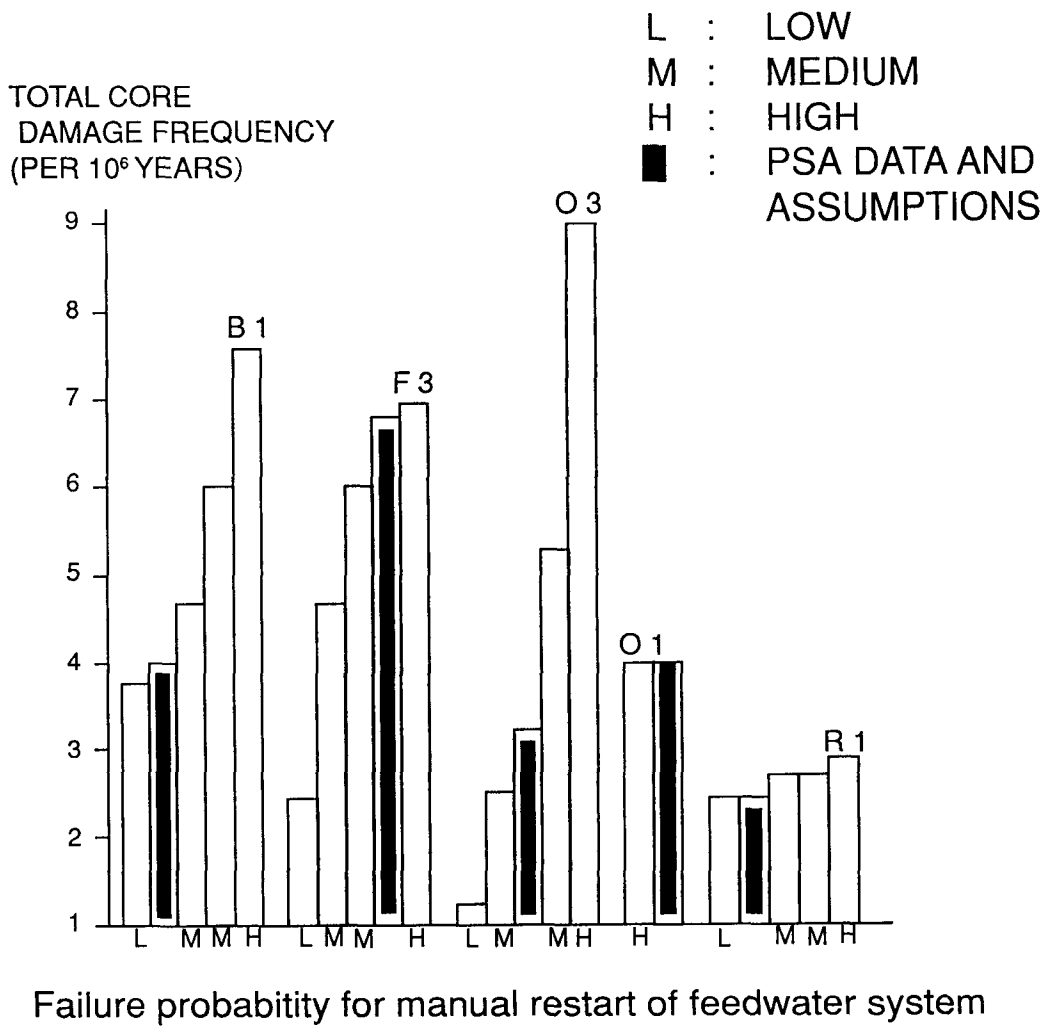


Figure 4.11

Sensitivity analysis of manual restart of feedwater system

4.3.4 Conclusions and future work

Based on recommendations from qualitative retrospective analysis comprehensive sensitivity studies have been performed concerning treatment of CCFs and human interactions in Swedish PSAs. Sensitivity analysis proved to be an efficient tool for demonstrating the impact of use of different assumptions, methods and data on the results of the studies. In this way guidance is provided with respect to these aspects of current analyses, which call for future efforts in form of supplementary studies and/or research projects.

The sensitivity studies have varying degree of detail. While in the case of e.g. CCF-contributions for MOVs an extensive analysis has been made in order to generate plant-specific data, most of the studies concerning human interactions are somewhat more arbitrary. The choice of probabilities to be used in different sensitivity studies was, however, in all cases made with due regard to the analyses supplied within the PSAs or other supplementary investigations.

Specific methodological findings of the present work concern impact of lower failure multiplicities in the context of CCF-contributions, sensitivity to assumptions concerning extension schemes and comparative evaluation of the MGL-and alpha-factor methods. Future work within the CCF-analysis will concentrate on proper consideration of defensive measures against CCFs, generation of plant-specific CCF-data for important groups of components using Swedish operating experience, and on more consistent treatment of CCF-contributions in systems with non-standard level of redundancy. Projects aiming at realization of these goals have recently been started (Mankamo, 1989 and Hirschberg, 1989).

In case of human interactions the base case analyses as reported within the Swedish PSAs are in most applications not sufficiently detailed and extensions are motivated. The sensitivity studies confirm the importance of e.g. manual depressurization for F3 and O3 plants and of manual back-flush operation for O1, B1 and R1 plants.

Finally, some recommendations have been given concerning the treatment (i.e. models and data) of CCFs and human interactions within the plant-

specific reference PSAs which will be generated in the near future (Carlsson et al., 1988). These reference plant models will be based on consequent application to all plants of similar assumptions concerning treatment of these and other PSA-elements (e.g. accident sequence modeling and quantification, systems modeling, reliability data, etc.). In this way plant-specific issues will be emphasized but at the same time the available PSAs will become more comparable. This will facilitate active use of the PSAs in the decision making process. It should be remembered that within sensitivity studies one aspect at time has been studied. Integration of all recommendations including those concerning other PSA-elements will inevitably lead to a different overall picture, which may influence future priorities.

4.4 Limitations of PSA

The limitations of PSA techniques contribute to the overall uncertainty of the results. It is of great importance to point out the main limitations and hereby facilitate decision-making and prevent possible misuse of PSAs.

Based on references (Lewis, 1984) and (Pulkkinen, 1986) and on general experiences from the PSA-related work (Hirschberg, 1987b) examples of intrinsic and practical limitations are given below. In some cases it is hard to make a distinction between these two groups, i.e. there might exist potential for improved treatment of an intrinsic limitation.

4.4.1 Intrinsic limitations

1) Incompleteness. Incompleteness of PSA originates from technical complexity of large systems, from difficulties to identify, model and quantify all potentially significant internal interactions between systems, components, human beings and corresponding external interactions with environment, and from possible misses in the management and review of PSA. Obviously, there are no guarantees that all significant accident sequences can be identified, but credibility of the studies is expected to increase with time. It should be kept in mind that each identified sequence represents a whole group of kindred scenarios. Integration of new operating experience (i.e. calibration based on the real world) within the concept of "living PSA" will contribute to reduction of incompleteness uncertainties. Sensitivity analysis may also be employed to some extent in this context (Hirschberg and Knochenhauer, 1986). Finally, a well-structured review process will contribute to assurance of satisfactory completeness.

2) Data base. Data base will always be more or less inadequate. This applies also to relatively frequent failures, at least with respect to detailed knowledge of distributions. Other, more serious failures might never occur and associated failure probabilities are bound to be based on

judgement and on extrapolations from other applications. This point is closely related to the item of uncertainty.

3) Human interactions. Spectrum of possible human errors is very large. The same applies to the ability to act innovatively, to solve problems and to correct mistakes. Although the overall goal is to take into consideration both abilities and limitations of human beings when designing systems, formulating procedures, establishing work organisation and carrying out training activities, the possibility of mistakes cannot be excluded. However, human reliability is a quite different concept than a component's reliability. It is natural to talk about average components while "average human being" hardly exists. Consequently, there are no PSA-models which can provide fully satisfactory representation of human behaviour.

4) Common cause failures. Generally, complexity of the design, involvement of human beings and influence of environmental factors create a potential for dependencies between and within the systems, which may increase the potential for multiple failures. While most types of dependencies can be explicitly modeled (which constitutes one of the main advantages of PSA-methodology), common cause failures (CCFs) represent a subset of dependencies which due to scarceness of data and/or lack of knowledge are not represented in detail in the analytical models (event trees and fault trees). A variety of different causes may be hidden behind each CCF-contribution. It is not practically possible to distinguish between these causes and all possible sources are usually collected together to form one contribution for each analysed set of redundant components. In practice, for systems with three or four redundant trains there may be several contributions for each set of components, corresponding to different failure multiplicities. Similarly to human interactions there is an infinite spectrum of possible scenarios resulting from hypothetical root causes and coupling mechanisms, which might result in a common cause failure. It is, however, not possible to treat (i.e. model and quantify) unknown failures, which is closely related to the problem of completeness.

5) Uncertainty. Uncertainty is an inseparable characteristics of probability. As often forgotten corresponding hidden uncertainties are present also in deterministic analyses. In a PSA they are brought to light. The possibility to express and model uncertainties is one of the basic ideas behind PSA.

4.4.2 Practical limitations

1) Consistency. Experience shows both similarities and differences between the PSAs performed. Efforts have recently been made in Sweden (Carlsson et al., 1987 and Carlsson et al., 1988) to separate on the one hand those discrepancies which reflect differences in design and operation and on the other hand those which are due to differences in modeling approaches. According to the findings (Carlsson et al., 1988) better consistency can be achieved.

2) Conservatism. The objective of a PSA is to provide a plant-specific realistic model of accident propagation. This means that conservatism should be avoided. In reality the uncertainties are frequently handled by

means of conservative margins whose magnitude is not known. In addition, proper credit is not always taken for normally operating systems which have ability to prevent or mitigate the accident. The final quantitative result might then be of no value and the relative importance of different sequences might be distorted.

3) Uncertainty. Numerous examples can be given of careless treatment of uncertainties. No clear distinctions are usually made between the parametric, modeling and incompleteness uncertainties and their relative importance. The analysts are not always aware of which type of framework (frequentist or subjectivist, i.e. Bayesian) they actually apply which may lead to inconsequences.

4) Human interactions. Apart from intrinsic limitations, modelling of human interactions is subject to shortcomings which can be improved. This applies in particular to qualitative modeling of operator tasks in the control room, where depending on the particular situation encountered different types of behaviour (skill-, rule- and knowledge-based) may be expected (Rasmussen, 1983). Understanding of cognitive aspects of operator behaviour is limited within the PSA-community and bridging of the gap between technicians and psychologists is desirable. Treatment of recoveries in the PSAs is frequently pessimistic or lacking. The available data for human interactions apply only to well structured tasks. The modeling of human behaviour has not yet reached the level where any accurate predictions of error probabilities can be made (Wahlström, 1986). Structured procedures are, however, available for use of expert judgement in a systematic way.

5) Dependencies. Treatment of dependencies is not always well structured and consequent. Some CCF-models are based on questionable assumptions or are being applied without proper regard to their limitations. The coverage of CCF-analyses can often be questioned. Potential CCFs in auxiliary systems (e.g. electric power supply) are frequently neglected. This may also apply to the completeness of explicit modeling of dependencies in such systems. Generally, available methods for quantification of CCF-contributions are not compatible with status of data sources. Recent developments (e.g. Mosleh et al., 1988) provide, however, a framework for performing different stages of CCF-analysis.

6) External events. Lack of relevant data and complexity of the problem creates large uncertainties. Among those external events which most frequently appear as dominant risk contributors, treatment of seismic hazards appears to be most difficult. Progress in this area is expected due to increasing knowledge about seismicity, fracture mechanics and seismic response.

7) Time dependencies. The basic logical models of PSAs (event trees, fault trees) can only to a limited extent simulate the numerous types of time dependencies which are involved (Simola et al., 1988) and which may be important. Supplementary analyses of these aspects are seldom made within the PSAs.

8) Documentation. There is a substantial potential for improvements. Many PSAs are badly structured and/or written by and for PSA-specialists. This limits significantly the use of PSAs and creates difficulties in PSA-based decision-making.

4.4.3 Validity of absolute estimates

As stated above the main merit of PSA is that a frame is provided for a systematic identification of chains of events which may lead to accidents and for realistic assessment of the associated frequencies. This is equivalent to identification of dominant risk contributors. There are many examples of design and procedural deficiencies which have been disclosed as a result of PSA-work. Based on PSA-results modifications are often made at the plants in order to achieve a more balanced risk profile. Such use of PSA-techniques has indisputable advantages and the validity of analysis results is frequently moderately sensitive to the uncertainties due to intrinsic and practical limitations. In this context the use of PSA-results for decision-making is based on relative criteria, which as opposed to absolute criteria are not totally dependent on the exactness of predictions and, consequently are more forgiving (Hirschberg and Knochenhauer, 1988).

Reliance on the bottom-line results of PSAs and, consequently, use of formal safety goals in the regulatory process is a subject to considerable controversy ("One should resist one-digit statements about safety." (Lewis, 1984)). In some countries introduction of safety goals has been considered as a possible solution to the regulatory dilemma. A good review of safety goals for nuclear power plant regulation may be found in reference (Levine and Stetson, 1986). Current research projects carried out in Nordic countries (Carlsson et al., 1987; Carlsson et al., 1988; Hirschberg and Knochenhauer, 1988) clearly demonstrate the spectrum of problems encountered when comparing different PSAs and consequently difficulties associated with use of absolute probabilistic criteria. Thus, direct use of plant-specific numerical results in the absolute sense should be made with great caution, having in mind a wide spectrum of intrinsic and practical limitations as well as the involvement of subjective judgement in almost all tasks of a PSA. A new major comparative study (U.S. Nuclear Regulatory Commission, 1989) has made the importance of expert opinions in the PSA-context very visible.

Intuitive use of PSA-based goals is frequently employed on a system/subsystem level e.g. for evaluation of design tradeoffs. This is rather straightforward and certainly beneficial with respect to public safety as well as plant reliability. Introduction of formal criteria for licensing is, however,

hardly motivated in view of the problems outlined and in view of inadequate precision of presently available safety goals. Implementation of such goals would require detailed specification of analysis procedures (a formidable and practically impossible task whose realization would not encourage future developments and hardly promote safety improvements). A compromise solution is suggested in (Murley, 1985): "The safety goals should not be used within a regulatory framework of strict acceptance or non-acceptance criteria but should be considered as one factor in arriving at regulatory judgement."

4.5 Decision-making in View of Uncertainties

4.5.1 Treatment of uncertainties

In each decision making situation one has to choose among a set of alternatives, $\{d_i\}$, the consequnces of which have to be evaulated and mutually compared (Pulkkinen and Pörn, 1989). The list of alternative actions has to be as exhaustive as possible and exclusive, i.e. only one alternative is to be chosen. To choose among alternative actions is, however, a decision under uncertainty. This uncertainty originates from the uncertain (random) events $\{E_j\}$, which are dependent on the decision taken and are unknown at the moment of decision. In the example of manual contra automatic depressurization considered in subchapter 4.2 such events may consist of human errors by the operator or failure occurences which make the automatic system unavailable. There are, of course, many other events which are common to both alternatives.

As will be seen in the next section, to evaluate the various decision alternatives it is necessary to estimate the likehood or probability of the uncertain events, $P(E_j|d_i)$, conditioned by each alternative decision d_i. The estimation of these probabilities is the main task of any safety analysis.

The uncertainty considered in this section is related to the determination of the probabilities $\{P(E_j|d_i)\}$. The modeling of both the system structure and the unavailability of its components is uncertain because of limitations of the analysis and lack of knowledge about the complex relationships. Further, the probability models usually are based on parameters, $P(E_j|\Theta,d_i)$ where the parameters Θ are uncertain because of sparse input data.

Hitherto, mainly the parametric uncertainty has been treated by describing the uncertainties with probability distributions. However, some recent papers on Bayesian method in uncertainty analysis (Clarotti, 1989 and Pulkkinen, 1989) indicate the possibility to describe even the modeling uncertainty in probabilistic terms. This will hopefully become possible in practice by the future development of the uncertainty analysis techniques. At present the modeling uncertainty is mostly assessed by conventional sensitivity analysis.

How can we treat the uncertainties discussed above in the decision making process? Fortunately we can use a basic probability law, which in terms of notations we have already presented, reads

$$p(E_j|d_i) = \int p(E_j|\Theta,d_i)p(\Theta|d_i)d\Theta,$$

where we have included the model parameter Θ and the (parametric) uncertainty distribution $p(\Theta|d_i)$. The probability on the left hand side of the expression given above is a single number and has no uncertainty bounds around it. The probability itself expresses the total uncertainty concerning the occurence of the event E_j, i.e. it incorporates the uncertainty in the values of the model parameters Θ too. Typical examples of Θ are failure rates - time or demand related - on component level, CCF-parameters on system level and core damage frequency on plant level. The determination of the joint distribution $p(\Theta|d_i)$ is the main objective of the uncertainty analysis. The difficulty in obtaining this objective depends, of course, strongly on the level and complexity of the decision variable to be used.

From the probability law above, where the parameter Θ comprises all parameters of the PSA model, some interesting and important conclusions can be drawn:

- The parameter uncertainty distribution $p(\Theta|d_i)$ is used as a whole
- No point estimates of parameters (e.g. component reliability characteristics) are necessary. Furthermore, use of point values might lead to nonconservative results (Clarotti, 1988)
- There is no uncertainty band around $P(E_j|d_i)$, i.e. there is no room for probability of probability and not for uncertainty propagation either (Clarotti, 1989).

Is the last item in conflict with the efforts of this project, where much emphasis has been put on the propagation of parametric uncertainties through the accident sequence model? The uncertainty propagation can, at least in practice, be defended if the uncertainties are propagated from the original level of parameters to some higher level. Then the uncertainty propagation can be considered as a pure transformation of probability distributions. Thus in case of the sequence analysis of this project the core damage frequency might be the high level parameter, up to which the uncertainties are propagated. Further, the exact evaluation of the accident probability according to the equation is very difficult and the Monte Carlo simulation seems to be the only practical approximative method for this purpose. The resulting uncertainty distribution of the core damage frequency can then be used, according to the earlier described basic probability law, to yield the desired probability of core damage during a given time period.

The advantage of such an uncertainty propagation is the possibility to reveal those parameters that have the greatest impact on the final probability. This feature of unertainty propagation has been utilized in this project in terms of uncertainty contributors described in subchapter 4.2.

4.5.2 Decision making under uncertainty

In the previous section we presented the probabilities $P(E_j|d_i)$, where both d_i and E_j runs through an exhaustive and exclusive list of decisions and uncertain events. In addition to these probabilities the decision maker has to evaluate the consequences $C(d_i,E_j)$ of each pair of decision and event. Because the consequences may be of quite different size and type the decision maker needs a yardstick by which the consequences can be measured and compared to each others (Pulkkinen and Pörn, 1989). Such a yardstick is the concept of utility.

Well established decision theoretic models (Lindley, 1988) help us to combine these separate quantities in a logical and coherent way to finally reach a decision which maximizes the expected utility or minimizes the expected risk. Although the implementation of the neat, logical theory may be difficult in some practical cases, it would be worthwhile to aim at in the future development. Such a step should give a desirable structure both to the analysis work and to the decision process.

Summarizing, much light can be thrown on the decision problem by the mere attempt to provide an exhaustive list of events E_j, the outcome of which will affect the consequnces. As such uncertain events we may think of the occurence of mutually exclusive accident sequences which every PSA normally presents. The task to identify a really complete list of events includes the same problem of completeness as we encounter in all PSA work. Much work in the form of conventional PSA as well as more specific safety analysis today are devoted to the determination of the probabilities $\{P(E_j|d_i)\}$. As these are a measure of uncertainty they will also incorporate the uncertainty associated to the analysis itself, namely the parametric and modeling uncertainties. This requires that the latter types of uncertainty are described by probability distributions. Finally the analyst has to present the consequence $C[d_i,E_j]$ for each pair of decision and uncertain event, in the range from no damage at all to the worst possible accident.

Thus the procedure from the analysis point of view is relatively clear as far as such decision influencing factors are concerned that can be quantified. Well aware of the fact that all analyses are incomplete in some respects it is very important that this incompleteness is highlighted by explicitely presenting all the boundary conditions and simplifying assumptions. As far as the analyst has not been able to include the modeling uncertainty into probability measures, this uncertainty must be emphasized by presenting the results of traditional sensitivity analyses.

