nks
Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-36
ISBN 87-7893-087-1

Experience from the comparison of two PSA-studies

Jan Holmberg and Urho Pulkkinen
VTT Automation, Finland

March 2001

Abstract

Two probabilistic safety assessments (PSA) made for nearly identical reactors units (Forsmark 3 and Oskarshamn 3) have been compared. Two different analysis teams made the PSAs, and the analyses became quite different. The goal of the study is to identify, clarify and explain differences between PSA-studies. The purpose is to understand limitations and uncertainties in PSA, to explain reasons for differences between PSA-studies, and to give recommendations for comparison of PSA-studies and for improving the PSA-methodology.

The reviews have been made by reading PSA-documentation, using the computer model and interviewing persons involved in the projects. The method and findings have been discussed within the project group. Both the PSA-projects and various parts in the PSA-model have been reviewed. A major finding was that the two projects had different purposes and thus had different resources, scope and even methods in their study.

The study shows that comparison of PSA results from different plants is normally not meaningful. It takes a very deep knowledge of the PSA studies to make a comparison of the results and usually one has to ensure that the compared studies have the same scope and are based on the same analysis methods.

Harmonisation of the PSA-methodology is recommended in the presentation of results, presentation of methods, scope, main limitations and assumptions, and definitions for end states, initiating events and common cause failures. This would facilitate the comparison of the studies.

Methods for validation of PSA for different application areas should be developed. The developed PSA review standards can be applied for a general validation of a study. The most important way to evaluate the real feasibility of PSA can take place only with practical applications.

The PSA-documentation and models can be developed to facilitate the communication between PSA-experts and users. In any application consultation with the PSA-expert is however needed.

Many real uncertainties can be identified by comparing PSAs. Generally, comparisons are recommended as a method to review the quality of a PSA-study and as a method to analyse uncertainties of the study.

Keywords

Review of PSA, quality of risk analysis, uncertainty analysis

NKS-36
ISBN 87-7893-087-1

Pitney Bowes Management Services Danmark A/S, 2001

The report can be obtained from
NKS Secretariat, P.O. Box 30
DK – 4000 Roskilde
Phone +45 4677 4045
Fax +45 4677 4046
http://www.nks.org
e-mail: nks@catscience.dk

Foreword

This study is part of the Nordic nuclear safety research (NKS) programme 1998–2001. This project was financed by NKS and Swedish Nuclear Power Inspectorate (SKI). The comparison study has been performed in co-operation with the utilities FKA and OKG that provided information about their safety studies. This final report has been prepared with aid of the project team: Lennart Agrenius, Agrenius ingenjörsbyrå, Jonas Bergman, OKG, Jan Tomas Bergström, Relcon, Anders Hallman, SKI, Göran Hultqvist, FKA, Krister Nilsson, SwedPower AB, Pekka Pyy and Kaisa Simola, VTT Automation. The authors thank the project team and the power utilities for their valuable assistance during the project.

Espoo, March 2001

Authors

Table of contents

Abbreviations

AOT	Allowed outage time (in Technical Specifications)
ASAR	As-operated safety analysis report
BWR	Boiling water reactor
CCI	Common cause initiator
CCF	Common cause failure
EOP	Emergency operating procedures
FKA	Forsmark kraftgrupp AB
FMEA	Failure mode and effects analyses
FSAR	Final Safety Analysis Report
HRA	Human reliability analysis
HTG	Högsta tillåtna gränsvärdet, Safety limit
LER	Licensee event report
LOCA	Loss of coolant accident
MAAP	Modular Accident Analysis Program
OKG	Oskarshamn kraftgrupp
PSA	Probabilistic safety assessment
RCPB	Reactor coolant pressure boundary
RPS	Reactor protection system
RPV	Reactor pressure vessel
SKI	Swedish nuclear power inspectorate

Summary

Two probabilistic safety assessments (PSA) made for nearly identical reactors units (Forsmark 3 and Oskarshamn 3) have been compared. Two different analysis teams made the PSAs, and the analyses became quite different. The goal of the study is to identify, clarify and explain differences between PSA-studies. The purpose is to understand limitations and uncertainties in PSA, to explain reasons for differences between PSA-studies, to give recommendations for comparison of PSA-studies and to give recommendations for improving the PSA-methodology.