As important findings of the efforts that have been made on uncertainty analysis within this project we may summarize:

- The Bayesian approach is advantegeous due to its ability to handle small amounts of data, and even non-statistical information.
- Performing full uncertainty analysis is quite necessary for the consequent decision analysis. Point-estimate quantifications are both insufficient and can be missleading.
- The classical decision theory provides a structure and a framework for addressing the issue of decision making uncer uncertainty.

4.6 References

ABB Atom AB (1985)
Forsmark 3 Safety Study (in Swedish), February 1985.

Apostolakis, G.E. (1989)
Uncertainty in Probabilistic Safety Assessment. Nuclear Engineering and Design, 115, pp. 173-179, North-Holland, Amsterdam, 1989.

Apostolakis, G.E., ed. (1988)
Reliability Engineering & System Safety, 23, pp.247-320, 1988.

Apostolakis, G. and Kaplan, S. (1981)
Pitfalls in Risk Calculations. Reliability Engineering, 2, pp. 135-145, 1981.

Bengtz, M. and Hirschberg, S. (1987)
Retrospective Analysis of Human Interactions in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. RAS-470(87)5 (ABB Atom Report RPC 87-54), July 1987.

Bengtz, M. and Hirschberg, S. (1988)
Sensitivity Studies of CCF-contributions for Motor-operated Valves in the Swedish PSAs. Report RAS-470(88)24 (ABB Atom Report RPC 88-91), July 1988.

Bento, J.-P., Björe, S., Ericsson, G., Hasler, A., Lydén, C.-O., Wallin, L., Pörn, K., Åkerlund, O. (1985)
Reliability Data Book for Components in Swedish Nuclear Power Plants. Report RKS 85-25, prepared by ABB Atom AB and Studsvik Energiteknik AB for Nuclear Safety Board of the Swedish Utilities and Swedish Nuclear Power Inspectorate, May 1985.

Björe, S. (1988a)
Sensitivity Study of Manual Reactor Shutdown in the Swedish PSAs. Report RAS-470(88)25 (ABB Atom Report RPC 88-101), July 1988.

Björe, S. (1988b)
Sensitivity Study of Manual Initiation of Reactor Cooling Shutdown System (321) in the Swedish PSAs. Report RAS-470 (88)27 (ABB Atom Report RPC 88-135), October 1988.

Björe, S. (1988c)
Sensitivity Study of Manual Restart of Feedwater System in the Swedish PSAs. Report RAS-470(88)34 (ABB Atom Report RPC 88-136), October 1988.

Björe, S. (1988d)
Sensitivity Studies of Systematic Misconfiguration of Redundant Components in the Swedish PSAs. Report RAS-470 (88) 31 (ABB Atom Report RPC 88-164), December 1988.

Björe, S. and Hirschberg, S. (1989)
Arrangement of Tests of Redundant Components. Report RAS-470 (88)30 (ABB Atom Report RPC 89-25), January 1989.

Carlsson, S., Hirschberg, S. and Johanson, G. (1987)
Qualitative Review of Probabilistic Safety Assessment Characteristics. PSA '87 - International SNS/ENS/ANS Topical Meeting On Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Carlsson, L., Hirschberg, S., Johanson, G., Pörn, K. and Wilson, D. (1988)
Can Different PSAs be Compared and Used in Nationwide Decision Making? Status of and Experience from the Swedish ASAR-program. OECD/CSNI Workshop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Clarotti, C.A. (1988)
Failure Rate Estimation, A Dangerous Nonsense in a Bayesian View. Reliability Engineering and System Safety, 20, pp. 117-126, 1988.

Clarotti, C.A. (1989)
PSA, Subjective Probability and Decision Making. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Fleming, K.N. (1975)
A Reliability Model for Common Mode Failures in Redundant Safety Systems, Proceedings of the Sixth Annual Pittsburgh Conferene on Modeling and Simulation. General Atomics Report GA-A-13284, April 1975.

Fleming, K.N. and Kalinowski, A.M. (1983)
An Extension of the Beta Factor Method to Systems with High Levels of Redundancy. Report PLG-0289, August 1983.

Hannaman, G.W. and Spurgin, A.J. (1984)
Systematic Human Action Reliability Procedure (SHARP). Electric Power Research Insititute, Report EPRI NP-3683, June 1984.

Hirschberg, S. (1987a)
Retrospective Analysis of Dependencies in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. RAS-470(87)4 (ABB Atom Report RPC 87-36), July 1987.

Hirschberg, S. (1987b)
Probabilistic Safety Analysis: Limitations and Current Development. Lecture Notes, NKA Seminar Risk Analysis and Safety Philosophy, Otnäs, Finland, November 12-13, 1987.

Hirschberg, S. (1988)
NKA-project Risk Analysis (RAS-470): Boundary Conditions for Reference Study on Uncertainty and Sensitivity Analysis. Report RAS-470(88)1 (ABB Atom Report RPC 88-137), February 1988.

Hirschberg, S. (1989)
Project Plan: Defences Against Common Cause Failures (CCFs) and Generation of CCF-data. Pilot Study for Diesel Generators (DGs). ABB Atom Report RPC 89-60, July, 1989.

Hirschberg, S. ed. (1987)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report RAS-470(86)14 (ABB Atom Report RPA 86-241), June 1987.

Hirschberg, S., ed. (1989)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Reference Study on Human Interactions. Final Report RAS-470(89)17 (ABB Atom Report RPC 89-112), December 1989.

Hirschberg, S., Björe, S. and Jacobsson, P. (1989a)
Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA '89 -International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S. and Jacobsson, P. (1988)
NKA-project Risk Analysis (RAS-470): Reference Study on Uncertainty and Sensitivity Analysis, Phase 1. Report RAS-470 (88)15 (ABB Atom Report RPC 88-82), June 1988 (Revised November 1988).

Hirschberg, S. and Jacobsson, P. (1989)
NKA-project "Risk Analysis" (RAS-470): Reference Study on Uncertainty and Sensitivity Analysis, Phase 2 & 3. Report RAS-470(89)6 (ABB Atom Report RPC 89-42), May 1989.

Hirschberg, S., Jacobsson, P., Petersen, K.E., Pulkkinen, U. and Pörn, K. (1989b)
Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Hirschberg, S., Jacobsson, P., Pulkkinen, U. and Pörn, K. (1989c)
Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S. and Knochenhauer, M. (1986)
Application of Sensitivity Analysis in Nuclear Power Plant Probabilistic Risk Assessment Studies. Risø International Conference on Models and Uncertainty in the Energy Sector, Risø, Denmark, February 11-12, 1986.

Hirschberg, S. and Knochenhauer, M. (1987)
Advantages of the Four-divisional Safety Design. IAEA International Conference on Nuclear Power Performance and Safety, Vienna, Austria, September 28 - October 2, 1987.

Hirschberg, S. and Knochenhauer, M. (1988)
Applicability of Probabilistic Safety Criteria in View of Evaluation of PSA Results. IAEA Technical Committee Meeting on the Use of Probabilistic Safety Criteria, Vienna, Austria, April 11-15, 1988.

Jacobsson, P. (1988a)
Comparison of two CCF-models, Alpha-factor Model and MGL-model. Report RAS-470(88)29 (ABB Atom Report RPC 88-108), August 1988 (Revised in October 1988).

Jacobsson, P. (1988b)
Sensitivity Study of Manual Depressurization and Manual Reclosure of 314-valve in Swedish PSAs. Report RAS-470(88)26 (ABB Atom Report RPC 88-113), August 1988.

Jacobsson, P. (1988c)
Sensitivity Study of Back-flush Operation in Swedish PSAs. Report RAS-470(88)28 (ABB Atom Report RPC 88-118), October 1988.

Jacobsson, P. (1988d)
Sensitivity Study on Diesel Generator and Pump CCF-data in the Swedish PSAs. Report RAS-470(88)32 (ABB Atom Report RPC 88-160), December 1988.

Knochenhauer, M. (1988)
NKA/RAS-450 Project: Pilot Project On Valve Data Analysis. ABB Atom Report RPC 88-59, June 1988.

Levine, S. and Stetson, F.T. (1986)
Safety Goals for Nuclear Power Plant Regulation. Progress in Nuclear Energy,17, pp. 203-229, 1986.

Lewis, H.W. (1984)
Probabilistic Risk Assessment: Merits and Limitations. 5th International Meeting on Thermal Nuclear Safety, Karlsruhe, Federal Republic of Germany, September 10-13, 1984.

Lindley, D.V. (1988)
Making Decisions. Second edition, John Wiley & Sons, 1988.

Lydell, B.O.Y., Moieni, P. and Spurgin, A.J. (1986)
Human Reliability Analysis of Ringhals 1 Back-flush Operations. Report NUS-4911, NUS-Corporation, July 1986.

Mankamo, T. (1988)
Dependent Failure Modeling in Highly Redundant Structures - Application to BWR Safety Valves. Scandinavian Reliability Engineers Symposium 1988, Västerås, Sweden, October 10-12, 1988.

Mankamo, T. (1989)
Project Plan: CCF Analysis of High Redundant Systems, Safety Relief Valve Data Analysis and Reference Application. Avaplan Oy Report, September, 1989.

Moricz, P. (1988)
Barsebäck Nuclear Power Plant - Human Reliability Analysis of Back-flush Operations after a Loss of Coolant Accident. Scandinavian Reliability Engineers Symposium 1988, Västerås, Sweden, October 10-12, 1988.

Mosleh, A., Fleming, K.N., Parry, G.W., Paula, H.M., Worledge, D.H., Rasmuson, D.M. (1988)
Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Procedural Framework and Examples. Report NUREG/CR-4780 (EPRI NP-5613), PLG-0547, vol. 1, January 1988.

Mosleh, A. and Siu, N.O. (1987)
Multi-parameter Common Cause Failure Model. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Murley, T.E. (1985)
Implementation of Safety Goals in NRC's Regulatory Process. ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, California, U.S.A., February 24 - March 1, 1985.

NUS-Corporation (1984)
Ringhals 2 Safety Study. Report NUS-4365, May 1983 (Revised February 1984).

OKG AB (1986)
Oskarshamn 3 Safety (in Swedish), 1986.

OKG AB (1987)
Oskarshamn 1 Safety Study (in Swedish), 1987.

Parry, G.W. (1984)
Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty. 1984 Annual Meeting of the Society for Risk Analysis, Knoxville, Tenn., September 30 - October 3, 1984.

Petersen, K.E. (1990)
Reference Study on Uncertainty and Sensitivity Analysis, Phase 2. Report RAS-470(89)7, Risø, to be published 1990.

Pulkkinen, U. (1986)
Comments on Uncertainties and Limitations of Systematic Risk Analyses. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.

Pulkkinen, U. (1989)
Bayesian Uncertainty Analysis of Probabilistic Risk Models. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Pulkkinen, U., Huovinen, T. and Kuhakoski, K. (1987)
Combination of Several Data Sources. PSA '87 -International SNS/ENS/ANS Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

Pulkkinen, U., Kuhakoski, K., Pyy, P. (1988)
Uncertainty and Sensitivity Analysis of an Accident Sequence in Forsmark 3 PSA - VTT Contribution to the Phase 1 of the NKA/RAS-470 Reference Study on Uncertainty and Sensitivity Analysis. Report RAS-470(88)16 (VTT Report SÄH 18/88), October 1988.

Pulkkinen, U., Kuhakoski, K. and Pyy, P. (1989)
Reference Study on Uncertainty and Sensitivity Analysis. Report on Phases 2-3. Report RAS-470(89)9 (VTT Report SÄH 22/89), September 1989.

Pulkkinen, U. and Pörn, K. (1989)
Uncertainty in Safety Analysis and Safety Related Decision Making. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Pörn, K. (1988)
Analysis of parametric uncertainty in the PSA of Forsmark 1/2 (in Swedish). Studsvik Report NP-88/46, 1988.

Pörn, K. (1989)
Some Comments on CCF-quantification, The Experience from the Nordic Benchmark. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-20, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 243-255.

Pörn, K. and Fahlén, R. (1988)
Reference Study on Uncertainty and Sensitivity Analysis. Report RAS-470(88)17 (STUDSVIK Report NP-88/53), October 1988.

Pörn, K and Fahlén, R. (1989)
Reference Study on Uncertainty and Sensitivity Analysis, Code Comparison and Best Estimate. Report RAS-470(89)8 (STUDSVIK Report NP-89/81), September 1989.

Rasmussen, J. (1983)
Skills, Rules and Knowledge; Signals, Signs and Symbols and other Distinction in Human Performance Models. IEEE Trans. on Systems, Man and Cybernetics, SMC-13, 3, 1983.

Samanta, P.K., O'Brien, J.N. and Morrison, H.W. (1985)
Multiple-Sequential Failure Model: Evaluation of and Procedures for Human Error Dependency. Report NUREG/C-3837, May 1985.

Sandstedt, J. (1988)
Pipe Break Frequencies (in Swedish). Report RELCON-16/88, November 1988.

Simola, K., Pulkkinen, U. and Huovinen T. (1988)
Analysis of Time Dependencies in Probabilistic Safety Assessments. Scandinavian Reliability Engineers Symposium, Västerås, Sweden, October 10-12, 1988.

Swain, A.D. and Guttman, H.E. (1983)
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, NUREG/CR-1278, August 1983.

Swedish State Power Board (1984)
Ringhals 1 Safety Study (in Swedish), October 1983 (Revised in August 1984).

Sydkraft (1987)
Barsebäck 1 Safety Study (in Swedish), January 1985 (Revised January 1987).

Tuvesson, L. (1988)
Sensitivity Study - Repair of Containment Cooling Spray System Function (322/721/712) in Swedish PSAs. Report RAS-470 (88)33 (ABB Atom Report RPC 88-141), December 1988.

U.S. Nuclear Regulatory Commission (1989)
Reactor Risk Reference Document. Report NUREG-1150, Washington, D.C., U.S.A., June 1989.

Wahlström, B. (1986)
Probabilistic Safety Analysis and Human Errors. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.

5. STUDIES OF SELECTED TOPICS

This chapter covers the activities of the RAS-470 project concerning such aspects as time-dependent phenomena in PSA (Simola et al., 1988), combination of data sources (Pulkkinen et al. 1988) and treatment of external events (Hirschberg and Gunsell, 1989). A common feature of these topics is that the associated uncertainties play a major role and that potential for improvements in the context of PSA is significant.

5.1 Time-dependent Phenomena in PSA

The PSA-models are usually constructed to describe the plant safety in a static way. Several time-dependent phenomena are modeled as various time averages or stationary situations. If PSAs are applied in continuous monitoring of the plant safety or in dynamic decision making, more detailed models for time-dependencies are needed. The time-dependent PSA-models and problems were shortly reviewed within the NKA/RAS-470 project (Simola et al., 1988). The various time-dependencies were classified and characterized, the time-dependent reliability models were discussed and two small case studies concerning ageing of nuclear power plant pipings and statistical analysis of motor-operated valve failure data, were performed.

5.1.1 Classification and characterization of time dependencies

The time-dependent phenomena affecting the results of PSA are numerous and in many cases they are coupled with each other and with other mechanisms. To give an outline of the phenomena a simplified classification of time-dependent mechanisms is presented in Table 5.1. In the following each time dependency category is also shortly characterized.

The time dependency of failure rates is not usually taken into account in PSAs, mainly because of the lack of statistical evidence and practical models. The core damage frequency is directly proportional to the initiation event frequency. Usually the time dependency of failure rates of individual components does not have a very strong impact on the core damage frequency, but the failure rates of a set of components may increase simultaneously which might strongly affect the final result.

Table 5.1

Time dependency categories

Time dependency category	Remarks
Time-dependent failure rates	- affect the component failure probability and initiating event frequency
1. AGEING	
2. LEARNING	- different for components with short and long life lengths
	- different ageing mechanisms
Time-dependent unavailabilities	- not always modeled in PSAs - affect also CCF-probabilities
1. TEST INTERVAL DEPENDENCIES 2. TEST ARRANGEMENT DEPENDENCIES 3. LATENT FAILURES NOT REVEALED IN TESTS 4. REPAIR UNAVAILABILITIES	- rather complicated models
Time dependencies of accient sequencies	- affect both level 1 and 2 PSA results
1. TIME-DEPENDENT SUCCESS CRITERIA	- one of the main uncertainties in PSA
2. TIMING OF EMERGENCY SYSTEM OPERATION	- different models exist
3. TIMING OF OPERATOR ACTIONS 4. TIME DEPENDENCY OF OPERATOR ERROR PROBABILITIES 5. TIME-DEPENDENT PHYSICAL PHENOMENA	- treatment with sensitivity studies
Increase of statistical evidence	- problem of living PSA
	- possibility to take several factors into account in PSA failure data

The time dependency of failure rates and initiating event frequencies can be divided in two categories depending on the mean time between failures or events. Components with rather short mean time between failures (compared with the plant operation time) may have trends in failure processes such that the time between successive failures will tend to become shorter (or longer) depending on the effectiveness of repair and maintenance actions. In other words the failure behaviour of the components depends on the earlier failure history and it cannot be described by the ususal renewal models. This kind of ageing may be typical of process components such as valves, pumps and diesel generators. Also most of the anticipated transients behave in the same way. The ageing process may be connected directly to the time or to the failure events; models for both cases are discussed later.

Some componets, e.g. pipings and pressure vessels have rather long life-lengths and it is not probable that they will fail during the plant operation. In these cases the interesting entity is the time up to the first failure. If the time up to the first failure obeys nonexponential distribution we can use the word ageing. The methods to estimate or determine these distributions are numerous but in practice the empirical evidence is missing.

The unavailability of a standby system is dependent on the interval between tests or inspections. In PSAs, the unavailability of standby system is usually evaluated as mean unavailability, which is test interval dependent. Only in rare cases the exact (calendar) time-dependent unavailability is required. If the test or inspection interval is long or if there are failures which are not revealed in tests the evaluation of the exact unavailability may be useful. For this purpose estimates of standby failure rates and time independent failure probabilities are needed. The estimation of these parameters from plant operation experience sets requirements on the plant data collection.

The standby system unavailability is also dependent on the test arrangements, especially timing of the tests is essential. Common cause failure probabilities are also affected by test arrangements. The system availability estimates are very sensitive to assumptions made about the revealability of latent common cause failures and test arrangements.

The time dependency of repair unavailabilities is not often critical for the PSA-results. Only in cases where recovery from failures is considered it has an essential impact on the results. An example is the recovery from the loss of offsite power.

Accident propagation after initiating events is a time-dependent phenomenon. Accident development is highly dependent on the startup moment of emergency systems. Success criteria concerning emergency systems change with time, for instance, requirements on residual heat removal decrease with time after an accident. Some emergency systems must start many times during the accident sequence. The above time-dependent phenomena have an effect both on the probability of accident and its consequences (level 2 & 3 PSA).

The time dependency of operator error has been taken into account in several analyses. Operator errors are coupled to other time-dependent features of an accident and the analysis of all important factors is extremely difficult.

Operating experience concerning plant disturbances, component failures, test and repair actions and other human actions cumulates during the plant operation. Using this operating experience or evidence it is possible to update both data bases and PSA-models. If the failure models used are compatible with the operating experience, i.e. the failures follow the models postulated in PSA, strengthening of evidence leads to greater confidence of PSA-results.

Larger statistical data bases make it possible to analyse failure mechanisms in detail. Statistical tests may reveal incompatibilities between models and experiences. In order to take these observations into account new statistical models are usually introduced. These models may, for instance, describe the non-exponentiality of the repair time distributions. Generally these models have more parameters which must be estimated from data. The estimation of multiparameter models requires more data for which increase of statistical evidence during plant operation is not sufficient. Thus the increase of statistical evidence does not necessarily lead to greater statistical confidence of the PSA-results.

5.1.2 Models of time dependencies

Failures of a component for which the failure time distribution remains the same during the plant history can be described with the usual renewal process models (see for example Cox, 1962 and Rau, 1970). If the failure times are exponentially distributed the renewal model is reduced to a homogeneous Poisson process.

Renewal process models yield the probabilities of failure occurrences. The expected number of failures over certain time interval is of general interest. If the derivative of the expected number of failures exists, it is called the renewal density which in our case describes the expected number of failures per time unit. It should be noted that generally the renewal density is not constant. However, it is practically constant after a rather short time period.

The statistical estimation of renewal processes reduces to the estimation of parameters of life length distributions for which there exists a lot of statistical software (see Huovinen, 1989).