The reviews have been made by reading PSA-documentation, using the computer model and interviewing persons involved in the projects. The method and findings have been discussed within the project group. Both the PSA-projects and various parts in the PSA-model have been reviewed. The following reasons were applied for explaining differences: 1) purpose of the PSA, 2) scope of the study, 3) methods used, 4) use of knowledge about systems, functions and phenomena, 5) actual differences between the plants.

A major finding was that the two projects had different purposes and thus had different resources, scope and even methods in their study. Oskarshamn 3 study was influenced by the fact that the utility had performed a detailed PSA for an older unit at the site, and that PSA played an important role for continued operating license of that unit. The utility's goal is to have similar studies for all their units. Forsmark 3 did not have any specific reference study, and neither so specific goal.

The study shows that comparison of PSA results from different plants is normally not meaningful. It takes a very deep knowledge of the PSA studies to make a comparison of the results and usually one has to ensure that the compared studies have the same scope and are based on the same analysis methods. It is important to understand that PSA can never be complete. It is a learning process where operating experience, knowledge and methods develop.

Harmonisation of the PSA-methodology is recommended in the presentation of results, presentation of methods, scope, main limitations and assumptions, definitions for end states (core damage categories), definitions of initiating events, and definitions of common cause failures. This would facilitate the comparison of the studies.

Methods for validation of PSA for different application areas should be developed. The developed PSA review standards can be applied for a general validation of a study. However, the present PSA-studies are so complex that reviews should be detailed. The most important way to evaluate the real feasibility of PSA can take place only with practical applications.

The PSA-documentation and models can be developed to facilitate the communication between PSA-experts and users. In any application consultation with the PSA-expert is however needed. For a person that has not participated in a PSA-project, it is usually difficult to understand all features that should be taken into account in a PSA-application.

Many real uncertainties can be identified by comparing PSAs. Generally, comparisons are recommended as a method to review the quality of a PSA-study and as a method to analyse uncertainties of the study.

1 Introduction

Probabilistic safety assessment (PSA) is an analysis process aiming at identifying and quantifying risks related to a system or process. PSA is based on thorough and consistent application of probability models. It integrates many kinds of knowledge as well as results from technical analyses into a comprehensive probability model. Inevitably, PSA is based on many assumptions and modelling restrictions. Some are known and explicitly presented in the analysis, some are implicitly accepted and used in the modelling work.

In nuclear safety field, PSA has become the main method for risk assessment. Since the pioneering reactor safety study, WASH-1400 (ref.1), the overall approach for performing PSA is about the same in all PSAs. However, the many degrees of freedom in the analysis process and methods make the comparison of different PSA-studies difficult. Therefore it might not be fair to draw conclusions between two nuclear power plants just based on PSA-studies.

There are, nevertheless, needs for comparing PSA-studies, because there is a intention to use PSA, complement to deterministic safety analyses, to support decision making in safety-related issues. For instance, acceptance criteria based on core damage frequency have been formulated in many countries.

Since we have this desire to apply PSA for safety management but we are also aware of the sensitiveness of the approach, it might be worth studying more deeply how mature method PSA is. One way to study such question is to compare PSA-studies. For that purpose, the recently issued PSAs for two nearly identical Swedish reactors, Forsmark 3 and Oskarshamn 3, are excellent material. The PSAs were made by two different power companies and analysis teams, and the analyses became quite different. By comparing these two studies, we hope to get answers to questions like:

- Why two PSA-studies can be so different?
- Which differences are most important?
- Should methods, documentation or boundary conditions be harmonised?
- How to use PSA?
- How to validate PSA for applications?
- How to compare PSA-studies?

This report presents a comparison of two PSA-studies. Section 2 discusses premises for this comparison study, section 3 describes the purpose, scope and method, section 4 presents the two PSA-studies, section 5 summarises the differences between the PSAs, section 6 discusses the reasons and impacts of differences, section 7 gives recommendations and section 8 concludes the report.

2 On the comparison of PSA-studies

2.1 Background for the comparison study

The background for this comparison study was discussions concerning uncertainty analyses of PSA. The purpose of an uncertainty analysis is to identify and documents the uncertain assumptions, variables or models, and to evaluate their impact on the final results of PSA. Uncertainty analysis can be seen as a part of the quality assurance of PSA, since the analysis should critically evaluate the relationship between various pieces of evidence, assumptions, models, and results of PSA. An uncertainty analysis also identifies the additional evidence or analyses needed in both reviewing and clarifying PSA.

Basically, it is possible to qualify PSA by making an entire independent analysis, independent checks for certain issues or an uncertainty analysis. In most cases it is not feasible to make reanalyses, and thus uncertainty analysis is a convenient approach. The question is then what is a feasible method for an uncertainty analysis, what uncertainties should be dealt with, how uncertainties should be documented and how uncertainties should be accounted in applications of PSA.

One practical way to analyse uncertainties is to compare studies. A comparison can considerably widen the perspective regarding uncertainties, if different approaches and methods are to be compared. On the other hand, some uncertainties can be missed, in the case analyses are identical.

Forsmark 3 and Oskarshamn 3 PSAs were chosen as references to study uncertainties and to develop an approach for an uncertainty analysis. The results of these PSAs were very different even if the studies should be quite similar, and it is not easy to explain why it is so. To begin with unifying factors, we can mention that

1. the reactor design is the same
2. deterministic analyses in Final Safety Analysis Report (FSAR) are mostly the same
3. overall approach for PSA is the same following the tradition developed already in WASH-1400
4. regulatory requirements were the same (ASAR 90, ref. 2) and same recommendations were available (SUPER-ASAR, ref. 3, 4)
5. same computer codes applied: Risk Spectrum for PSA-modelling and quantification, MAAP for thermohydraulic analyses regarding core cooling
6. common failure data were applied (T-book, LOCA-frequencies, CCF-factors).

The same reactor designs and practically identical FSARs mean that there should not be any differences regarding descriptions of the plant, functions and systems. The analyses of FSAR are conservative, and if they are replaced by more realistic analyses, the studies may end up with different success criteria.

The overall approach in the studies is the same. A number of initiating events have been identified and defined, event trees constructed for the initiating events, system success criteria analysed for each function, fault tree models made for the systems, probabilities are assessed for the basic events and minimal cut sets solved by a computer. When looking in details, methodological differences can be found.

The same regulatory requirements mean that the scope of the studies, at the minimum, should be same. The Swedish requirements have been expressed in the ASAR-programme. In addition, there has been several joint projects between Swedish nuclear industry and regulatory body leading to recommendations regarding methods and data. Above all, the SUPER-ASAR project is worth mentioning. See more in chapter 0.

The PSA-code affects how things are modelled and presented in a study. The application of the same code in deterministic analyses should definitely reduce differences.

A PSA-study needs both plant-specific and generic data. In this Swedish case, the component failure data mostly comes from the joint database, published as T-books. Moreover, there have been joint projects to estimate CCF-parameters (SUPER-ASAR; high-redundant CCFs, ref. 5).

Despite of those unifying factors there are lots of differences both concerning model, documentation and results. Real differences between the plants or different assumptions applied for uncertain issues cannot solely explain the discrepancy. We have to look more deeply at the analysis process and the method in order to explain the differences. So, it turned to be more interesting to study the whole essence of PSA instead of just uncertainties, and the scope of the comparison study was redefined, see section 0.

Comparisons of PSA-studies have been made earlier. One relevant reference for us is the SUPER-ASAR documentation. The next chapter describes the ASAR-programme and related requirements and recommendations for PSA-studies in Sweden.

2.2 ASAR-programme

The Swedish Nuclear Power Inspectorate (SKI) guidelines associated with the ASAR (As-operated Safety Analysis Report) programme have specified the approximate contents and scope of PSA. Detailed contents and time schedule for PSA work have been later decided in discussions with the utilities. Only Oskarshamn 3 had the performance of a PSA as a licensing requirement.

The ASAR programme is related to the requirement of periodical safety reviews of every nuclear power plant. Reports are to be submitted every 8–10 years to SKI.

2.2.1 ASAR 80-programme

The first guideline, ASAR 80, came 1982 (ref. 6) and included an internal event level 1 PSA for all Swedish nuclear power plants. The ASAR 80 had a significant impact on the development of methods, databases and computer codes for PSA.

2.2.2 SUPER-ASAR

In 1986, SKI initiated a comparative review of all PSAs, the SUPER-ASAR project. The aim of SUPER-ASAR was to review and compare the existing Swedish PSA-studies. For that purpose there were five studies available in 1987: Barsebäck 1&2, Forsmark 3, Oskarshamn 1, Oskarshamn 3 and Ringhals 1. These studies are made for BWR-units. The PSA made for Ringhals 2, which is a PWR, was also partly reviewed in the project.

The goal of SUPER-ASAR was

- to compile and compare the results in the studies with respect to differences in assumptions, modelling and incompleteness
- to identify deficiencies in the studies and needs for complementary analyses
- to provide input for PSA-related R&D work.