If we do not assume the "as good as new" behaviour we must use models different from the renewal process models. The most simple models are modifications of Poisson processes. According to the non-homogeneous Poisson model, the component is not replaced with a new one after failure. It is assumed that the hazard rate of the component after failure is exactly the same as immediately before failure, i.e. the component behaves in "as bad as old" manner (see Snyder, 1975 and Keller, 1984). The intensity of the process is a general function of time which makes it possible to model both learning and ageing. It is worth noticing that non-homogeneous Poisson process models only describe the ageing with time and in these models the number of failures which occurred earlier in the component does not affect the future behavior.

In practice, the failure intensities may also depend on the number of failures which occurred earlier in the component. In this case we speak about ageing/learning with events. Snyder (1975) discusses several models of this category and Vaurio (1986) gives an application example concerning learning from reactor accidents.

Ageing with both time and events can also be modeled (see Snyder, 1975). In principle the models are rather simple modifications of Poisson processes but they will not be discussed here. Their practical application to PSA-models may be rather complicated and their estimation requires a lot of data.

The ageing trends can be identified from field data by applying some standard statistical techniques. Akersten (1986) discusses the bivariate TTT-transform. Although the method is not very complicated it seems that its application requires a lot of evidence.

Components with long lifetime do not probably fail during plant operation time but the probability of failure occurrence may increase in time. In PSA-applications we are interested in the distribution of the time up to the first failure. The hazard fucntion may depend on several parameters which can be estimated from data. In practice failure occurrences are so few that the estimation is rarely successful and thus the failure time distribution cannot usually be postulated directly.

One possibility to obtain the failure time distribution is to construct a stochastic process which describes the random development of a failure. The failure time distribution may be derived from the stochastic process models by calculating for example first passage time distributions. The parameters of these processes can be evaluated on the basis of material properties of the component. Models based on various stochastic processes are discussed in the literature (see Birnbaum and Saunders, 1969; Bogdanoff and Kozin, 1985, Moelling and Gallucci, 1985, Ditlevsen, 1986, Newby, 1987); most of them are based on Markovian processes.

Usually the time dependency of component or system unavailabilities is neglected in PSA-models. This kind of time dependency is discussed in more detail in another NKA-project, NKA/RAS-450 (Laakso et al., 1990) and thus we do not consider these models here.

The unavailability of continuously operating systems is usually evaluated with Markow models which reach the stationary state in rather short time. This is the reason why the stationary probabilities are used instead of the exact time-dependent expressions. In some undoubtedly rare cases exact values are needed.

The time-dependent success criteria of emergency systems can, in principle, be modeled by using standard fault tree techniques. However, accident mitigation can be seen as a phased mission problem, modeling of which requires consideration of some additional features. Mankamo (1986) discusses various approaches, such as phased mission diagram and event sequence diagram in which also operational decisions can be included. For quantification of phased mission problems Mankamo (1986) suggests use of various conditional unavailabilities or projected unavailabilities. The phased mission analyses are also discussed in (Fussell et al., 1981).

Many phenomena, including those encountered in the Nordic Reference Study on Uncertainty and Sensitivity Analysis can be formulated in the form of phased mission reliability problem (see subchapter 4.2). The lack of data concerning failure rates of components activated several times during a rather short time period limits the practical validity of these approaches.

In many cases the timing of operator interactions is very important for accident mitigation. This problem can also be evaluated using methods of phased mission reliability analysis. However, it is difficult to estimate operator error probabilities and estimation must be based on judgements.

The operator error probabilities are dependent on the time available for the operator to understand the situation and take necessary measures. This problem is usually solved by using time-reliability curves and so called cognitive reliability models.

Usually the increase of statistical evidence is not modeled in PSA. If the statistical failure models are compatible with the operating experience then the increase of evidence leads directly to smaller uncertainty of final PSA-results. To avoid incompatibilities between operating experiences and PSA failure models more detailed analyses of operating experiences are needed.

These analyses should include estimation of constant failure rates and statistical tests for ageing trends, estimation of time-dependent failure rates, evaluation of statistical confidence intervals for model parameters, and depending on the situation many other analyses. These analyses require very efficient failure reporting systems which also include data on the numbers of system and components demands.

5.1.3 Case studies

5.1.3.1 Pipe failures

In a nuclear power plant, many safety-related systems contain components that can be affected by a long-term age degradation. The prediction of ageing is important to estimate the level of safety and reduce the uncertainties in PSAs. In a PWR plant, the major limiting component for the technical lifetime is the reactor pressure vessel since it is difficult and expensive to replace. Most of the other ageing components are changeable or repairable. Here we concentrate on modeling of piping degradation.

Pipe cracking in light water reactors can result from cyclic loadings; the phenomenon is called fatigue crack growth. The crack growth modeling is usually based on data from accelerated life testings. Another type of pipe degradation is intergranular stress corrosion cracking (IGSCC) occurring in sentitized, heat affected zones in welds in connection with environmental effects (e.g. stresses and high oxygen content in water). IGSCC propagates faster than corrosion fatigue and causes defects in BWR piping, which can result in leakages if the damaged pipes are not repaired or replaced in time. IGSCC can be mitigated by using suitable materials and by reducing the oxygen content of water.

Repeated experiments in identical laboratory conditions show significant scatter in crack growth rates giving reason to a stochastic interpretation rather than a deterministic approach. In spite of this, the crack growth has usually been modeled with deterministic means. The large fluctuation of crack growth rate around the expectation value can be taken into account using probabilistic interpretation of the phenomenon. Probabilistic models of crack growth can be divided into two groups: the use of probability distributions of the lifetime, and stochastic processes describing the crack growth rate.

Choice of a suitable distribution depends on the specific case. The distribution should fit the physical behaviour of the modeled phenomenon. Thus the physical background should be well known. Corrosion induced failure of stainless steel specimens under simulated conditions has been modeled

with various distributions, the most frequent ones being Weibull-, Gamma-, Log-normal- and extreme value distributions. Also Birnbaum-Saunders model has been used. Kozin and Bogdanoff (1987) studied the role of third order statistics and compatibility of different distributions and physical facts. Their conclusions argue that Weibull distribution is unsuitable to describe the crack growth, and they suggest the use of log-normal, inverse Gaussian and Birnbaum-Saunders models.

Due to the conceptual and calculational flexibility of Markov processes they have been applied as basis for the cumulative damage models (discussed in Bogdanoff and Kozin, 1985 and Kozin and Bogdanoff, 1987). In many cases, the Markov property can be assumed, and the phenomenon can be described by a Markov process. In the simplest case, the process is stationary and discrete in time and in state. The effect of incomplete crack monitoring and repair actions can be included in the Markovian cumulative damage models rather easily.

Discrete time and state models are applicable to problems with cyclic loading, discretised time representing the cycles and state corresponding to different crack depth (damage state). The crack growth model can be illustrated by a simple transition probability matrix. This approach concerns the cyclic loading and the Markov property is assumed only between the crack tip conditions at the end of the cycle. It must be pointed out that the crack propagation is not continuous in time. For continuous crack propagation (constant stress) other models should be applied. One possibility is to assume that cycles occur randomly in continuous time according to a simple homogeneous Poisson process and the cracks propagate acccording to the crack growth model. The estimation of the parameters of the crack growth model is difficult.

Other considered stochastic models for crack growth are the randomization of Paris equation (Paris and Erdogan, 1963) and its various forms. The Paris equation is a deterministic model for fatigue crack growth. In order to take into account the stochastic behaviour of the phenomenon, the Paris model can be randomized. The simplest case is to randomize the pre-existing crack distribution, but more sophisticated methods have also been developed.

Ditlevsen (1986) studied the randomization of the logarithmic form of Paris equation. Sobczyk (1986) has also developed a stochastic crack growth model based on randomization of the Paris equation, and studied the properties and usefulness of the model. The crack growth is a function of time which is connected to the random occurrence of stress cycles. In addition the unknown random factors of environment are taken into account as a white noise.

The time evolution of a structural reliability can be described with a stress-strength model where the applied stress or load and the strength of the structure are continuous stochastic processes. Generally, the strength decreases in time while the stress is assumed for example to fluctuate around a time-independent expectation value. The failure occurs when the stress exceeds the strength.

The computer code PRAISE (Piping Reliability Analysis Inlcuding Seismic Events) has been developed in Lawrence Livermore National Laboratory to simulate the life history of a PWR primary coolant piping (Lu et al., 1981). Later, the program has been modified and extended to consider residual and vibratory stresses, and stress corrosion cracking prediction in BWRs (Harris et al., 1982 and Harris et al., 1986).

The fatigue crack growth is modeled using the Paris fracture mechanics model with stochastic inputs of initial crack size distributions, material properties, stresses, and detection probabilities. The crack growth is two-dimensional so that also the crack length is calculated with fracture mechanics model. Preservice and inservice inspections are also considered. The initiation of stress corrosion cracking is calculated from stresses, sensitization, and environmental efforts related to the oxygen content in the water. The material parameters are calculated generally by a linear regression of data from stress corrosion cracking tests and residual stresses. The deviation is taken into account by assuming , for example, that the parameters are log-normally distributed. The estimates of residual stresss levels are adjusted to agree with field observations.

5.1.3.2 Statistical ageing analysis of motor-operated valves in Swedish nuclear power plants

In order to demonstrate the use of nonhomogenous Poissson processes as ageing models, Swedish motor-operated valve operating experiences were analysed. The data base was the failure history of motor-operated valves at some Swedish nuclear power plants. The same data base was analysed in the Common Cause Failure Data Benchmark Exercise (Hirschberg, ed., 1987) and it was supplied by ABB Atom from the Scandinavian Nuclear Power Reliability Data system (ATV-system). The total number of failures was 340 and the failures were classified into two categories (critical and noncritical failures).

A simple nonhomogenous Poisson process model (Weibull-process) was applied. The model parameters were estimated with the maximum likelihood method. The estimation was carried out using the computer code ENHPP developed by VTT (Huovinen, 1989). The code ENHPP finds the maximum of the likelihood function and evaluates the covariance matrix of the parameter estimates based on the Fisher's information matrix.

The failure histories were analysed plantwise because of the possibility of differencies between plants. Further, critical and noncritical failures were analysed separately. The valve population at each plant is assumed to be homogeneous, i.e. each valve is assumed to behave according to the same monhomogenoeous Poisson process. The validity of this assumption may be questioned but in case of other assumptions the failure data would have been insufficient. The observations concerning the decrease or increase of failure intensities could be used as a guideline for further qualitative and quantitative data analyses.

Results of the statistical analyses indicated both reliability growth and decrease. The failure trends could partly be due to changes in failure reporting principles. In some cases the existence of failure trends was rather clear, but the identification of the cause of the phenomenon would have required extensive qualitative analyses. In most of the cases the statistical significance of the results was not sufficient.

The analyses were mainly statistical and quantitative. It was not possible to carry out detailed quantitative analyses of failure causes, mechanisms and

repair activities. The qualitative analyses are extremely important in identification of various ageing mechanisms. More knowledge on the principles of failure data collection and failure reporting is also needed.

The use of nonhomogeneous Poisson process models constitutes one possibility to describe the observed failure trends. The models are rather simple and their statistical treatment is easy with existing computer software. Various failure trends, including reliability growth and deterioration, may be described by nonhomogenous Poisson models. However, it should be pointed out that these models are based on the mathematical minimal repair (as-bad-as-old) assumption, and thus they describe only such, rather peculiar failure processes.

5.1.4. Conclusions and recommendations

Some recomendations and conclusions concerning the analysis of time dependent phenomena can be drawn on the basis of the work done withing this project. First of all, much research should be carried out in order to identify the most important ageing mechanisms and forms of time dependence. The identification must be based on the knowledge concerning the physics of ageing and thermohydraulic processes. Furthermore, the results of PSAs are needed to choose the components or phenomena for which the time dependency analysis should be performed. In this choice use of sensitivity analyses and applications of importance measures are recommended.

The results of a level 1 PSA may be used to choose the components having the dominant impact on the core damage probability. Use of the higher level PSA as a basis for component choice might lead to different results which include impact of the consequences of reactor accidents. Both of these aspects are important and the choice should be done carefully. At the system level, the results of systems reliability analyses can be used.

After selection of the interesting time-dependent phenomena one should perform detailed qualitative analyses in order to identify the most significant aspects. At component level these analyses should include failure mode and effect analyses especially focused on ageing mechanisms and physical analyses of different types of corrosion etc. Also maintenance effect

analyses are needed. At the system level, the effect of physical phenomena during accident should be studied in order to identify the possible time-dependent success criteria and various phases of accident propagation. The effect of tests and the revealability of failures are also important.

Modeling of time dependencies depends on the specific system under consideration, on failure mechanisms and on statistical data available. The models must not be too complicated and they must be compatible with the available data. In the course of modeling, various sensitivity analysis are useful for making proper decisions.

The time dependency analysis is not a task of a conventional PSA. It is possible that detailed time dependency analyses require too much resources to be included in the standard PSA. However, a detailed review of PSAs can lead to recommendations to include time dependency analyses of some specific issues. Some of the time dependency analyses are typical of so called living PSA.

Research activities concerning ageing of reactor pressure vessels and pipings is being carried out in several institutes and the results are not yet available. Also projects concerning the nuclear power plant life extension are in progress. In the Nordic countries we should be able to follow the research and apply the results in an efficient way.

5.2 Combination of Data Sources

5.2.1 Introduction

The lack of relevant and sufficient data is a problem often encountered in PSAs. Very often this problem has to be solved by generating purely subjective estimates or subjective probability distributions for unknown parameters on the basis of judgements.

In many cases also the structure of accident models is uncertain and the models are based on judgements of the analysis team. The problems are related to physical phenomena occurring during an accident or to the success

criteria of the emergency systems. Frequently the models are conservative. The problem was dealt with for example in the course of the NUREG-1150 study (U.S. Nuclear Regulatory Commission, 1988).

Nowadays there are several reliability data sources available. The power plant utilities, suppliers and the international organizations collect operating experiences from nuclear and conventional power plants. The uncertainty about the value of unknown parameters or the physical models is often solved by combining several pieces of evidence or judgements of several experts. There are some procedures for combining different data sources. However, applications of these methods are highly subjective.

The heterogeneity of nuclear power plants with respect to their main characteristics of the plants, on the one hand, and to the differences between the operational performances, on the other hand, results in a problem: how relevant or usable are the the availability data from different sources or the operating performance data from other plants, when we are evaluating, for example, plant specific failure rates of components for PSA-studies. Although the components and the plants are quite identical with respect to their engineering characteristics, there can be some plant operation and maintenance related factors, which correlate with the performances of the plants and their components.

Within this project the problem was encountered both in the CCF-data Benchmark Exercise and in the Reference Study on Uncertainty and Sensitivity Analysis. In the CCF-data Benchmark Exercise the CCF-probability had to be estimated on the basis of failure observations from various systems with different redundancy levels and designs. In the Reference Study on Uncertainty and Sensitivity Analysis similar problems were connected with estimation of human error probabilities and judgements concerning the relevance of failure data. The problems were also discussed in some separate reports concerning combination of several data sources and Bayesian uncertainty analyses of risk models (Pulkkinen et al., 1987 and Pulkkinen, 1989).

5.2.2 Methods

5.2.2.1 Empirical Bayes methods

In the Swedish Reliability Data Book (T-Book; Bento et al., 1985) the problem of combination of several data sources has been solved by utilizing an empirical Bayes-method. It is assumed that component failure rates or failure probabilities per demand are random variables. The component to component variability of failure is described by a probability distribution (gamma distribution for failure rate and beta distribution for failure probability) and the distribution is estimated from the component failure observations. The estimated distribution is then used as a prior distribution in the Bayesian evaluation of individual component failure parameters. Rather similar method developed by Vaurio and Lindén (1986) is used by the Finnish utilities in their PSA work. These empirical Bayes procedures make it possible to incorporate the experiences from other plants or components into the estimation of individual component parameters. The empirically estimated prior distribution describes in a way the inhomogeneity of the component population and thus the problem of the relevance of various data sources with respect to the case under analysis has been solved. The methods are not fully Bayesian according to the classification by Singpurwalla (1986). The recent Bayes-empirical-Bayes-method developed by Pörn (1989) for the coming version of the T-book follows the Bayesian paradigm completely. As opposite to the empirical-Bayes method the Bayes-empirical-Bayes method is based on subjectively assessed prior distribution.

The methods for estimating failure parameters may be judged as "empirical" or "subjective". In fact, the empirical-Bayes method is "empirical" since all distributions are estimated directly on the basis of statistical data. The Bayes-empirical-Bayes method is "subjective" because the prior distributions are selected subjectively by the analyst. However, the above classification is not complete. Every trial to model failure phenomena includes a subjective element since the models are always selected more or less subjectively in order to make the calculation possible. Also the data bases used in the estimation process are chosen subjectively. Furthermore, the observations are often interpreted in various ways which are always effected by some

analyst dependent factors. These factors originate from the experience which the analyst has gathered; they may be based on statistical or empirical observations but they cannot exhaustivly be formulated for example with likelihood functions or with other similar concepts.

The objectivity of the "empirical methods" can thus be questioned because of the enormous number of possible interpretations of the raw data material. The objectivity of the "objective methods" cannot be increased by forgetting these uncertainties.

5.2.2.2 Weigthing methods

In the PRA Procedures Guide (U.S. Nuclear Regulatory Commission, 1983) a method referred to as the "mixture method" is discussed. It involves fitting a suitable prior to each generic source (E_i, i = 1, 2,,....,, n) and then combining the individual distributions ($f_i(\theta|E_i)$, where θ is the parameter of interest) by forming a mixture:

$$f(\theta) = \sum_{i=1}^{n} w_i f_i(\theta|E_i),$$

where $0 \leq w_i \leq 1$, $w_i + w_2 + \ldots + w_n = 1$ are the weighting factors.

The PRA Procedures Guide also provides a method to update the weighting factors and discusses the methods to give the numerical values for the factors. The selection of the weights is always based on judegements.

Another method for combining several evidences has been proposed by Pulkkinen et al. (1987). Basically the same ideas have been applied by Mosleh and Siu (1987) in estimation of common cause failure probabilities. Both approaches utilize the possibility to define a subjective probability distribution in the space of all relevant evidences or operational experiences.

Again, it is assumed that there are N independent data sources or evidences E_i, i = 1, 2,...., n. Furthermore, the relevance (or usefulness) of the evidence E_i to be used as evidence for the case being analysed is interpreted in a probabilistic way:

$$P(E_i \text{ is relevant}) = w_i, \quad 0 \leq w_i \leq 1, \; i = 1,2,\ldots,n$$

For completely relevant data sources $w_i = 1$. Since the weights w_i are interpreted as subjective probabilities, it is a problem of the calculus of probability to evaluate whether several data sources are simultaneously relevant. If the evidences are independent then the probability of each combination of evidences may be calculated by multiplying the weights:

$$P(E_i,\ i \in I \text{ relevant},\ E_i,\ i \notin I \text{ not relevant}) = \prod_{i \in I} w_i \prod_{i \notin I} (1 - w_i) = \varepsilon_I,$$

where $I = \{i_1, i_2, \ldots\ldots, i_k\}$, $k \leq n$ is a set of relevant evidences. There are 2^n different sets of relevant evidences each having its own weight ε_I. The combination of evidences belonging to a set of relevant evidences, I, is called "extended evidence", and it is denoted as the union

$$E_I^* = \bigcup_{i \in I} E_i$$

For example, if the original evidences are $E_i = \{v_i \text{ failures at } m_i \text{ tests}\}$, the extended evidence is of the form

$$E_I^* = \{\sum_{i \in I} v_i \text{ failures in } \sum_{i \in I} m_i \text{ tests}\}$$

If the knowledge concerning the unknown quantity θ prior to the observations is expressed as a prior distribution the posterior distributions, $f(\theta|E_I^*)$, corresponding to each extended evidence, can be determined using the Bayes formula. The final posterior distribution in which all the extended evidences are included is the mixture of the form:

$$f(\theta|E^*) = \sum_I \varepsilon_I f(\theta|E_I^*)$$

The above mixture method was applied by VTT in the Reference Study on Uncertainty and Sensitivity Analysis. The particular case was the analysis of the frequency of the inititating event, and the original evidences were the operating experiences from the Swedish nuclear power plants. Pulkkinen et al. (1987) applied the method in the case of examplary data set concerning the failure probability of a component. The example is also presented here in order to illustrate the method. The data sources and the probabilistic weights of each source are shown in Table 5.2.

Table 5.2

Data for example case

Data source i	Number of failures k_i	Number of trials m_i	Probabilistic weights CASE 1 w_i	CASE 2 w_i
1	0	100	0.1	0.1
2	0	50	0.1	0.1
3	0	20	0.9	0.1

The two cases of Table 5.2 are analysed to illustrate the effect of the choice of weight on the final posterior. In CASE 2 all data sources are considered rather irrelevant. In the analysis, the prior distribution was assumed to be the uniform distribution over the unit interval, and thus the final posterior distribution is a mixture of beta distributions. In CASE 2 the posterior distribution has much more probability mass on large failure probability values, which is due to the weighting factors. The cumulative distributions and probability density functions are shown in Figure 5.1.

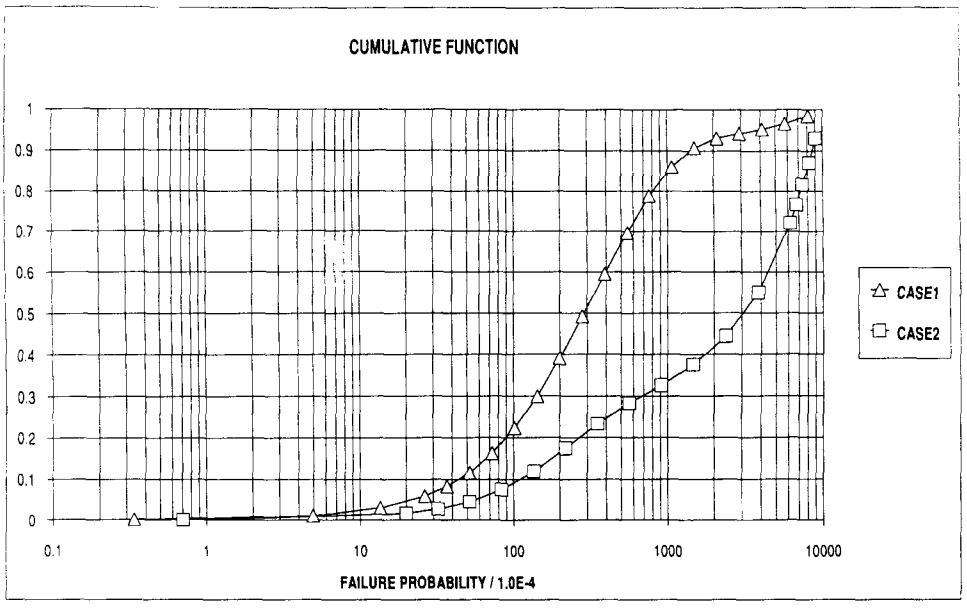
5.2.2.3 Nonprobabilistic methods

Pulkkinen et al. (1987) also considered the possibility to apply so called Shafer-Dempster theory of evidence developed by Shafer (1976). The theory of evidence is based on a slight modification of the axioms of probability. In the theory of evidence the additivity of the probability measure is replaced with the property

$$Bel(A \cup B) \geq Bel(A) + Bel(B) - Bel(A \cap B),$$

where $Bel(\cdot)$ denotes the counterpart of probability, the belief function. In the case of probability "$\geq$" is replaced with strict equality.

The results obtained by applying the theory of evidence are comparable with those obtained using probabilistic methods. This has been demonstrated by Pulkkinen et al. (1987) and in a different case by Holmberg et al. (1989). However, the theory is not fully developed for continuous spaces. Furthermore, the interpretation of the belief functions is not as simple as the interpretation of probability.



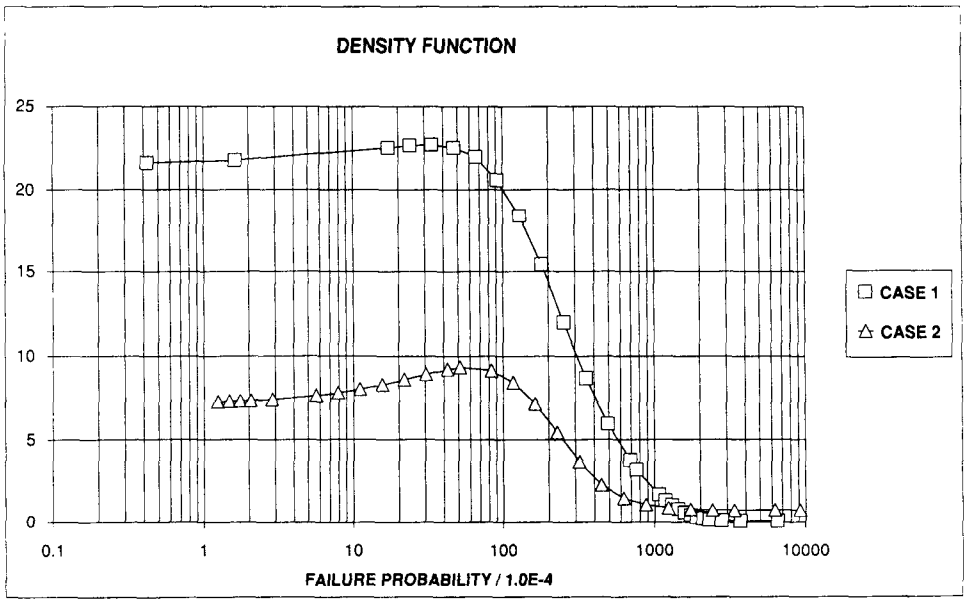


Figure 5.1

Cumulative distributions and probability density functions for example cases

The concepts of modern quantitative risk analysis are probabilistic. In order to use nonprobabilistic methods the concepts of risk analysis should be translated to nonprobabilistic language. This requires much research work and the applicability of results in practical risk analysis may be questionable.

5.2.3 Conclusions

The statistical problems of risk analysis are due to lack of empirical evidence for reliable estimation of the parameters of risk models. For that purpose several methods for combination of different data sources have been proposed and discussed. Many of the problems are caused also by the interpretation of probability. In the present project the problems were frequently encountered, and they had to be solved on the basis of the prevailing state-of-the art.

The solutions discussed in this section are aimed to be practical and, above all, such that they make it possible to use all existing evidence in a systematic way. In some cases their mathematical or philosophical background may not be solid or generally accepted.

The methods discussed yield reasonable solutions for some specific cases. The weighting method proposed by Pulkkinen et al. (1987) has been applied in practical case studies and similar methods are also used by Mosleh and Siu (1987). The same kind of methods are also applied when combining expert opinion. The weighting method contradicts slightly the assumptions behind exponential failure models, and thus this kind of models should be applied with care.

In the present project nonprobabilistic methods were not practically appplied due to the difficulties in the interpretation of the basic concepts and results of these methods. On the basis of minor efforts allocated to this subject it is not possible to draw any strong conclusions about the applicability of the nonprobabilistic approach. There are many problematic issues related to application of nonprobabilistic methods, which, however, have probabilistic solutions. The use of nonprobabilistic methods may, however, help to find solutions to the problems of expert judgements, risk valuation, and acceptance and societal risk analysis.

5.3 Treatment of External Events

5.3.1 Design related defensive measures against external events

In the following external events are defined as accident initiators which are extrinsic to the affected components but not necessarily external to the plant. Examples of external events to be considered in safety analyses include: earthquake, fire, internal and external flooding, extreme winds (tornados, hurricane), lightning, missiles, aircraft crash, chemical explosion.

Several PSAs carried out for plants characterized by low degree of physical separation of structures, systems and components show that considerable contributions to the frequency of severe core damage originate from external events. In many cases it is very difficult to give accurate predictions of low probability events like core damages caused by external phenomena. The probabilistic tools are no longer reliable. It is definitely preferable to have a design which is relatively insensitive to this type of accident initiators.

The four-divisional separation as implemented in ABB Atom's BWR 75 design (with Forsmark 3 and Oskarshamn 3 as reference plants) provides effective inherent defense measures against external low probability/high consequence events. Furthermore, a consistent and logical application of the principles of physical separation aslo means the absence of complicated links, interactions and interconnections between safety related functions.

Reactor shutdown (reactor protection system (RPS) function), emergency core cooling, reactor coolant makeup and emergency residual heat removal are subject to the "two-out-of-four" redundancy principles (in practice with exception for RPS "one-out-of-four" for most initiators). All systems supporting these functions are completely separated into four subsystems. Physical separation means that e.g. the emergency cooling systems are situated in four separate bays in the reactor building, adjacent to the primary containment (Figure 5.2). The onsite standby power units (four diesel generator sets), are situated in four diesel buildings on different sides of the reactor building.

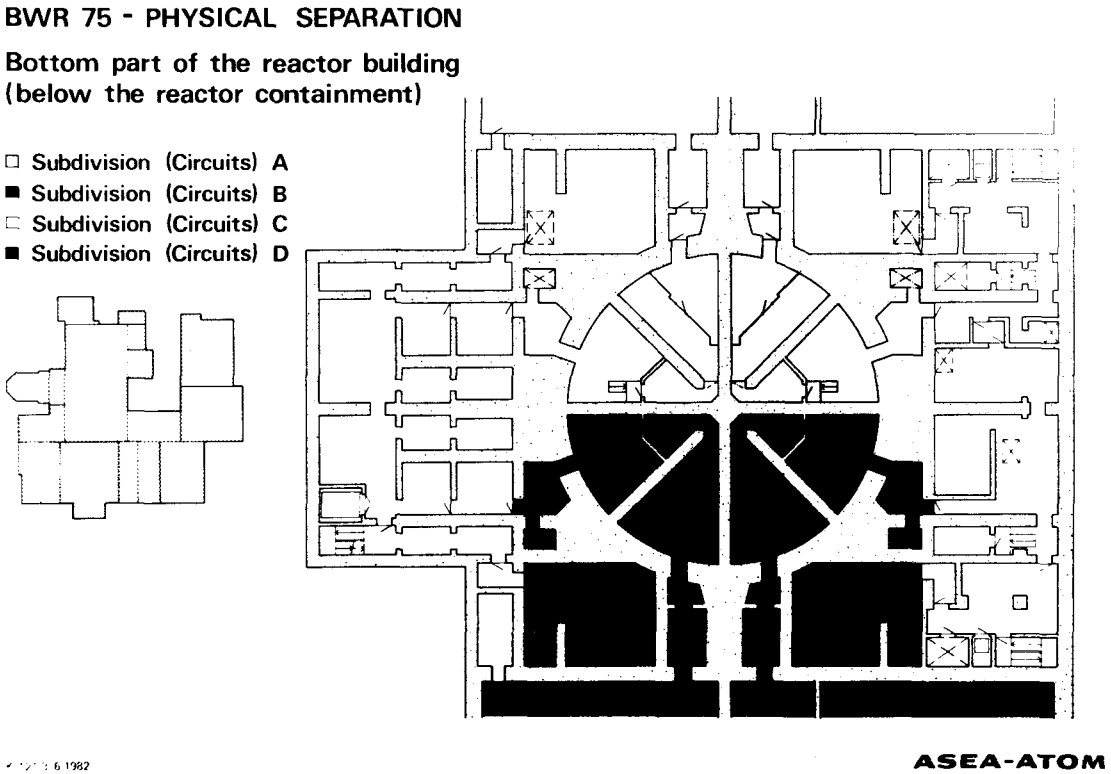

BWR 75 - PHYSICAL SEPARATION
Bottom part of the reactor building
(below the reactor containment)
□ Subdivision (Circuits) A
■ Subdivision (Circuits) B
□ Subdivision (Circuits) C
■ Subdivision (Circuits) D
ASEA-ATOM

Figure 5.2

As far as practically possible even the operational and safety equipment have been separated both from physical and functional point of view. This limits the possibility of failure propagation.

As a consequence of extensive separation between redundant subsystems the protection level of the plant is not sensitive to protection level of separate subsystems as long as it can be shown that a sufficient number of subsystems is unaffected by the event considered.

In view of the design principles outlined above some specific measures of protection against external events, adapted in ABB Atom's BWR 75, will be shortly summarized. For more details we refer to reference (Hirschberg and Tirén, 1989).

5.3.1.1 Flooding protection

Possibility of external flooding, caused by a high water level, is site-dependent. In the Forsmark 3 and Oskarshamn 3 case (BWR 75 reference plants), the protection of the safety equipment against such eventuality is generally assured by placing it on a level which will not be reached by the water from external sources, even under extreme conditions.

The criterion for protection against internal flooding is that safety functions should not be impaired. To meet these requirements, certain rooms containing safety related equipment are designed to be leak-tight to prevent the water from propagation to adjacent rooms. Furthermore, to limit the outflow from a pipe break, the plant is equipped with room monitoring equipment which automatically actuates isolation of the break, thus limiting the outflow to the room.

The analyses of internal flooding have been made for all buildings of safety interest. The different buildings have been designed with discharge opening and runoff ways to meet the water loads from potential internal flooding and satisfy safety requirements.

5.3.1.2 Fire protection

The fire protection rests mainly on passive principles (separation between redundant safety systems, use of fire resistant construction and materials, reduction of quantities of combustible material).

The general principle adapted in BWR 75 is that subs A and C are separated from subs B and D by being placed in different fire zones. In no case must a fire zone share the ventilation equipment or air ducts with another fire zone (with exception for main exhaust air stack), i.e. separate systems are provided for normal ventilation emergency filters and smoke extraction. The fire zones are separated by fire-resistant structures. The main buildings of BWR 75 are divided into nine fire zones (Figure 5.3) which in turn are divided into fire cells of two types (with separate and common normal ventilation, respectively). The degree of separation is determined by the fire-load of the area considered and also by other hazards.

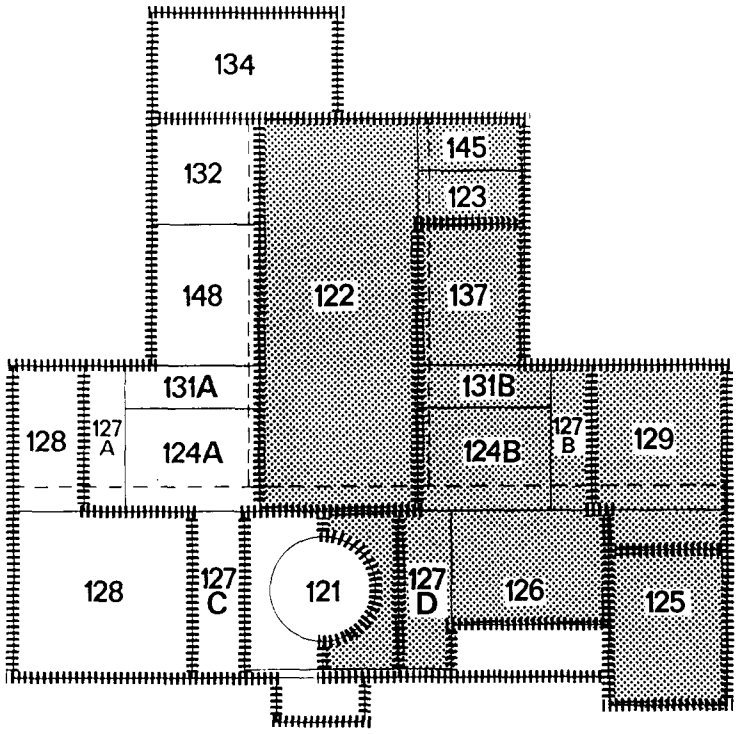
Extensive fire systems include the alarm system consisting of two independent parts, 60 separate ventilation systems for normal ventilation and 15 systems for smoke extraction, and numerous extinguishing systems.

In view of the general separation principles and the features of ventilation and fire extinguishing systems, it is highly improbable that the fire could affect more than one sub.

5.3.1.3 Seismic protection

Among the Swedish plants specific seismic requirements were only put on Forsmark 3 and Oskarshamn 3. The ground motion horizontal acceleration for Forsmark 3 was estimated as 0.15 g for the Safe Shutdown Earthquake (SSE). A seismic classification of buildings and structures of these two plants was made. As in the case of other safety related considerations, the basis was formed by American rules, regulations and guidelines. Figure 5.4 shows which buildings are subject to seismic design.

Verification and seismic qualification of equipment has been performed using engineering judgement, static analysis, dynamic analysis and testing.



121 Reactor building
122 Turbine building
123 Condensate cleanup system building
124 Auxiliary systems buildings A, B

125 Entrance building
126 Control building
127 Diesel buildings A, B, C, D
128 Waste building

129 Active workshop building
131 Auxiliary cooling water buildings A, B
132 High voltage switchgear building
134 Transformer building

137 Turbine cooling water systems building
145 Offgas building
148 Storage building

Boundary of fire zone
A/C side, designation A x
B/D side, designation B x

Figure 5.3
Fire zones

BWR 75 — BUILDINGS, SEISMIC DESIGN

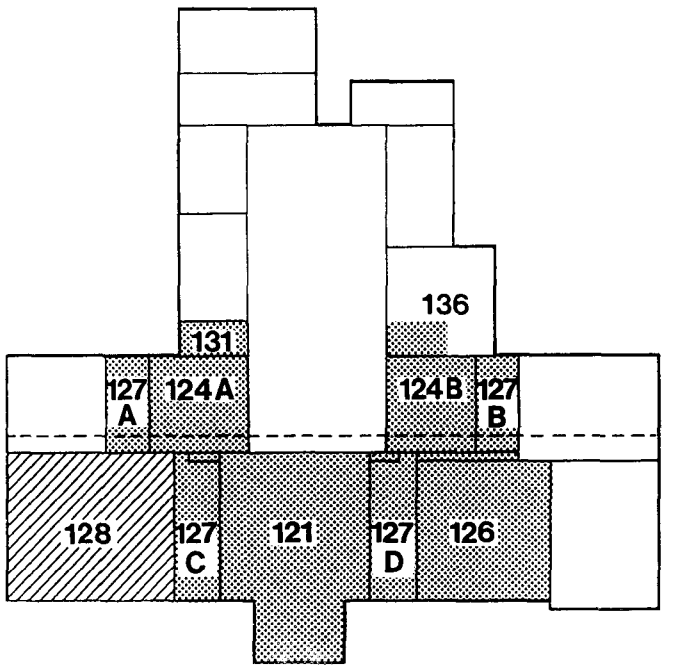


Figure 5.4

The following buildings are designed to assure safe shut-down of the reactor following an earthquake of specified magnitude:

121 Reactor building
124 Auxiliary systems buildings A,B
126 Control building
127 Diesel buildings A,B,C,D

131 Auxiliary cooling water building
136 Cooling water screening plant building
(128 Waste building*))

*) Only to the extent necessary to avoid release of stored radioactive material to the groundwater

The seismic input for all equipment are the floor response spectra obtained from the dynamic analysis of different building structures. The reactor with internals, the reactor building, containment and most process piping have been analysed dynamically. Static analysis has been used where it is obvious that a given component has its natural frequency above 33 Hz, which is outside the frequency range of the earthquake. Where the seismic design has not been possible to verify by analytical methods, testing has been performed. Engineering judgement has preferably been used to evaluate the risk that nonseismic equipment might jeopardize seismically classified equipment.