SUPER-ASAR was restricted in level 1 PSAs because that was the status of PSA in the 80's. The project focused in the scope of the studies, documentation, modelling and assumptions. The deficiencies or deviations that were identified for each study were categorised into the following groups:

1. a non-conservatism in a study that probably leads to an underestimation of the core damage frequency
2. a non-conservatism in a study that probably does not lead to an underestimation of the core damage frequency
3. a deficiency in a study the impact of which is difficult to judge
4. a conservatism in a study that probably leads to an overestimation of the core damage frequency
5. identified difference that helped in identifying a non-conservatism in another study.

Needs for development and harmonisation of methods were identified for the following problem areas:

- LOCA frequencies and categorisation.
- External pipe breaks regarding completeness of the analysis.
- Transient frequencies and categorisation.
- Assumptions related to total loss of residual heat removal regarding containment response, cavitation of pumps with suction from condensation pool.
- Modelling of the feedwater system regarding functional dependencies, quantification and operator actions.
- Modelling of the reactor pressure relief system regarding plant response in overpressurisation, consequences of failed closure and analysis of manual depressurisation.
- Failure data regarding use of T-boken and updating of failure data.
- CCF-models and data regarding quantification principles and data analysis.
- Common Cause Initiators regarding completeness of the analysis and method.
- Modelling of back flushing regarding phenomenon and manual actions.
- Human interaction regarding resolution, completeness and method.

Findings and recommendations have had a great impact in the ASAR 90-programme and the next generation of the PSAs in Sweden.

2.2.3 ASAR 90-programme

The guidelines for the second round of the safety review, ASAR 90, were given in 1991. The emphasis was put on the completion of the studies. It has placed increased stress on providing an integrated risk picture, suitable for the living PSA approach. This includes extensions of PSA to other operating modes, external initiating events, level 2 analysis, analysis of Common Cause Initiators (CCI), more detailed modelling of loss of coolant accident (LOCA) categories, modelling of electrical power supply and signals.

After the ASAR 90, review of PSAs will not be connected to the ASAR-programme. The new regulatory guide SKIFS 1998:01 (ref. 7) requires that PSA is part of the continuous safety management, which means that the plant must have a PSA-programme, competence for PSA-related activities and quality assurance routines for PSA.

3 Purpose, scope and method for the comparison

3.1 Goal and purpose

The goal of the comparison study is to identify, clarify and explain differences between PSA-studies. As a research object, two studies made for identical nuclear power plants have been chosen.

The purpose of the comparison study is

- to understand limitations and uncertainties in PSA
- to explain reasons for differences between PSA-studies
- to give recommendations for comparison of PSA-studies
- to give recommendations for improving the PSA-methodology.

The purpose of the comparison study is *not* to evaluate the quality of the PSA-studies.

3.2 Scope

The objects for the comparison are level 1 PSA-studies made for Forsmark 3 and Oskarshamn 3. The Forsmark 3 PSA used in the comparison was issued in 1995. Concerning Oskarshamn 3 PSA, the "phase 3" documentation issued in 1999 have mainly been used.

Differences in level 2 studies are not discussed. Use of PSA, i.e. PSA-applications, is also beyond the scope of the study.

3.3 Method

The reviews have been made by reading PSA-documentation, using the computer model and interviewing persons involved in the projects. The method and findings have been discussed within the project group.

The reviews have been divided into the following topics:

1. the PSA-project
2. analysis of initiating events
3. event tree analysis
4. systems analysis
5. human reliability analysis
6. common cause failures and failure data.

Under each topic, the purpose was to identify issues where the two studies differ from each other, to explain the reason for the differences and to judge the impact of the difference. A work report has been written for each topic.

3.3.1 Explanation of differences between PSAs

Table 1 contains a tentative categorisation of various reasons that can be used for explaining differences between the studies. It should be noted that even other reasons can be defined, but we have tried to manage with these ones. There are always connections between the reasons, and some reasons are easier to identify than other ones.

Table 1. Categories of reasons for differences between studies

• Purpose of PSA • Scope of the study • Analysis method • Use of knowledge: Analysis teams use different facts as a basis for an assumption, e.g. different analyses used for defining a system success criterion • Actual difference between the plants

By purpose of PSA, we mean purposes defined by the utility. Definition of purposes can be found in the PSA-documentation, project plan, the utility's PSA-policy statement or by interviewing persons responsible for PSA-activities. Purposes affect the goal of the PSA-project, resources and scope. On the other hand, available resources can restrict purposes.