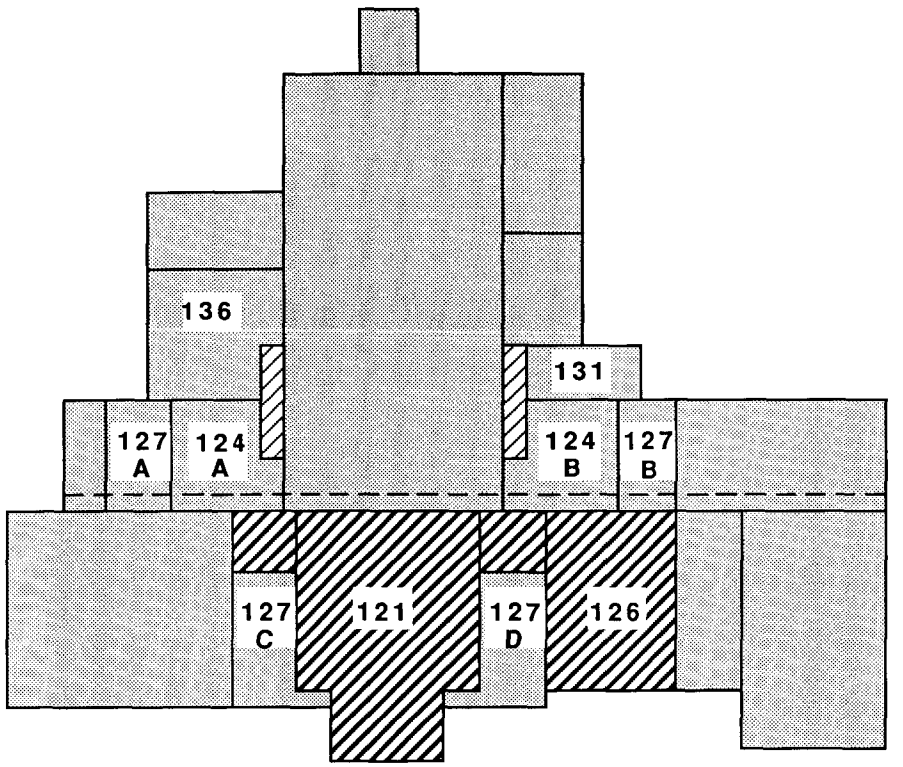
5.3.1.4 *Aircraft crash protection*

The need for protection of a nuclear power plant against an aircraft crash is related to the location of the plant. In the BWR 75 design basic protection is achieved by structure reinforcements and by locating redundant portions of safety related systems in building compounds which are separated in such a way that the aircraft cannot damage redundant parts (Figure 5.5). Special attention has to be given to the risks associated with the burning of huge amounts of aircraft fuel. The fire can affect emergency ventilation systems and may lead to the choking of redundant diesel generators, needed for emergency power. Thus, air intakes may need special protection. Further protection can be obtained by reinforcing certain walls and roofs to withstand specific impacts defined by aircraft speed, size and angle of approach.

The loading cases studied concern both impact of a fast military airplane and of a large commercial aircraft. The final verification of the ability to withstand such impacts is obtained by FEM calculations, using detailed models of the reinforced concrete structures. For protection against a large commercial aircraft the required thickness of the roof slab is of the order of two meters.

5.3.1.5 *Missiles protection*

Analyses of two types of missiles have been carried out for Forsmark 3 and Oskarshamn 3 plants: internally generated missiles associated with component overspeed failures and missiles that could originate from high-energy system ruptures.



121 Reactor building
124 Auxiliary systems buildings A,B
126 Control building
127 Diesel buildings A, B, C, D
131 Auxiliary cooling water building
136 Cooling water screening plant building

Figure 5.5
Aircraft crash protection

Examples of potential missiles are:

- break in a control rod drive
- bolts in main control rod drive
- bolts in the reactor pressure vessel flange
- overspeed missiles from the cooling system for the containment atmosphere.

In all cases analysed it has been shown that it is either impossible to generate a missile or that a generated missile cannot jeopardize the functions of safety systems.

A special consideration has been given to turbine missiles, which constitute the main missile hazard outside the containment. Due to extensive overspeed protection, the geometrical arrangements and existence of intermediate walls the risks are negligible. This applies also to a full break of the feedwater tank which could generate a missile (the tank gable).

Protection against pipe whips is provided by separation and/or by means of restraints or local shields for vital equipment. Consequently, secondary missiles generated from the whipping pipe are very unlikely. Consequences of jet impingement are minimized by separation which inside the containment is carried out by distance or by barriers. This makes it impossible or highly improbable for a missile to affect more than one sub.

In conclusion, the missile analyses carried out on a case-by-case basis ensure that the basic safety goals are not endangered by missiles. Overall integrity of buildings and structures housing safety-related equipment is maintained.

5.3.2 Probabilistic analyses of external events

Probabilistic external event analyses are presently being performed as supplementary studies to the existing Swedish level 1 PSAs for plants where inherent protection against such events is not as extensive as for BWR 75 design.

Those external events which are of primary interest having in mind the Swedish conditions are: fire, internal flooding, earthquake and aircraft crash. The approach to analysis of such events and results obtained will be presented in the following.

5.3.2.1 General considerations

Probabilistic analyses of the impact of external events on the safety of nuclear power plants are carried out by the utilities which are supported by the vendor and by consultants.

Frequently, the first analyses performed serve as pilot projects, i.e. the application is in some cases carried out in parallel with extensive methods development. The development may concern both the physical phenomena associated with the progression of a particular external event being analysed and the PSA-related modeling. Thus, the methods have frequently been tested directly step by step which provides feedback to the ongoing research work. This statement is particularly valid for seismic analyses. Due to such an ambitions approach the efforts spent on analyses of external events have been rather resource-intensive and have required long project time periods.

In all cases a computer-based, detailed plant model (event trees and fault trees) for internal events has already been available when external event analyses were to be initiated. These basic models were used to varying extent depending on the type of initiating event being analysed. In applicable cases the existing models were modified in order to account for event-specific impacts.

The primary purpose of the external events analysis as practiced in Sweden is to investigate their challenge to the plant safety and to identify possible weak points. Thus, in this context there is no ambition to provide an as realistic as possible assessment of the associated risks although the approach is to be based on credible assumptions. Consequently, due to the uncertainties involved the assumptions tend to be systematically conservative and high data values are used for screening purposes. The numerical values obtained as the end result of the described approach are frequently excessively pessimistic which should be kept in mind whenever comparisons with the PSA results for internal events are made. For that reason the results presented in this review will concentrate on qualitative findings.

Table 5.3 summarizes in qualitative terms the potential impact of different initiators on safety functions and on mitigating systems.

Some of the experiences of the Swedish State Power Board from PSA-based internal flooding and fire analyses have been reviewed in (Gunsell, 1986 and Gunsell et al., 1987).

5.3.2.2 Internal flooding analysis

Until now analyses have been carried out for the Ringhals 1 plant (BWR) both for water flooding (1983-84) and for steam spreading from systems carrying steam or hot water (1987), and for the Ringhals 2 (PWR) plant for water flooding (1987-88).

The following screening assumptions were used for water flooding analyses:

- Breaks or leaks with similar impact were treated as one group.
- All submerged equipment assumed failed.
- All submerged electrical equipment including junction boxes assumed to cause short-circuit.
- Reactor shutdown assumed even if no automatic signal is identified.
- No credit taken for manual repair of a leak.
- Different leak probabilities used for different components such as pipe sections, pumps, heat exchangers and bellows.
- Size of the leak is not the primary factor determining severity of the event.

For each group of events the pathways of water were identified and the corresponding water levels in each room were calculated.

The analysis of internal steam spreading has great similarities to the water flooding, eventhough the number of systems with a potential for steam release and also the number of possible pathways are much smaller. All leakages lead to automatic isolation of the leaking part (non-isolated leaks of primary coolant are covered by internal event analysis). Given the leak locations and pathways the temperature and moisture content were calulated in different rooms. These results were then compared with the conditions the

Table 5.3

Impact on safety and mitigating systems
Scheme for estimating the potential risk from different events

S = Strong
W = Weak

Initiating event	PSA level 1				level 2		level 3	
	Scram	Core cooling	Residual heat removal	Recovery	Containment integrity	Dedicated mitigating features (filtered venting etc)	Source term dispersion	Evacuation
Internal-transient	S	S	S	W	W	W	W	W
-LOCA	W	S	S	W	W	W	W	W
-vessel failure	S	S	S	S	S (BWR) W (PWR)	S	W	W
-LOCA outside containment	W	S	S	S	S	W	W	W
Flood, plant internal (water)	W	S	S	W	W	W	W	W
Flood, plant internal (water and steam)	W	S	S	W	W	W	W	W
Fire	W	S	S	S	W	(S)	W	W
Seismic	S	S	S	S	S	S	W	W (Sweden)
Aircraft	W	S	S	W	S	W	W	W
Wind	W	S	S	W	W	W	S	W (Sweden)
Snowfall	W	S	S	S	W	(S)	S	S
Lightning	W	S	S	W	W	W	S	W

equipment was originally designed to withstand. The failure probability for all electrical components along the pathway was assumed to be 0.1 although it was shown that the design criteria were slightly exceeded for a short time only.

The main result from the internal flooding analysis for Ringhals 1 was that the electrical dependencies between different systems in the plant were extensive and in several cases not acceptable. Thus, common circuit breakers would fail if anyone of the connected components is short circuited, causing also the other components' failure. In addition, some safety systems were connected to the same overcurrent protection switch as non-safety equipment (not qualified for accident environment) inside containment. Short-circuit in the non-safety equipment might disable several safety systems. Based on the results of these analyses modifications (separation) were introduced in the electrical systems at Ringhals 1 during the overhaul period 1985. This resulted in a reduction of the contribution of internal flooding to the core damage frequency by a factor of 30. It is worth noting the principles valid for overcurrent protection switches in the BWR 75 design (Forsmark 3, Oskarshamn 3):

- each switch is connected to equipment in only one system
- safety equipment and operational equipment in the same system are connected to different switches
- separate switches are used for equipment within and outside of containment.

The analysis of internal steam spreading at Ringhals 1 showed that its contribution to core damage frequency is low, i.e. given realistic assumption at least one order of magnitude smaller than that obtained for internal flooding.

The internal flooding analysis for Ringhals 2 showed that break in the salt water cooling system gives a large contribution. Automatical pump stop has been proposed given a large leak. In the case of internal steam spreading the available discharge openings and runoff ways have been judged as insufficient. Finally, openings between compartments which are supposed to be separated have been identified during the walk-through analyses.

Based on the experiences from internal flooding studies we conclude that available analysis techniques are adequate and efficient.

5.3.2.3 Fire analysis

Although fire analysis shows similarities with flooding analysis with respect to the principles of approach, the methodology for fire analysis is more complex and demanding since use of advanced simulation tools might be needed.

Three computer codes for simulation of compartment fires (BRAND, COMPBRN, DSLAY1), all using a two-zone model, are available in Sweden. BRAND was developed by ABB Atom, COMPBRN by UCLA and DSLAY1 by the Swedish National Defence Research Institute. Typical information generated by these codes comprises temperatures and heat fluxes during a fire. Thus, basis is provided for estimation of failure times of objects (e.g. cables) and for indicating the potential for flashover in the compartment. The results are subject to rather large uncertainties. Recently, the features of the codes have been compared and evaluated (Hallberg et al., 1986) with main emphasis on the needs specified by the fire risk analyses which were in progress at that time. Although all the codes mentioned above use the relatively simple two-zone model, there are still significant differences in the modeling details, capacities of the programs, and in assumptions made. Several case studies have been performed, independently as well as in form of benchmark-type analyses for oil fire, vertical cable tray fire and horisontal cable tray fire. Figure 5.6 shows an example of comparative oil fire simulations.

Until now the simulation codes have been used as a supporting tool for decisions concerning the predicted fire growth and propagation. In this way also assumptions used in the screening process are supported. Some of the central conclusions are as follows:

1) In case of flashover fire propagation to adjacent rooms is likely through openings (if present), or through enclosing boundaries (if the critical surface temperature is exceeded). Flashover is assumed to be possible when the mean temperature in the hot gas layer exceeds 300°C. This may happen if 25-35 l oil is available for combustion.

2) If no venting is present the fire is likely to be limited when availability of oxygen becomes low. The same applies also to cable compartments with normal ventilation (less than three air-exchanges per hour). Furthermore, given lack of oxygen the flashover and fire propagation to adjacent rooms are not likely. However, the smoke layer may ignite violently if air is supplied, e.g. by opening a door.

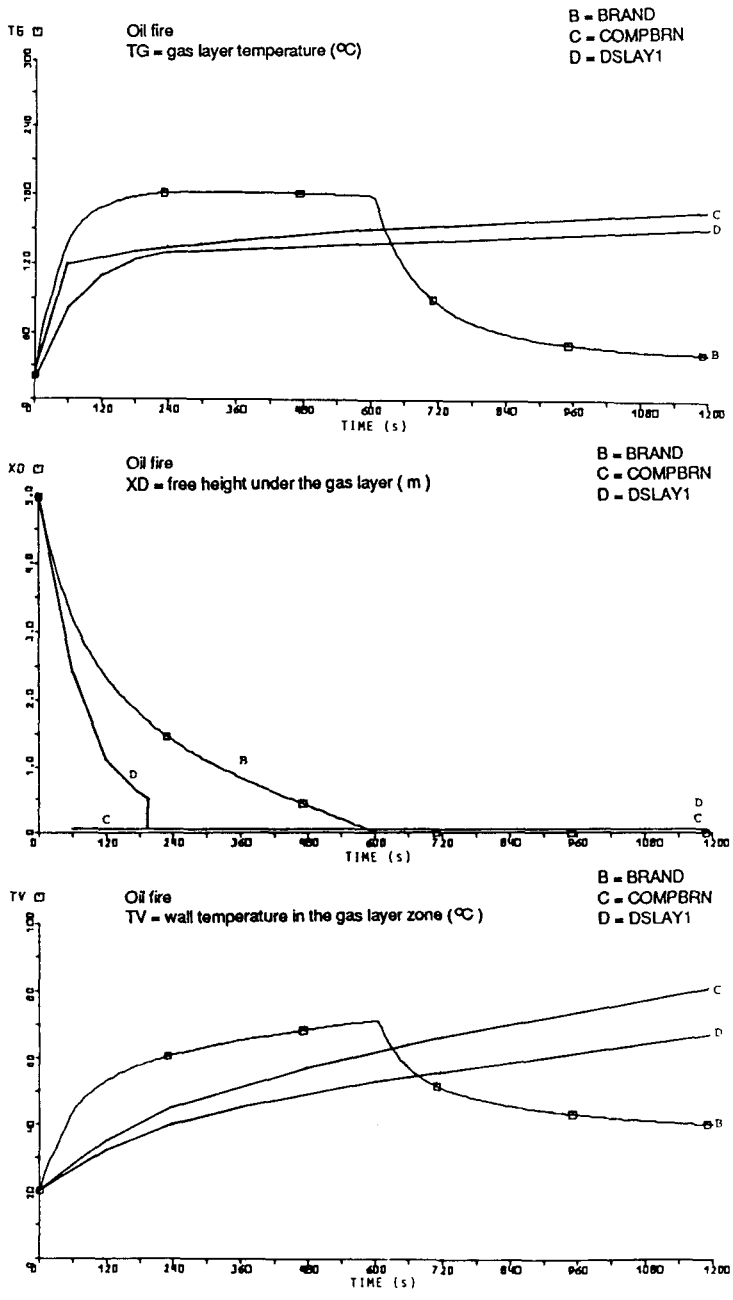


Figure 5.6

Comparative oil fire simulations

3) The rates of smoke filling and temperature increase depend in the first hand on the heat generation in the fuel bed and on the size of the compartment. It may take less than 5 minutes for oil or vertical cable fires, and about 10 minutes for horisontal cable fires, before the compartment is filled with smoke. In a room with a floor area of 100 m^2 and 5 m height, the combustion of 10 kg oil may give a temperature of about 200°C within 5 minutes. Given a low ventilation rate the combustion and maximum temperature will soon be governed by the access of oxygen. The smoke that leaves the room will not be capable to cause a secondary fire in other rooms.

Some typical assumptions made frequently in the Swedish probabilistic fire analyses are:

- All equipment in the affected compartment is assumed to fail. More realistic failure probabilities could be generated by taking into consideration such factors as: oxygen consumption, location of object of interest, heat generation in the fuel bed, etc.

- Fire fighting systems are either not credited (Barsebäck) or only automatic fire fighting systems are credited (Ringhals). No credit is taken for manual actions which is motivated by the fact that the time to reach high temperatures is short.

- Fire is assumed to contribute negligibly to the probability of reactor shutdown failure.

- Accident sequences with frequencies lower than 10^{-8} per year are not analysed.

- Only electrical equipment is assumed to be affected by the fire while passive components (e.g. check valves, safety valves) are not affected.

- Operator failure probability has been increased as compared to internal initiators. This is motivated by the possibility that the process information may be distorted in case of fire.

At this point fire analyses have been carried out for Barsebäck 1 by Sydkraft (1986-89) and for Ringhals 1 (1986-89) and Ringhals 2 (1987-88) by the Swedish State Power Board. The Barsebäck analysis was divided into two phases. In the second phase also failure of signal cables has been taken into account, while the first phase was limited to components which fail directly or are affected by failure of electrical power supply/other support systems. OKG presently performs fire analysis for Oskarshamn 2 and a corresponding study for Oskarshamn 1 will be initiated in the autumn of this year.

In all cases the available computer-based plant models from PSAs for internal events are used as a basis. The models were modified with respect to failure

probabilities of affected components, but as a rule no new components had to be added. This is a consequence of using detailed fault tree models. Since the number of affected components usually is large the efficient handling of the fault tree models by use of dedicated computer codes is a critical factor. A useful feature of the SUPER-TREE code (Hirschberg and Knochenhauer, 1989), developed by ABB Atom and used by the Swedish State Power Board, is the ability of the program to temporarily modify the fault trees in order to adapt to specific analysis needs (e.g. analysis of fire or flooding). This is done by assigning attributes to gates and basic events.

Thorough walk-through analyses have been made in order to assign fire frequencies to fire cells of interest. After primary screening typically 100 compartments are of interest with respect to fire initiation. The frequencies used are typically between 10^{-2} and 10^{-4} per year and are based on the availability of combustible material, ignition probabilities, personnel trafic through the compartments etc. Totally 13 fires have been registered at Swedish plants during 58 reactor years. This leads to an average fire frequency of 0.2 per reactor and year.

For Ringhals 1 few weak points were identified. Flooding analysis which preceded fire analysis led to identification of most presumptive problems. However, more disciplined approach was introduced at the plant with respect to allowed temporary presence of combustible materials.

For Ringhals 2 the analysis performed resulted in significant modifications concerning physical separation of charging pumps and embaking of the floor under RCP in the containment to limit the spread of oil leakage. The changes were motivated by unacceptably high contributions to the core damage frequency.

For Barsebäck 1 there are 17 fire cells which contribute more than 10^{-8} per year to the core damage freguency; four of them contribute 95 % of the total core damage frequency caused by fires. Some improvements of fire protection were introduced after the first phase. The results of the second phase will be subject to modifications including taking credit for fire fighting systems. Presently further improvements are discussed (separation, protection of critical cables).

Preliminary results of fire analysis for Oskarshamn 2 indicate that contributions from the fire hazard are significant, especially for the signal cables.

Generally, use of more flexible simulation codes for fire propagation would be desirable for handling of multiple rooms or oddly shaped compartments. Application of advanced codes (e.g. Harward family of models) could be of interest in this context. Relaxation of the conservative assumptions concerning impact of fires on components, and crediting for fire fighting systems would lead to more balanced results.

5.3.2.4 Seismic Analysis

In the area of seismic analysis there are only few studies available for the Swedish plants. Geological conditions are quite stable in Sweden. For this reason, no specific seismic requirements were formulated in connection with the erection of the first nuclear plants. While only Forsmark 3 and Oskarshamn 3 have been designed for a safe shutdown earthquake (SSE) of 0.15 g with the U.S. NRC Regulatory Guide 1.60 ground response spectrum, mitigating systems (i.e. filtered venting and an independent containment spray system) recently installed at all plants, are all designed to meet this criterion.

In 1986 the Swedish Nuclear Power Inspectorate and the three utilities initiated a major project SEISMIC SAFETY, aiming at an in-depth seismic risk assessment for the nuclear power plants in Sweden. This covers definition of the seismic hazard and reflection of the unique seismological features of Sweden. Results obtained until now have been reported and presented (Engelbrektson, 1989). The methodology used, though it contains established elements, is partly novel.

Evaluation of the seismic hazard has been based on data from observed earthquakes in northern Europe since 11th century (977 earthquakes) and from observations in southern Sweden and in Denmark after 1375 (733 earthquakes). According to the findings, the "Swedish" design earthquake is less demanding than that of U.S. NRC Regulatory Guide 1.60. Thus, the duration is expected to be significantly shorter (5-7 seconds compared to about 20 seconds) and the design response spectrum is lower at frequencies

below 10 Hz and slightly higher at higher frequencies. Naturally, this will have impact on the floor response spectra which now are being generated for some plants, using the new findings.

The analyses performed earlier, i.e. a prestudy for Ringhals 1 (1984-85) and first phase of the analysis for Oskarshamn 1 (1987-89) use the U.S. NRC Regulatory Guide 1.60 spectrum. Presently, comprehensive analyses are in progress for Ringhals 1 and Ringhals 2.

In Ringhals analyses the PSA models have been mainly used to define the minimal system/component requirements. In the prestudy for Ringhals 1 fragility curves based on walk-through analyses and on some structural calculations have been used. The main core damage scenarios which have been identified are: lift-off of the reactor pressure vessel, failure of reactor shutdown due to bending of control rod drives and instability of the central part of the containment. The results were regarded as unacceptable and continued in-depth analyses were recommended.

The recommendations from the prestudy are now being followed-up in the ongoing Ringhals 1 analysis carried out by the Swedish State Power Board in cooperation with ABB Atom. The methodological approach with respect to use of fragilities has not been finally defined. A pilot study has been performed for one of the reactor water makeup systems. The approach chosen combines walk-through analysis with review of the component drawings supplemented by simple calculations (whenever needed). For walk-through analysis check-lists were developed. For pipes calculations are performed concerning their capacity given static and dynamic loads. Given the results of walk-through analysis, components are compared with reference components of the Forsmark 3 plant designed to meet seismic standards. The obtained results are promising. In addition, serious weaknesses of electrical equipment (with respect to components as such and their installation) were identified as a result of walk-through analysis of electrical systems. Finally, preliminary results obtained using floor response spectra based on the "Swedish" design earthquake show a much more favourable picture for the reactor building and for the containment in comparison with results of the prestudy, while the loads for the electrical system building are by and large the same.

A somewhat different approach has been chosen by EQE in the pilot study for Oskarshamn 1 (Landelius et al., 1989). The analysis has been focused on estimation of the seismic margin of the new mitigation systems. Some of the components of these systems interface with the existing systems in Oskarshamn 1, not designed to meet the seismic criteria. The different stages of seismic margin assessment (walk-through, screening, seismic margin calculations) have been carried out. The margin assessment is based on the earthquake experience data and the results and insights obtained in the performance of seismic PSAs. Pilot application concerns containment spray system which has been shown to have a satisfactory seismic capacity provided the seismic adequacy of anchorage of the heat exchangers' framing is further verified. Some other systems i.e. reactor scram system and the battery-backed net need to be assessed for seismic margin to verify the seismic adequacy of certain components. Dynamic structural analyses performed by ABV show that the reactor building has high seismic capacity, while some weak points have been identified in the containment.

5.3.2.5 Aircraft crash analysis

The available analyses concern Ringhals and Forsmark plants. In spite of conservative assumptions the combination of estimated accident density and the critical hit area leads to low probabilities of hit (frequency of the order of 10^{-7} per reactor and year). Consequently, further analyses are not motivated.

5.3.3 Conclusions

A systematic program aiming at supplementing the existing Swedish PSAs for internal events with studies of external events is presently being carried out. The focus is on early plant generations since the latest Swedish BWR plants have design features which include inherent defensive measures against external events.

The probabilistic analyses focus on internal flooding, fire and seismic hazard. Other external hazards are not of primary concern for the Swedish conditions. The approach being used concentrates on identification of potential weak points while the numerical precision is of secondary

importance. Due to large uncertainties involved this approach has usually a conservative bias. However, whenever unacceptable results (from the point of view of safety level) are obtained and might be attributed to the analysis simplifications, in-depth studies are performed based on refined methods. Generally, the models (event trees, fault trees) of the available PSAs for internal events are used as a starting point for the analyses of external events. Rationalization of work has been possible due to extensive use of comupter tools for handling of large fault trees.

Flooding analysis is sufficiently mature and no principal difficulties exist. In case of fire analysis there is a need of analytical support in form of reliable codes for simulation of fire propagation in order to enable more realistic approach and to model fire growth in complex geometries. Seismic analyses are most resource-intensive. The new developments concerning "Swedish" seismic design spectra are presently being implemented in plant-specific studies and different methodological approaches are tried.

The analyses performed have been successful in identification of weak points at the plants and several modifications recommended by the studies have been implemented. In a number of cases the hereby achieved safety improvements are significant.

5.4 References

Akersten, P.E. (1986)
The Bivariate TTT-Plot - A Tool for the Study of Non-constant Failure Intensities. Scandinavian Reliability Engineers Symposium, Finland, October 14-16, 1986.

Bento, J.-P., Björe, S., Ericsson, G., Hasler, A., Lydén, C.-O., Wallin, L., Pörn, K., Åkerlund, O. (1985)
Reliability Data Book for Components in Swedish Nuclear Power Plants. Report RKS 85-25, prepared by ABB Atom AB and Studsvik Energiteknik AB for Nuclear Safety Board of the Swedish Utilities and Swedish Nuclear Power Inspectorate, May 1985.

Birnbaum, Z.B. and Saunders, S.C. (1969)
A New Family of Life Distributions. Journal of Applied Probability, 6(2), pp. 319-327, 1969.

Bogdanoff, J.L.G. and Kozin, F. (1985)
Probabilistic Models for Cumulative Damage. John Wiley & Sons, New York, 1985.

Cox, D.R. (1962)
Renewal Theory. John Wiley & Sons, New York. 1962.

Ditlevsen, O. (1986)
Random Fatigue Crack Growth - a First Passage Problem. Engineering Fracture Mechanisms, 23, pp. 467-477, 1986.

Engelbrektson, A. (1989)
Characterization of Seismic Ground Motions for Probabilistic Safety Analyses of Nuclear Facilities in Sweden. 10th International Conference on Structural Mechanics in Reactor Technology, Anaheim, California, U.S.A., August 14-18, 1989.

Fussel, J.B., Johnson, M.P., Campbell, D.J. and Montague, D.F. (1981)
Phased-Mission Systems Reliability Analysis. Volume 1: Methodology. Report NP-1945, Electric Power Research Institute, 1981.

Gunsell, L. (1986)
Analysis of External Events in Nuclear Power Plants. Scandinavian Reliability Enginereers Symposium, Otaniemi, Finland, October 14-16, 1986.

Gunsell, L., Nirmark, J. and Resare, M. (1987)
Fault-tree Modelling and Failure Probabilities in External Event Analysis. PSA '87 - International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Hallberg, T., Hirschberg, S., Pedersén, M., Tannenberg, D. and Akerlund, O. (1986)
Fire Risk Analysis: Status of Computer Codes for Simulation of Compartment Fires. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.

Harris, D.O., Lim, E.Y., Dedhia, D.D., Woo, H.H. and Chou, C.K. (1982)
Fracture Mechanics Models Developed for Piping Reliability Assessment in Light Water Reactors. Piping Reliability Project. Report NUREG/CR-2301, U.S. Nuclear Regulatory Commission, 1982.

Harris D.O., Dedhia, D.O., Eason, E.D. and Patterson, S.D. (1986)
Probability of Failure in BWR Reactor Coolant Piping. Report NUREG/CR-4792, U.S. Nuclear Regulatory Commission, 1986.

Hirschberg, S. , ed. (1987)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report RAS-470(86)14 (ABB Atom Report RPA 86-241), June 1987.

Hirschberg, S. and Gunsell, L. (1989)
Defensive Measures Against External Events and Status of External Event Analysis in Swedish Probabilistic Safety Assessments for Nuclear Power Plants. Second International Post-SMIRT 10 Seminar "Probabilistic Risk Assessment (PRA) of Nuclear Power Plants for External Events", Irvine, California, U.S.A., August 21-22, 1989.

Hirschberg, S. and Knochenhauer, M. (1989)
SUPER-NET, A Multi-purpose Tool for Reliability and Risk Assessment. International Post-SMIRT 10 Seminar "The Role and Use of PCs in Probabilistic Safety Assessment and Decision Making", Beverly Hills, California, U.S.A., August 21-22, 1989.

Hirschberg, S. and Tirén, I. (1989)
Design-related Defensive Measures Against Dependent Failures. ABB Atom's Approach. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-20, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 71-100.

Holmberg, J., Silvennoinen, P. and Vira, J. (1989)
Application of the Dempster-Shafer Theory of Evidence for Accident Probability Estimates. Reliability Engineering and System Safety, 26, pp. 47-58, 1989.

Huovinen, T. (1989)
Estimation of Some Stochastic Models Used in Reliability Engineering. VTT Research Report 598, April 1989.

Karlsson, C. and Knochenhauer, M. (1987)
Mapping of the Influence of Periodical Testing and Preventive Maintenance on the Auxiliary Feedwater System in Forsmark 1 and 2 (in Swedish). Report RAS-450(87)5. (ABB Atom Report RPC 87-45), June 1986.

Keller, A.Z. (1984)
A Generalised Theory of the Nonhomogeneous Poisson Process. 8th Advances in Reliability Technology Symposium, University of Bradford, England, April 25-27, 1984.

Kozin, F., Bogdanoff, J.L. (1987)
Probabilistic Methods of Fatigue Crack Growth: Results and Speculations. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Laakso, K., Knochenhauer, M., Mankamo, T. and Pörn, K. (1990)
NKA/RAS-450 Final Report: Optimization of Technical Specifications Using Probabilistic Methods - A Nordic Perspective, to be published 1990.

Landelius, M., Ravindra, M.K., Hardy, G.S. and Hasimoto, P.S. (1989)
Seismic Margin Review of Mitigation Systems in Oskarshamn. 10th International Conference on Structural Mechanics in Reactor Technology, Anaheim, California, U.S.A., August 14-18, 1989.

Lehtinen, E., Pulkkinen, U. and Kuhakoski, K. (1988)
Methods for Combining Plant Specific Operating Experience Data with Data from Other Nuclear Power Plants in PRA/PSA studies. Technical Committee Meeting on Evaluation of Reliability Data Sources, International Atomic Energy Agency, Vienna, Austria, 1988.

Lu, S., Streit, R.D. and Chou, C.K. (1981)
Probability of Pipe Fracture in the Primary Coolant Loop of a PWR Plant. Report NUREG/CR-2189, vol. 1-9, U.S. Nuclear Regulatory Commission, 1981.

Mankamo, T. (1986)
Phased Mission Reliability - A New Approach Based on Event Sequence Modelling. Scandinavian Reliability Engineering Symposium, Otaniemi, Finland, October 14-16, 1986.

Moelling, D. S. and Gallucci, R.H.V. (1985)
Markovian Probabilistic Fracture Mechanics Analysis Applied to Estimating Failure Probabilities of a PWR Primary Coolant Pipe. International Conference on Nuclear Power Plant Ageing, Availability Factor and Reliability Analysis, San Diego, California, U.S.A., July 8-12, 1985.

Mosleh, A. and Siu, N.O. (1987)
On the Use of Uncertain Data in Common Cause Failure Analysis. PSA '87 - International SNS/ENS/ANS Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Newby, M. (1987)
Comments on Fatigue Crack Growth Models. Reliability Engineering, 18, pp. 57-60, 1987.

Paris, P.C. and Erdogan, F. (1963)
A Critical Analysis of Crack Propagation Laws. Journal of Basic Engineering, Ser. D, 85(4), 528(1963).

Pörn, K. (1989)
On Empirical Bayesian Inference Applied to Poisson Probability Models. Draft Report Studsvik/NP-89/7, 1989.

Pulkkinen, U. (1989)
Bayesian Uncertainty Analyses of Probabilistic Risk Models. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2 - 7, 1989.

Pulkkinen, U., Huovinen, T. and Kuhakoski, K. (1987)
Combination of Several Data Sources. PSA '87 - International SNS/ENS/ANS Topical Conference on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

Rau, J. G. (1970)
Optimization and Probability in Systems Engineering. Van Nostrand Reinhold Company, New York, 1970.

Shafer, G. (1976)
A Mathematical Theory of Evidence. Princeton, Princeton University Press, 1976.

Simola, K., Pulkkinen, U. and Huovinen, T. (1988)
Treatment of Time Dependent Phenomena in PSA. Report RAS-470 (87) 15 (VTT Report SÄH 13/88), October 1988.

Singpurwalla, N.D. (1986)
A Unifying Perspective on Statistical Modeling. GWU/IRRA/Serial TR-86/4, The George Washington University, School of Engineering and Applied Science, Institute for Reliability and Risk Analysis (1986).

Snyder, D.L. (1975)
Random Point Processes. John Wiley & Sons, New York, 1975.

Sobczyk, K. (1986)
Modeling of Random Fatigue Crack Growth. Engineering Fracture Mechanics, 24, pp. 609-623, 1986.

U.S. Nuclear Regulatory Commission (1983)
PRA Procedures Guide. Report NUREG/CR-2300, January 1983.

U.S. Nuclear Regulatory Commission (1989)
Reactor Risk Reference Document. Report NUREG-1150, June 1989.

Vaurio, J.K. (1986)
Applications of a New Reliability Growth Model that Fits Data. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.

Vaurio, J.K. and Lindén, G. (1986)
On Robust Methods for Failure Rate Estimation. Reliability Engineering, 14, pp. 123-132, 1986.

6. SUMMARY OF INSIGHTS, CONCLUSIONS AND RECOMMENDATIONS

In the NKA/RAS-470 project three problem areas encountered in PSA-work, have been in focus, i.e.:

- dependencies with special emphasis on common cause failures
- human interactions
- uncertainty aspects.

In the following the main insights, conclusions and recommendations regarding the three main problem areas are summarized. With respect to the findings of this project, concerning some additional specific topics which have been addressed (time-dependent phenomena, combination of data sources, treatment of external events), we refer to the conclusions given in respective sections of chapter 5.

The main emphasis in this summary is on findings originating from Nordic experiences and on insights most relevant for applications in the Nordic countries.

6.1 Dependencies

6.1.1 Treatment of explicitly modeled dependencies

It has been demonstrated that treatment of dependencies may be considered as a strong part of the Nordic PSAs. Characteristically, most of the findings in form of identified plant deficiencies involve unintended dependencies. In several cases the insights have led to introduction of modifications at the plants and, consequently, to significant safety improvements.

The identified dependency-related deficiencies belong to one of the following categories: functional dependencies, shared-equipment dependencies and equipment-related Common Cause Initiators (CCIs). In some cases completeness in the treatment of these types of dependencies may be questioned and, in addition, not all discrepancies between the analyses can be explained by design differences. In fact they originate from different perception of the design, different assumptions, errors in the analyses, or

differences in scope, degree of detail and level of ambition. However, from the methodological point of view treatment of these three categories of dependencies does not represent a major modeling problem. The approach used in Nordic countries is based on consequent application of the small event tree/large fault tree techniques, which takes care of functional and shared-equipment dependencies in a rather mechanistic way. Possible problems (given high degree of detail) may originate from computerized Boolean reductions or/and from manual reductions of large logical models. Potential for such errors has been significantly reduced in view of progress made with respect to capacity of computer codes for fault tree analysis. From the point of view of quality assurance (which involves assurance of reasonable completeness) use of efficient computer codes for fault tree handling, as practised in Nordic countries, is also essential.

Three types of CCIs are possible: external events, internal events causing severe environmental stresses and internal (equipment-related) initiators which may involve functional dependencies not covered by the "generic" transient categories. The first mentioned two types of CCIs are not included in the current Swedish and Finnish base studies, although several analyses concerning e.g. internal flooding, fire, earthquake and air crash have been performed or are in progress for some plants. In this context the four-divisional separation constitutes an effective defensive measure against most low probability events with great damage potential. Modeling of external events requires special techniques; a separate review covers status, methodology and insights from Swedish probabilistic studies of external events (see section 5.3 of this report). Associated uncertainties are usually very large, particularly in the case of seismic analysis which constitutes the most serious modeling challenge. It should be emphasized that loss of offsite power, sometimes regarded as an external CCI, is a transient covered by the conventional event tree/fault tree approach.

With respect to equipment-related internal initiators a thorough well documented plant-specific study of support and control systems which may affect both normally operated systems as well as standby safety systems, is motivated. Examples of such systems include reactor water level measurement, electric power supply, pressurized gas systems and secondary cooling systems. Study of equipment-related CCIs is rather straight-forward but time

consuming. It ensures the completeness of a PSA, although in some cases a certain overlapping with the standard type of event tree/fault tree approach cannot be excluded.

Apparently, treatment of functional and shared-equipment dependencies, and equipment-related CCIs does not represent a serious modeling problem, given a consequent approach. Practical limitations naturally exist in this context but with time consistency and completeness of the present PSAs will certainly improve. Findings of the Swedish SUPER-ASAR project (Carlsson et al., 1987 and Carlsson et al., 1988), constitute an important step towards this goal.

More serious modeling problems are usually encountered in the case of physical interactions, human interaction dependencies and residual common cause failures.

Generally, the failures which may be induced by the normal operational environment are part of the conventional analysis. This is due to the fact that:

1) The equipment is assumed to be qualified for such environment.

2) The failure rates used are based on operational experience and are assumed to reflect the actual operational environment.

3) Support functions such as component cooling are covered by the fault tree model and constitute a part of functional or shared-equipment dependencies.

4) Residual common cause failure contributions to some extent include intercomponent physical interaction dependencies not covered by the other approaches.

A documented, systematic and comprehensive study of physical interactions not covered by the points above should be a part of any PSA. This may involve dedicated qualitative or/and quantitative analyses of phenomena of special interest. In some cases physical interactions lead to requirements on operator actions which may be quite demanding. A typical example is back-flush operation identified as an important function for the early generations of ABB Atom's BWRs. Successful mitigation of large and medium LOCAs requires that the emergency core cooling suction pathways are maintained

free from debris. Failure to initiate or failure to correctly carry out back-flush operation will lead to loss of core cooling and ultimately to core damage, unless timely recovery actions are taken.

Think-through and walk-through analyses are helpful tools for identification of potentially significant physical interactions. A systematic procedure for structured integration of engineering judgement in such analyses has been developed in one of the Swedish PSAs (Ericsson and Hirschberg, 1984). This facilitates to examine impact of some environmental factors (grit, humidity, corrosion and other chemical reactions, vibration, temperature and thermal stress, radiation) and gives a rough and quick overview of facility-related events causing severe environmental stresses (fire, energy release through explosion, water hammer, structural failure, flow blockage, leakage, electrical interference; some of these phenomena may belong to CCI-category). The procedure is most efficient for plants with relatively low degree of separation and with substantial operating experience.

Of particular interest are analyses of dynamic effects such as: pipe whips, jets, secondary missiles and pool-dynamic loads, which may follow upon a pipe break within the reactor containment. Studies assessing unavailability contributions from dynamic effects for systems mitigating the consequences of internal pipe breaks are essential, but frequently lacking. In one of the Swedish PSAs dynamic effects contribute significantly to unavailability of pressure relief, emergency core cooling and auxiliary feedwater system, given large or medium LOCA. Analysis of dynamic effects is a relatively complex task which may be facilitated by introduction of "rules of thumb" based on engineering judgement.

Four types of human interactions with some potential for dependencies have been treated in most of the Swedish PSAs:

1) Maintenance and test outages that may increase system unavailability.

2) Manual actuation signals to systems and equipment in case of failure of automatic signals, and local manual actuation of equipment.

3) Manual initiation of safety systems, involving decision and e.g. proper alignment of valves.

4) Misconfiguration of components in redundant trains.

Some simple rules may be applied when modeling human interaction dependencies. Thus, test and maintenance activities should be represented in the fault trees. Simultaneous multiple failures due to maintenance outages may be analysed by means of maintenance matrices. Such matrices are developed for all safety systems to determine the likelihood of more than one train being maintained simultaneously. Manual actuation of redundant components in different trains is treated as a common event. The essential operator actions are modeled either in the event trees or in the fault trees. Operator actions considered as critical for propagation of accident sequences, i.e. operator actions which have impact on functional intersystem dependencies, are explicitly represented in event trees. Naturally, failure to observe an indication or to diagnose correctly the nature of the event, is equivalent to no responses being carried out. Systematic misconfiguration of redundant components and systematic calibration errors may be modeled explicitly or the corresponding unavailability contributions may be covered by separate CCF-contributions. Assumed independency between human interactions concerning redundant trains should at least be supported by qualitative arguments (e.g. staggered testing of different subs, automatic restoration of components to original position after test, favourable conditions for recovery) and/or by situation-specific analyses.

Difficulties encountered in treatment of errors of commission, which obviously may introduce complex dependencies, call for further research. Confusion matrix approach has recently been applied in this context in one of the Finnish PSAs (Vuorio and Vaurio, 1987).