By scope we mean items included in the risk assessment. Differences in scope always lead to differences in the results. A minimum scope is usually defined in a regulatory guide.

Impact of analysis method is an interesting question. What is the impact of applying a top-down approach instead of a bottom-up approach? In a top-down approach, the top event, e.g. the system failure, is defined first and then causes for the system failure is identified. Fault tree modelling is a top-down method. In a bottom-up approach the single items, such basic events, are first identified and then their consequences are identified. Failure mode and effects analysis (FMEA) and event tree modelling are bottom-up methods. The method can affect that different items are screened out or included, dependencies are assumed differently, items are defined differently or that probabilities are estimated differently.

Ideally, we can say that purpose, scope and the analysis method are determined before the analysis work is started. Then the modelling is just an intellectual process affected by facts resolved with the method and choices made by the analysis team.

Facts depend on knowledge and can be gained by analysing the plant. What is considered a fact is subjective. Different facts can be identified as a reason for different models or probability estimates.

Finally, we have the natural reason that actual differences between the plants make the models different. Note that an actual difference can be caused also by randomness (aleatory uncertainties). For instance, the difference between failure rates of identical components belongs to the category of an actual difference.

Discussion regarding reasons for differences is continued in Section 6.

3.3.2 Evaluation of impacts of differences

Tabe 2 contains a list of criteria that have been applied in the evaluation of the impacts of differences. By quantitative impacts we mean impact on the numeric results. Core damage frequency is the top quantitative result in level 1 PSA. In addition, it can be interesting to compare cut sets and importance measures.

Quantitative impacts have been evaluated crudely. Sensitivity analyses have been performed only in few cases.

Qualitative impacts are at least as important as quantitative, but they are not so easy to define. Concerning the model, completeness issues and modelling adequacy are relevant aspects. Concerning use and administration of the study, limitations in applications, user-friendliness and quality of documentation are important.

Tab 2. Criteria for evaluation of the impact of differences between the PSAs.

Quantitative impact	Qualitative impact
• core damage frequency • frequency of a specific undesired consequence • core damage frequency for a specific initiating event • relative importance of functions, systems and basic events	• completeness • modelling adequacy • limits applications • affects user-friendliness • quality of documentation (clarity, references)

4 Description of the studies

4.1 Reactor design of Forsmark 3 and Oskarshamn 3

Forsmark 3 and Oskarshamn 3 represent the 4th generation of ABB Atoms boiling water reactors (ASEA-ATOM BWR 75). The thermal power output is 3300 MW and the electrical output is 1160 MW net. Both units started commercial operation in 1985.

The general design principle is that safety systems are divided into four physically and functionally separated trains. This design principle makes the unit strong against area events like fire and flooding and against external hazards. The buildings and systems have been classified to hold earthquakes. Some other design features are mentioned in Table 3. There are also differences that have importance in PSA, as listed in Table 4.

Table 3. Some design features of Forsmark 3 and Oskarshamn 3.

- Reactor recirculation pumps are internal.
- Hydraulic scram is backed-up with screw insertion.
- Boron injection system is a manual back-up.
- Safety relief system consists of 16 valves that blows down to condensation pool.
- The reactor containment is designed for a pressure up to 0.6 MPa and during operation filled with nitrogen gas.
- A system for filtered venting connected to the containment in order to prevent radioactive release.
- Both auxiliary feedwater system and low pressure core cooling system consist of four separate trains taking water from the condensation pool.
- 2-out-of-4 logic in the reactor protection system.
- The electric power systems consist of four separate trains and four diesel generators supply emergency power.
- A single turbo generator and a feedwater tank.

Table 4. Differences between Forsmark 3 and Oskarshamn 3 design.

- Logic for regulation of auxiliary feedwater system: low level in reactor pressure vessel blocks the regulation in Oskarshamn 3.
- Logic signal for the actuation of depressurisation of the reactor pressure vessel in order to use the low pressure core cooling system (TB-function): in transient, a manual action is needed in Forsmark while it is actuated automatically in Oskarshamn 3 when the extra low level is reached.
- In Oskarshamn 3, the safety relief system includes lines for water blowdown. Such valves have recently been installed even in Forsmark but not accounted in PSA-95.
- Oskarshamn 3 has an extra feedwater system (system 328) that can be used as an extern water source if the cooling of condensation pool is lost.
- Oskarshamn 3 has a possibility to blow steam to feedwater tank which can be used as an alternative residual heat removal method.
- Link to the national grid is slightly different. In Forsmark, gas turbines start automatically in the case of loss of offsite power. In Oskarshamn, gas turbines are primarily for units 1 and 2, and to supply unit 3 manual start is needed.