6.1.2 Treatment of common cause failures

Identification

The Nordic CCF-data Benchmark Exercise concerning motor-operated valves (Hirschberg, ed., 1987) has demonstrated that basic CCF-identification can be reasonably performed based on failure reports from the Scandinavian Nuclear Power Reliability Data System and on the Swedish Licensee Event Reports (LERs). The methods used for CCF-identification are straightforward and require as a minimum information failure decriptions containing failure mode, criticality and time of detection. However, availability of much

more detailed background material including data on type of valve, physical location, manufacturers, maintenance policies etc, would decrease the impact of subjective judgement. Use of computers to aid in searching, sorting and generally reorganizing failure reports has been recommended.

The results of identification are directly dependent on intended scope (e.g. limitation to intrasystem CCFs), on choice of main identification factors (e.g. length of critical time period) and on assumed bounding conditions (e.g. definition and treatment of non-critical failures). Some desirable information is not available when the original failure reports are written; failure cause specification - if it is ever available - is often delayed. The uncertainty concerning the quality of reports originating from the overhaul period is a serious drawback; any improvement of these reports would be most welcome. In addition, when carrying out the screening procedures attention should be given to the types of tests carried out during normal operation and during overhaul, and their capacity of revealing critical failures. Treatment of multiple failure events detected during the overhaul period proved to be one of the most controversial and unresolved issues in the Benchmark Exercise.

Merits of classification systems as a supporting tool for CCF-identification (see e.g. Mosleh et al., 1988) depend on the structure of failure reports. The Swedish and Finnish failure reporting systems concern only components and supply in the first place information about failure modes. The use of classification systems which are cause-oriented is, consequently, of limited value in this case.

Quantification methods, data and uncertainties

Nordic CCF-data Benchmark Exercise (Hirschberg, ed., 1987) focused on impact of different assumptions involved in data treatment on the estimated CCF-contributions. Of primary interest in this context are such factors as: CCF-definition, use of application- and design-oriented screening, use of extension schemes and weighting of potential CCFs. With few exceptions most of the discrepancies in the estimates of CCF-contributions could be attributed to these factors rather than to the choice of a particular estimation method. These findings are consistent with the results of a parallel CCF Reliability Benchmark Exercise coordinated by Ispra Establishment (Poucet et al., 1987).

Based on the results of Benchmark Exercises the recommended approach to quantification, in applications where in-depth studies of raw data are possible, would employ direct assessment of CCF-contributions. Use of simple parametric methods is still of major interest when good quality single failure probability data (e.g. Swedish Reliability Data Book, Bento et al., 1985), are available. Parametric models are also suitable for checking the impact of modified assumptions and for performance of sensitivity studies, and may represent the only practically available option when the data are lacking or are scarce. As a follow-up to the Nordic CCF-data Benchmark Exercise a survey of various CCF-quantification models has been made, including relations between the parameters (Pörn, 1989).

The impact on PSA-results of different approaches to quantification of CCF-contributions has been studied by means of comprehensive sensitivity analyses (Hirschberg et al., 1989a) and uncertainty analyses (Hirschberg et al., 1989b,c). The sensitivity studies concern both data and methodological aspects. Examples of issues addressed involve: impact of lower failure multiplicities, generation of plant-specific CCF-parameters for motor-operated valves using identical assumptions concerning treatment of CCF-data, use of alternative approaches to mapping up and mapping down of impact vectors, comparison of Multiple Greek Letter (MGL) method (Fleming and Kalinowski, 1983) and alpha-factor method (Mosleh and Siu, 1987), systematic misconfigurations of redundant components, impact of practical arrangements of tests of redundant components and of policy applied with respect to identification of CCF-events by testing on the choice of suitable CCF-model, CCF-contributions in systems with ultra high level of redundancy, impact of defensive measures on estimation of CCF-parameters and importance of "state-of-knowledge" dependencies. Below follow some important insights from these studies. It should be noted that the conclusions drawn for Swedish PSAs are not necessarily generally valid.

1) Given a reasonable choice of higher order CCF-parameters the contributions to core damage frequency from lower failure multiplicities are small for plants with high level of redundancy. Use of models which properly take into account all relevant failure multiplicities is, however, recommended.

2) Use of a consistent approach to quantification of CCF-contributions in different PSAs has a strong impact on the results; in one of the analysed cases the total core damage frequency increased by 78 % when the new plant-specific CCF-parameters for motor-operated valves were applied.

The results are also sensitive to the choice of schemes for mapping up and mapping down of impact vectors (difference of 21 % in the above mentioned case).

3) The alpha-factor method (Mosleh and Siu, 1987) provides a more correct representation of statistical uncertainties than the MGL-model (Fleming and Kalinowski, 1983). In one of the analysed cases the MGL-based estimates of the mean and of the 90 % confidence bound for probability of quadruple failure of a set of redundant valves, represent an underestimation by a factor of 3.

4) Application of Multiple-Sequential Failure (MSF) model (Samanta et al., 1985) shows that the impact of postulated systematic misconfiguration of redundant components is small in case of the latest generation of Swedish BWRs. For elder plants the impact is more pronounced and becomes quite substantial for dependency factors of the order of 0.1.

5) The practical arrangement of tests of redundant components and policy applied with respect to identification of CCF-events by testing has impact on the choice of suitable CCF-model (Parry, 1984). Use of MGL- and alpha-factor methods is consistent with the origin of Swedish CCF-data, i.e. the presently available Swedish CCF-experience originates almost exclusively from plants where redundant components are tested simultaneously.

6) Presently available methods and data are not adequate for proper modeling of CCF-contributions in systems with ultra high level of redundancy. Of primary interest for ABB Atom's BWRs are pressure relief valves (e.g. 13-out-of-16 failure criterion), control rods, fine motion-drives, scram modules and frequency converters. Incorrect extrapolations of simple parametric methods to such redundancies have been observed in several cases. Application of an extended Common Load (CL) model (Mankamo, 1988) has been recently proposed as a solution to this problem. The model is defined in terms of subgroup failure probabilities, which means that simple, exact and consistent expressions for different success criteria can be derived. The underlying physical stress-strengh model provides understandable interpretations for the model parameters. Current activities (Mankamo, 1989) involve detailed data analyses and performance of sensitivity studies based on applications of extended alpha-factor and CL-methods (see below). It must be emphasized that also in this case the initial handling of data may in practice have a much stronger impact on the end result than the choice of quantification model.

7) One of the main problems in the current state of CCF-analysis is lack of a systematic approach to reflect inherent defensive measures against CCFs when generating CCF-parameters. Use of partial beta-factor method (Johnston, 1987) has been proposed as a solution to this problem. Some qualitative guidelines have been recently developed for defensive strategies in order to reduce susceptibility to CCFs (Crellin et al., 1988). In Swedish comparative studies (Carlsson et al., 1988) aiming at generation of reference plant models characterized by consistent treatment of central modeling topics (e.g. accident sequence modeling, data, human interactions, dependencies) recommended CCF-parameters have been assigned for different component groups taking into

consideration the degree of physical and functional separation at different plants. Present efforts are directed towards generation of the Swedish CCF-data book, which should reflect these aspects.

8) Current praxis with respect to boundary conditions of CCF-analysis means that residual CCF-contributions are usually limited to intrasystem dependencies. Thus, for practical reasons CCFs are seldom postulated for identical components belonging to different redundant systems. As a consequence of this approach the estimated impact of CCFs on overall level of safety does not fairly reflect advantages of high level of redundancy.

9) The parametric uncertainties associated with CCF-estimates corresponding to high failure multiplicities are large. However, as demonstrated in the Nordic reference study on uncertainty and sensitivity analysis (Hirschberg et al., 1989b,c) the estimates of the overall uncertainty interval may vary significantly depending on the choice of screening assumptions, quantification methods and probability distributions. Thus, the 90 % confidence bound for a quadruple CCF covered between one and three decades in the primary analyses carried out by different groups. Notable is also the decisive importance of "state-of-knowledge" dependences, which is not reflected in PSAs limited to point estimates.

As indicated above some problem areas within CCF-analysis require continued development efforts. In the area of CCF-contributions in systems with ultra high redundancy level a recently initiated Swedish-Finnish cooperation project is aimed to result in improved understanding of dependent failure mechanisms in such systems, in a practical analysis method and a documented data base for BWR safety/relief valves. Applicability to other ultra high redundancy systems is also considered.

Another high priority research project (Hirschberg, 1989) addresses plant-specific defensive measures against CCFs and aims at generation of representative CCF-data which properly take into account efficiency of such defences. The first phase being in progress concerns the central methodological aspects, while at this stage application will be limited to diesel generators. Future extensions to other types of components are planned. The intended approach is in line with current NRC-research centered on a cause-coupling-defense methodology (Parry et al., 1989) and benefits also from the recently formulated procedural framework for CCF-analysis (Mosleh et al., 1988). Also previous Nordic experiences from analyses of common cause failure data for diesel generators (Mankamo and Pulkkinen, 1982; Hirschberg and Pulkkinen, 1985), are being used. A somewhat simplified approach to accounting for the quality of CCF-defenses has recently been presented in one of the Finnish PSAs (Himanen et al., 1989).

6.2 Human Interactions

Human interactions have been studied partly by means of retrospective comparative studies of available PSA (Bengtz and Hirschberg, 1987; Pyy and Pulkkinen, 1988; Hirschberg et al., 1989a) and partly by means of a reference study concerning one of the major operator actions identified for the latest generation of Swedish BWRs (Hirschberg, ed., 1989). In relative terms smaller resources were allocated within the present project to the treatment of human interactions than to analysis of dependencies and uncertainties.

The comparative studies show that human interactions have relatively strong impact on the results of the studies, i.e. the contributions of human errors to the total core damage frequency is in most cases substantial. Characteristically, human errors associated with disabling of plant equipment during testing and maintenance before an initiating event are quite insignificant for plants with a high degree of redundancy and separation (Forsmark 3, Oskarshamn 3). On the other hand, a particular dynamic operator action during accident conditions (manual depressurization), has a very strong impact on the PSA-results for these plants. Modification of the actuation signal logic of the pressure relief system is presently being discussed. This would lead to substantial reduction of the total core damage frequency for the affected plants.

The principal human interaction contributing to the dominating accident sequences of the early generations of the Swedish BWR plants considered in this work (Barsebäck 1/2, Ringhals 1 and Oskarshamn 1) is failure to carry out back-flush operation in case of large or medium LOCA. In addition, the results obtained for some of the elder BWR plants are quite sensitive to the assigned probabilitites of manual reactor shutdown in case of a critical CCF in the reactor protection system (RPS). For the only one PWR analysed (Ringhals 2) failure to depressurize and failure to switch to high-head recirculation after small LOCA constitute the principal human interactions (some other actions have, however, only a slightly smaller importance).

Only few recoveries have been modeled in the studies. In relative terms most credit for restoring unavailable safety system functions has been taken in the Oskarshamn 3 PSA.

From the modeling point of view a wide spectrum of differences has been observed between human interaction analyses as performed in different PSAs. The attention given to human reliability analysis in the Swedish PSAs varies significantly. This is in contrast with the relatively detailed modeling of dependencies and common cause failures in most of the Swedish PSAs.

The possible reasons for not giving the highest priority to modeling of human interactions in the current Swedish PSAs are as follows:

1) It was rather natural to concentrate on hardware functions, at least in the first generation of Swedish PSAs. Treatment of hardware reliability is not a controversial subject and is supported by the Swedish data base of high quality and by relatively long operating experience. The results concerning hardware performance are considered as more credible and have in several cases led to plant modifications.

2) For the Swedish BWRs there are rather few critical operator actions during accident conditions and plant operators have extensive experience from handling such situations in simulator exercises. Another important factor is the so called "30 minute rule" valid for all ABB Atom BWRs. With few exceptions 30 minutes are available to the operators after an initiating event, before manual actions become necessary. For all Swedish BWRs at least 4 hours are available to assure proper function of the residual heat removal systems. Thus, the issue of time windows for operator actions is relatively simple.

3) The methods for efficient treatment of human interactions are presently being developed, are not well established, and the experience of their application is still very limited. All the Swedish PSAs have been generated in a relatively short period of time and there has been no time to incorporate the latest findings within the studies.

Thus, the limitations of the human interaction analyses have in most cases been prescribed by the intended scope of PSAs.

It is natural that after implementation of hardware improvements more attention is presently being given to the man-machine interactions. Areas of interest in the context of future research have been outlined in paragraph 3.3.5 of the present report. Of particular importance is the study of errors of commission, which in principle have been disregarded in the available studies. A more pronounced involvement of plant personnel and specialists in control room design is also desirable. Hopefully, a more constructive dialogue will be initiated between technical experts and behavioural scientists. From practical point of view it has been concluded that basically all aspects of

human interaction analysis in the Swedish PSAs can be improved. This includes both the degree of detail, methods and data, and documentation of the analyses.

The reference study concerning manual depressurization and carried out by all the groups demonstrated the importance of clear specification of boundary conditions for the analysis of human interactions. This applies e.g. to the success criteria and to the timing conditions.

Given similar boundary conditions the numerical agreement between the groups was quite satisfactory. This is not too surprising since two of the groups used THERP-method combined with data from the Handbook of Human Reliability Analysis (Swain and Guttman, 1983). Also the comparison of THERP- and HCR-method (Hannaman et al., 1985) carried out by one of the teams resulted in a good agreement between the predictions as far as the probability of misdiagnosis is concerned. However, the HCR-method gives in the analysed cases unrealistic estimates of the probability of incorrect carrying out of the task given correct diagnosis. In this context some flaws of the HCR-method have been pointed out.

The reference study resulted also in concrete recommendations concerning both ergonomical and procedural improvements. The simulator exercise proved to be very useful as a supporting analysis tool in spite of limitations related to differences in conditions which would be experienced by operators in real accident conditions.

The reference study on uncertainty and sensitivity analysis (Hirschberg et al., 1989 b,c) confirmed that the statistical uncertainties associated with the analysed human interaction contribution, are substantial. This is natural since no empirical evidence exists for the particular operator action. Independently of which model is used for estimation of the contributions, subjective judgement plays a central role when assigning failure probabilities to operator actions. However, the numerical consequences of changes in state-of-knowledge can be quite different when applying various models. This issue needs further investigations.

6.3 Uncertainty Aspects

The uncertainty aspects have been highlighted within the sensitivity analyses of CCFs and human interactions (Hirschberg et al., 1989a), within the reference study on uncertainty and sensitivity analysis (Hirschberg et al., 1989b,c) and within a separate study concerning decision making in view of uncertainties (Pulkkinen and Pörn, 1990).

Some uncertainty aspects in the context of treatment of CCFs and human interactions have already been described in sections 6.1 och 6.2 and will not be repeated.

The reference study demonstrated that the statistical uncertainties associated with the frequency of the analysed accident sequence are large. This was expected since the sequence involved a critical human interaction combined with common cause failures in a system characterized by a high level of redundancy.

As a result of modification of the approaches to modeling of some of the critical elements, made in the course of the study, the numerical agreement between the groups has been drastically improved in the best estimate phase.

"State-of-knowledge" dependences may have a surprisingly large impact on the quantitative results and must be taken into account in order to avoid underestimation. Thus, the result of a traditional point value analysis is not representative for the uncertainty distribution in cases where "state-of-knowledge" dependences have significant impact.

Some additional methodological insights concern:

- The usefulness of the linear standby failure model for applications involving phased mission operation. In the particular case analysed the model provided a more realistic representation than the simplified approach originally used in the reference PSA.

- Impact of higher order terms in the uncertainty polynomial as compared to first moment approximation. The actual impact depends on the degree of dependency between the cut-sets and on the absolute level of failure probabilities involved. The numerical importance of this aspect may be negligible when generating point estimates and significant when uncertainty distributions are properly propagated.

- Use of reduction of variance as a practical and simple measure of the uncertainty contribution from a particular variable. When this variable is assumed completely known (equal to a fixed value) while all others follow their uncertainty distributions, the variance of the final distribution will usually decrease. This variance reduction can then be considered as a measure of the uncertainty contribution from the variable in question.

- Application of the Bayesian approach which presupposes the acceptance of subjective probabilities and makes the propagation of uncertainties rather easy by the use of Monte Carlo technique. Monte Carlo simulation from multidimensional distributions was necessary in case of the linear standby failure model and interdependent CCF-parameters.

Good agreement between Monte Carlo based computer codes for uncertainty propagation (MONTEC, MOCARE, SAMPLE, SPASM) has been demonstrated. However, the precision of mean and standard deviation generated by Monte Carlo technique is much more dependent on the sample size than the precision of percentiles. Still, reasonably reliable estimates of the mean and standard deviations have been obtained using 5000-10 000 realizations. If more precise estimates are required development of an analytical approach might be necessary.

The present study demonstrated that uncertainty analysis based on the current Swedish PSAs and data is feasible, requires reasonable resources, and may be carried out using the available computer codes. Improvements with respect to more realistic uncertainty distributions for certain component types and with respect to increased flexibility of simulation codes are possible, and are already being implemented.

The sensitivity analyses performed proved to be an efficient tool for demonstrating the impact of use of different assumptions, methods and data on the results of PSA-studies. In this way guidance was provided with respect to these aspects of current analyses, which call for future efforts in form of supplementary studies and/or research projects.

In addition to the Reference Study on Uncertainty and Sensitivity Analysis some basic questions e.g:

- How to describe uncertainty?
- What is the purpose of uncertainty analysis?
- How to use the obtained uncertainty measures in the decision making process?

have been addressed.

Probability distribution is the most common measure of uncertainty. There are, however, several different probability concepts. Among these we prefer the subjective probability, which is interpreted as the degree of belief on the unknown state of nature. The subjective probability is always conditioned by existing (subjective) knowledge and can be updated (learning from experience) and used for statistical inference via application of Bayes theorem. This type of probability can be assigned also to nonstatistical events, a feature which is of great importance when modeling the uncertainty in safety analyses.

In general, the utmost objective of uncertainty analysis is to improve the precision of the decision making procedure (to make the correct decision as frequently as possible). In the reference study mentioned above the uncertainty around the core damage frequency (associated with a specific accident sequence) was studied based on the uncertainties of various reliability parameters on the component and task level. The study resulted in probability distributions describing the uncertainty about this partial frequency of core damage. These distributions can then be used to calculate e.g. the integral probability of core damage during the rest of the plant's lifetime, the latter probability being a risk (or utility) measure for the existing plant. Calculating such a risk measure for alternative designs and procedures, one gets a valuable support for the decision to be made. Thus the core damage probability is the final quantity of interest for the decision maker, a quantity that contains all uncertainties that have been quantified in the analytic process. The core damage frequency, on the other hand, is still an auxiliary parameter with an associated uncertainty distribution. By the propagation of uncertainties from basic parameters to core damage frequency it is possible to identify the most dominating sources of uncertainty, or to calculate the value of additional information on some parameter(s).

In decision making situations one has to choose between a set of alternative actions. According to decision theoretic models the decision maker chooses the action that has the maximum expected utility. The concept of utility is constructed to provide a tool for consistent ranking of each possible outcome and decision alternative. This concept is closely related to probability. According to the decision theoretic model it is also possible to calculate the value of information in some given respect. Such a value is of great benefit when resources have to be allocated for getting more information.

Within the area of PSA uncertainty analyses have been performed to some extent, but it is true that such analyses have not been utilized extensively in the decision making processes. In our view, the decision theoretic means are applicable also to safety related decisions. Of course, we are well aware of the fact that not all decision influencing factors can be quantified. Thus, in the future it would be worthwhile to further develop methods for the description of modeling uncertainties, to extend as far as possible the application of a decision theoretic model and to investigate the robustness of the decision procedure with respect to nonquantifiable factors. With regard to such factors, it would also be worthwhile to further develop methods for qualitative uncertainty analysis. By conducting qualitative uncertainty analyses one could identify additional sources of uncertainty, and roughly rank them with respect to the needs for detailed investigation.

6.4 Recommendations

Recommendations of the present project concern both approaches to specific modeling issues, need of supplementary analyses and need of future research activities. The most important recommendations have already been given implicitly or explicitly in the preceding subchapters. For the sake of clarity they are summarized in the following points.

1) It is advisable to explicitly model specific dependent failure mechanisms whenever possible and to make a clear distinction between the coverage of such modeling on the one hand, and the scope of the common cause failure analysis on the other hand.

2) Supplementary dependent failure analyses are needed concerning specifically:

   - Common Cause Initiators and dynamic effects following LOCA for the early generations of Swedish plants

   - Human interaction dependencies and possibly more detailed modeling of electric power supply for all Swedish plants.

3) Recommended approaches to quantification of CCF-contributions are use of:

   - direct assessment in applications where in-depth studies of raw data are being undertaken

   - alpha-factor model when good quality single failure data are available.

Preferably all relevant failure multiplicities should be taken into account. Systematic analyses of historical events including plant-specific interpretation provides increased understanding of failure mechanisms, eventhough the quantitative estimates are subject to large uncertainty.

4) Future research work in the context of CCF-analysis should concentrate on qualtitative aspects (failure mechanisms) and on collection of data. The projects considered as primary priorities are:

   - Systematic consideration of plant-specific defensive measures against CCFs and generation of representative CCF-data (based on Finnish/Swedish operating experience combined with qualitative insights), which properly take into account efficiency of such defences. A pilot project addressing these issues for diesel generators was already initiated in the beginning of 1990.

   - CCF-contributions in systems with ultra high level of redundancy. A pilot project including an application to pressure relief valves was already initiated in the beginning of 1990.

   - Search for Common Cause Initiators using the Finnish/Swedish operating experience. The root causes behind the incidents may provide valuable information of generic character. Possibly, potential interactions involving diversified systems, could be identified.

5) Analytical efforts within the field of human interactions should be intensified. Although PSA-methodology is not capable of handling the whole spectrum of issues in the context of man-machine interactions, it provides a frame for structuring the problems and for focusing the analyses on important aspects.

6) Main improvements of the present Swedish PSAs would involve:

   - Situation-specific studies of identified principal contributors

   - More systematic documentation of the analyses performed

   - Use of methods and data which better reflect state-of-the-art.

7) In the context of modeling of human interactions clear specification of boundary conditions for the analysis is of critical importance. This applies e.g. to the success criteria and to the timing conditions. Central role of subjective judgement has been highlighted. However, the numerical consequences of changes in state-of-knowledge can be quite different when applying various models. This issue needs further investigations. The HCR-method should be used with care in situations where the time needed to perform a task is comparable or much shorter than the total available time.

8) Use of carefully planned simulator exercises as a supporting analysis tool is strongly recommended. Plant personnel and specialists in control room design should participate in the analysis work to a greater extent than today.

9) The areas of main interest for future research in the context of human interaction analysis are as follows:

- Study of errors of commission including methodology development and applications. Highest priority is assigned to this activity.
- Higher degree of integration of reliability models, engineering judgement and operating experience with cognitive psychology.
- Model studies aiming at systematic use and interpretation of simulator experiments.
- Systematic search for human errors based on Finnish/Swedish operating experience.
- Systematic studies of possibilities for recoveries and their impact on PSA-results.

10) The results of a traditional point value analysis are not representative for the uncertainty distribution in cases where "state-of-knowledge" dependencies have significant impact. In such situations use of point values leads to underestimation and possibly to wrong conclusions. This motivates supplementing of the present Swedish PSAs with formal uncertainty analyses based on uncertainty propagation by the use of Monte Carlo technique. Available computer codes are suitable for that purpose.

11) The Swedish Reliability Data Book (T-book; Bento et al., 1985) provides generally reasonable mean values for failure probability of the components. Other uncertainty distribution parameters (confidence intervals) are in some cases not realistic. In addition, the grouping of components such as motor-operated valves should be based on test interval length rather than on the component size. Efforts to implement improvements with respect to these aspects are already under way and will be reflected in the new version of the T-book (to be issued in 1990). In this context the empirical-Bayes method based on the use of subjectively assessed prior distributions (Pörn, 1989), will be employed. Generally, among the different probability concepts subjective probability is the preferable one when carrying out probabilistic safety analyses.

12) In the future further efforts should be undertaken to use subjective probabilites to describe even modeling uncertainties. According to basic probability laws one can express the total uncertainty with integral probability values, i.e. without any furhter uncertainty bounds. This will greatly facilitate the decision making process. An important step in all uncertainty analyses is also to find the areas where additional information would be of greatest value. Future developments should include applications of decision theoretic models and investigations of the robustness of the decision procedure with respect to nonquantifiable factors.

6.5 References

Bengtz, M. and Hirschberg, S. (1987)
Retrospective Analysis of Human Interactions in the Swedish Probabilistic Safety Studies. Phase I: Qualitative Overview. Report RAS-470(87)5 (ABB Atom Report RPC 87-54), July 1987.

Bento, J.-P., Björe, S., Ericsson, G., Hasler, A., Lydén, C.-O., Wallin, L., Pörn, K., Åkerlund, O. (1985)
Reliability Data Book for Components in Swedish Nuclear Power Plants. Prepared by ABB Atom AB and Studsvik AB for Nuclear Safety Board of the Swedish Utilities and Swedish Nuclear Power Inspectorate, May 1985.

Carlsson, L., Hirschberg, S. and Johanson, G. (1987)
Qualitative Review of Probabilistic Safety Assessment Characteristics. PSA '87 -International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Carlsson, L., Hirschberg, S., Johanson, G., Pörn, K. and Wilson, D. (1988)
Can Different PSAs be Compared and Used in Nationwide Decision Making? Status of and Experience from the Swedish ASAR-program. OECD/CSNI Workshop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Crellin, G.L., Mott, J.E. and Smith, A.M. (1988)
Defensive Strategies for Reducing Susceptibility to Common Cause Failures. Volume 1: Defensive Strategies. Report EPRI NP-5777, June 1988.

Ericsson, G. and Hirschberg, S. (1984)
Treatment of Common Cause Failures in the Barsebäck 1 Safety Study. Fifth International Meeting on Thermal Reactor Safety, Karlsruhe, Federal Republic of Germany, September 9-13, 1984.

Fleming, K.N. and Kalinowski, A.M. (1983)
An Extension of the Beta Factor Method to Systems with High Levels of Redundancy. Report PLG-0289, August 1983.

Hannaman, G.W., Spurgin, A.J and Lukic, Y. (1985)
A Model for Assessing Human Cognitive Reliability in PRA Studies. 1985 IEEE Third Conference on Human Factors and Power Plants, Monterey, California, U.S.A.

Himanen, R., Kosonen, M. and Mankamo, T. (1989)
Defences against Common Cause Failures. Introduction to Quantitative Approach. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Hirschberg, S. (1989)
Project Plan: Defences against Common Cause Failures (CCFs) and Generation of CCF-data. Pilot Study for Diesel Generators (DGs). ABB Atom Report RPC 89-60, July 1989.

Hirschberg, S., ed. (1987)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Common Cause Failure Data Benchmark Exercise. Final Report, RAS-470(86)14 (ABB Atom Report RPA 86-241), June 1987.

Hirschberg, S., ed. (1989)
NKA-project "Risk Analysis" (RAS-470): Summary Report on Reference Study on Human Interactions. Final Report, RAS-470(89)17 (ABB Atom Report RPC 89-112), December 1989.

Hirschberg, S., Björe, S. and Jacobsson P. (1989a)
Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA '89 -International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S., Jacobsson, P., Petersen, K.E., Pulkkinen, U. and Pörn, K. (1989b)
Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Hirschberg, S., Jacobsson, P., Pulkkinen, U. and Pörn, K. (1989c)
Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A, April 2-7, 1989.

Hirschberg, S. and Pulkkinen, U. (1985)
Common Cause Failure Data: Experience from Diesel Generator Studies. Nuclear Safety, 26(3), pp. 305-313, May-June 1985.

Johnston, B.D. (1987)
A Structured Procedure for Dependent Failure Analysis (DFA). Reliability Engineering, 19, pp. 125-136, 1987.

Mankamo, T. (1989)
Project plan: CCF Analysis of Highly Redundant Systems; Safety Relief Valve Data Analysis and Reference Application. Avaplan Oy Report, September 1989.

Mankamo, T. and Kosonen, M. (1988)
Dependent Failure Modeling in Highly Redundant Structures - Application to BWR Safety Valves. Scandinavian Reliability Engineers Symposium, Västerås, Sweden, October 10-12, 1988.

Mankamo, T. and Pulkkinen, U. (1982)
Dependent Failures of Diesel Generators. Nuclear Safety, 23, pp. 32-40, January-February, 1982.

Mosleh, A., Fleming, K.N., Parry, G.W., Paula, H.M., Worledge, D.H., Rasmuson, D.M. (1988)
Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Procedural Framework and Examples. Report NUREG/CR-4780 (EPRI NP-5613), PLG-0547, vol. 1, January 1988.

Mosleh, A. and Siu, N.O. (1987)
Multi-parameter Common Cause Failure Model. 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Parry, G.W (1984)
Incompleteness in Data Bases: Impact on Parameter Estimation Uncertainty. 1984 Annual Meeting of the Society for Risk Analysis, Knoxville, Tenn., September 30 - October 3, 1984.

Parry, G.W., Paula, H.M., Mitchell, D.B., Whitehead, D.W and Rasmuson, D.M. (1989)
A Cause-coupling-defense Approach to Common Cause Failures. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Poucet, A., Amendola, A. and Cacciabue, P.C. (1987)
CCF-RBE Common Cause Failure Reliability Benchmark Exercise. Report EUR 11054 EN, Ispra Establishment, 1987.

Pulkkinen, U. and Pörn, K. (1990)
Uncertainty in Safety Analysis and Safety Related Decision Making. Report RAS-470(89)12, to be published 1990.

Pyy, P. and Pulkkinen, U. (1988)
Human Reliability in Probabilistic Risk Assessment. A Retrospective Study. Report RAS-470(87)10 (VTT Research Notes 908), November 1988.

Pörn, K. (1989)
Some Comments on CCF-quantification. The experience from the Nordic Benchmark. In Proceedings of the ISPRA Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 243-256.

Pörn, K. (1989)
An Empirical Bayesian Inference Applied to Poisson Probability Models. Draft Report Studsvik/NP-89/7, 1989.

Samanta, P.K, O'Brien, J.N. and Morrison, H.W. (1985)
Multiple-Sequential Failure Model: Evaluation of and Procedures for Human Error Dependency. Report NUREG/CR-3837, May 1985.

Swain, A.D and Guttman, H.E. (1983)
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report, NUREG/CR-1278, August 1983.

Vuorio, U.M. and Vaurio, J.K. (1987)
Advanced Human Reliability Analysis Methodology and Applications. PSA '87 - International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

APPENDIX A: RAS-470 PUBLICATIONS

References to the most important RAS-470 reports have been made in the preceding chapters. The list which follows below includes international publications (mainly conference papers) originating from the RAS-470 project. Additional publications in international technical journals are anticipated. The publications are given in chronological order.

Hirschberg, S. and Knochenhauer, M.
Application of Sensitivity Analysis in Nuclear Power Plant Probabilistic Risk Assessment Studies. International Conference on Models and Uncertainty in the Energy Sector, Risø, Denmark, February 11-12, 1986.

Hirschberg, S., Bengtz, M., Dinsmore, S., Petersen, K.E. and Pulkkinen, U.
Common Cause Failures: Identification and Quantification. Scandinavian Reliability Engineers Symposium, Otaniemi, Finalnd, October 14-16, 1986.

Pulkkinen, U.
Comments on Uncertainties and Limitations of Systematic Risk Analyses. Scandinavian Reliability Engineers Symposium, Otaniemi, Finland, October 14-16, 1986.

Hirschberg, S. and Knochenhauer, M.
The Role of Sensitivity Analysis in Probabilistic Safety Assessment. 9th International Conferene on Strucutral Mechanics in Reactor Technology, Lausanne, Switzerland, August 17-21, 1987.

Hirschberg, S., Bengtz, M., Dinsmore, S., Petersen, K.E., Pulkkinen, U.
Nordic Common Cause Failure Data Benchmark Exercise. PSA '87 -International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 -September 4, 1987.

Pulkkinen, U., Huovinen, K. and Kuhakoski, K.
Combination of Several Data Sources. International SNS/ENS/ANS Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, August 30 - September 4, 1987.

Hirschberg, S. and Bengtz, M.
Retrospective Analysis of Dependencies and Human Interactions in Swedish PSA Studies. Scandinavian Reliability Engineers Symposium, Helsingör, Denmark, October 5-7, 1987.

Hirschberg, S.
Probabilistic Safety Analysis. Limitations and Current Development. Lecture Notes, NKA Seminar Risk Analysis and Safety Philosophy, Otnäs, Finland, November 12-13, 1987.

Hirschberg, S.
Treatment of Dependencies and Human Interactions in PSAs. Lecture Notes, NKA Seminar Risk Analysis and Safety Philosophy, Otnäs, Finland, November 12-13, 1987.

Pulkkinen, U., ed.
Proceedings of the CCF Workshop, Lepolampi, Espoo, Finland, May 10-11, 1984. Report RAS-470(87)14 (VTT Work Report SÄH 38/87), December 1987.

Hirschberg, S.
Nordic Benchmark and Reference Studies within the Area of Probabilistic Safety Analysis. IAEA Research Coordination Meeting on Reference Studies on Probabilistic Modelling of Accident Sequences, Moscow, May 23-27, 1988.

Pulkkinen, U. and Simola, K.
Time Dependent Phenomena in PSA. OECD/CSNI Workshop on Program Systems and Computer Codes for Living PSA Application, Hamburg, Federal Republic of Germany, September 26-28, 1988.

Petersen, K.E. and Aid, H.
Use of Operator Training Simulators in Analysis of Human Interventions in Complex Industrial Systems. Scandinavian Reliability Engineers Symposium: Reliability in Power, Process Control and Transport, Västerås, Sweden, October 10-12, 1988.

Simola, K., Pulkkinen, U. and Huovinen, T.
Analysis of Time Dependencies in Probabilistic Safety Assessment. Scandinavian Reliability Engineers Symposium: Reliability in Power, Process Control and Transport, Västerås, Sweden, October 10-12, 1988.

Hirschberg, S.
Treatment of Common Cause Failures. The Nordic Perspective. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 9-29.

Hirschberg, S. and Tirén, L.I.
Design-related Defensive Measures Against Dependent Failures. ABB Atom's Approach. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 71-100.

Petersen, K.E.
Analysis of CCF-data - Identification. The Experience from the Nordic Benchmark. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 235-241.

Pulkkinen, U.
Multiple Related Failures from the Nordic Operating Experience. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 277-288.

Pörn, K.
Some Comments on CCF-quantification. The experience from the Nordic Benchmark. Proceedings of the Advanced Seminar on Common Cause Failure Analysis in Probabilistic Safety Assessment, Ispra, Italy, November 16-19, 1987. Kluwer Academic Publishers, Dordrecht/Boston/London, 1989, pp. 245-256.

Pyy, P. and Pulkkinen, U.
Treatment of Uncertainties in Human Reliability Analysis. Sixth EuroData Conference on Reliability Data Collection and Use in Risk and Availability Assessment, Siena, Italy, March 15-17, 1989.

Hirschberg, S., Björe, S. and Jacobsson, P.
Retrospective Quantitative Analysis of Common Cause Failures and Human Interactions in Swedish PSA Studies. PSA '89 - International Topical Meeting on Probability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S., Jacobsson, P., Pulkkinen, U. and Pörn, K.
Nordic Reference Study on Uncertainty and Sensitivity Analysis. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Pulkkinen, U.
Bayesian Uncertainty Analyses of Probabilistic Risk Models. PSA '89 - International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, Pennsylvania, U.S.A., April 2-7, 1989.

Hirschberg, S.
Review of Current Problems in Dependent Failure Analysis. 10th International Conference on Strucutral Mechanics in Reactor Technology, Anaheim, California, U.S.A., August 14-18, 1989.

Hirschberg, S. and Gunsell, L.
Defensive Measures Against External Events and Status of External Event Analysis in Swedish Probabilistic Safety Assessments for Nuclear Power Plants. Second International Post-SMIRT 10 Seminar "Probabilistic Risk Assessment (PRA) of Nuclear Power Plants for External Events", Irvine, California, U.S.A., August 21-22, 1989.

Hirschberg, S., Jacobsson, P., Petersen, K.E., Pulkkinen, U. and Pörn, K.
A Comparative Uncertainty and Sensitivity Analysis of an Accident Sequence. Scandinavian Society of Reliability Engineers Symposium, Stavanger, Norway, October 9-11, 1989.

Pulkkinen, U. and Pörn, K.
Uncertainty in Safety Analyses and Safety Related Decision Making. Scandinavian Reliability Engineers Symposium, Stavanger, Norway, October, 9-11, 1989.

Hirschberg, S.
Experiences from Dependent Failure Analysis in Nordic Countries, paper submitted for publication in Special Issue of Reliability Engineering and System Safety on Common Cause Failures.

Pulkkinen, U.
A Bayesian Approach for Uncertainty Analysis of Probabilistic Risk Models, paper submitted for publication in Reliability Engineering and System Safety.

APPENDIX B: GLOSSARY OF ABBREVIATIONS

ADDEP	Additive Dependency (Model)
ATOM	ABB Atom AB
ATV	Scandinavian Nuclear Power Reliability Data System
BE	Benchmark Exercise
BFO	Back-flush Operation
BFR	Binomial Failure Rate (Model)
BWR	Boiling Water Reactor
B1	Barsebäck 1
CCF	Common Cause Failure
CCI	Common Cause Initiator
CCSS	Containment Cooling Spray System
CL	Common Load (Model)
CSNI	Committee on Safety of Nuclear Installations
CV	Check Valve
DA	Direct Assessment
DRS	German Risk Study
EJ	Engineering Judgement
EPRI	Electrical Power Research Institute
ET	Event Tree
FT	Fault Tree
F3	Forsmark 3
GRS	Gesellschaft für Reaktor-sicherheit
HCR	Human Cognitive Reliability
HRA	Human Reliability Analysis
IGSCC	Intergranular Stress Corrosion Cracking
IREP	Interim Reliability Evaluation Program
LER	Licensee Event Report
LOCA	Loss of Coolant Accident

MFR	Multinominal Failure Rate (Model)
MGL	Multiple Greek Letter (Model)
MLM	Maximum-likelihood Method
MSF	Multiple-sequential Failure (Model)
NEA	Nuclear Energy Agency
NKA	Nordic Liaison Committee for Atomic Energy
NSAC	Nuclear Safety Analysis Centre
OAT	Operator Action Tree
O1	Oskarshamn 1
O3	Oskarshamn 3
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
RAS-450	NKA-project "Optimization of Technical Specifications Using Probabilistic Models"
RAS-470	NKA-project "Risk Analysis"
RHR	Residual Heat Removal
RISØ	Risø National Laboratory
RO	Reactor Operator
RPS	Reactor Protection System
RSCS	Reactor Shutdown Cooling System
R1	Ringhals 1
R2	Ringhals 2
SE	Shift Engineer
SHARP	Systematic Human Action Reliability Procedure
SNL	Sandia National Laboratories
SSA	Situation-specific Analysis
SSPS	Seabrook Study
STUDSVIK	Studsvik AB

T-book	Swedish Reliability Data Book
THERP	Technique for Human Error Rate Prediction
TO	Turbine Operator
TRC	Time-reliability Curve
TS	Technical Specifications
VTT	Technical Research Centre of Finland

THE RAS-400 STEERING COMMITTE

Torstein Bøhler	(Scandpower A/S)
Lennart Hammar	(Swedish Nuclear Power Inspectorate)*
Arne Hedgran	(Royal Institute of Technology, Stockholm)
Hannu Koponen	(Finnish Centre for Radiation and Nuclear Safety)
Hans Larsen	(Risø National Laboratory)
Franz Marcus	(Nordic Liaison Committee for Atomic Energy)

LIST OF PARTICIPANTS IN THE RAS-470 PROJECT

ABB Atom AB	Marit Bengtz Staffan Björe Stefan Hirschberg ** Peter Jacobsson
Risø National Laboratory	Hans Erik Kongsø Gerardo Martinez Kurt Erling Petersen
Studsvik AB	Henrik Aidnell Roland Blomqvist Stephen Dinsmore Rolf Fahlén Kurt Pörn
Technical Research Centre of Finland	Tapio Huovinen Jari Järvinen Kalle Kuhakoski Kaisa Simola Urho Pulkkinen Pekka Pyy
Finnish Centre for Radiation and Nuclear Safety	Reino Virolainen
Swedish Nuclear Power Inspectorate	Gunnar Johanson Bo Liwång *** Ralph Nyman
Imatran Voima Oy	Jussi Vaurio
Swedish State Power Board	Lars Gunsell
Teollisuuden Voima Oy	Risto Himanen

* Chairman
** Project Leader
*** RAS-400 Programme Coordinator