4.2 Forsmark 3 PSA

4.2.1 Earlier studies

The first study for Forsmark 3 was made in 1977 by Asea-Atom as an initiative of the Swedish Energy Commission (ref. 8). The study can be regarded as a comparison of Forsmark 3 and Peach Bottom II unit which was analysed in WASH-1400 study.

The result of the study was that the core damage frequency (3.1E-6/year) was estimated to be an order of magnitude lower than in Peach Bottom II. The main reasons for the lower core damage risk were

- higher redundancy of safety systems in Forsmark 3
- dual shutdown mechanism (hydraulic scram + screw insertion)
- safety systems do not have to serve the other units at the site
- the external grid is stronger by the link to 70 kV grid
- gas turbines
- operator actions are not needed within first 30 minutes after a LOCA.

The dominating core damage sequence was failed reactor shutdown after a transient due to failure in the reactor protection system (RPS). Systematic miscalibration or maintenance errors of logic equipment were mentioned as potential causes for the RPS failure.

The next study, issued in 1985, was performed by Asea-Atom for Vattenfall (ref. 9). The study was a complete level 1 study covering internal initiating events, LOCAs, transients and Common Cause Initiators.

The total core damage frequency was estimated to be 7.0E-6/year. The dominating core damage sequence was loss of feedwater initiating event, loss of auxiliary feedwater system due to a common cause failure between all four trains and failed manual depressurisation. The analysis points out the contribution of Common Cause Failures for core damage frequency in a nuclear power plant with Forsmark 3 kind of design philosophy.

4.2.2 Scope of the present study

The present study is a level 1 and 2 PSA issued in 1995 (ref. 10). Minor revisions have been made since that, but the document and the model that were available for this comparison study are from 1995.

The initiating events analysed are

- LOCAs inside containment
- LOCAs outside containment
- Transients
- Common cause initiators (CCIs) such as loss of support systems.

It should be noted that there are pre-studies regarding fire, flooding, steam and earthquake as well as low power operation modes for Forsmark 3 (ref. 11, 12), but they are reported separately.

The PSA-study is a complete updating of the previous 1985 PSA. Documentation and models have been totally revised. The study was reported as a part of the ASAR-review of Forsmark 3 in 1996.

4.2.3 Results (level 1)

The total core damage frequency is estimated to be 9.2E-6/year that is divided between the following core damage categories:

Core damage category	Frequency
core damage due to failed shutdown or core cooling	7.0E-6/year
core damage due to failed residual heat removal	2.2E-6/year

The dominating initiating event is loss of feedwater that contributes with 40% of the total core damage frequency.

The dominating core damage sequence is loss of feedwater, failed core cooling with the auxiliary feedwater system (327), successful manual depressurisation, but failed core cooling with the core spray system (323). The main cause for failed core cooling with the systems 327 and 323 is that the pumps in these systems are in the same rooms and the room cooling is assumed as a vital function. The dominating basic events are CCFs between pumps in the residual heat removal systems 712- and 721-pumps that are responsible for room cooling.

The following points are highlighted in the conclusions:

- the importance of room cooling for pumps in the systems 322, 323 and 327
- CCF between safety relief valves (system 314) has a large contribution, but will be decreased when the diversified safety relief valves will be installed
- containment and its protection system as well as accident management actions can mitigate 99.8% of the core damage sequences not to lead to uncontrolled radioactive release
- CCFs have a great contribution and there are a lot of uncertainties in CCF-factors
- ATWS has a relatively small importance
- water filling of the lower dry-well is important for mitigation of releases.

4.3 Oskarshamn 3 PSA

4.3.1 Earlier studies

The PSA-work for Oskarshamn 3 was initiated already in 1982 with the goal to verify the safety systems by using reliability analysis methods. This was part of the licensing requirements for the unit. The first analysis was reported in 1984 including an analysis of loss of offsite power initiating event (ref. 13). A complete level 1 study was issued in 1986 including internal initiating events (ref. 14).

The method was same as applied for Oskarshamn 1 unit in the ASAR-review 1982. At that time, PSA was called "systematic reliability analysis" (systematisk tillförlitlighets-analys, STA).

The core damage frequency was estimated to be 3.2E-6/year. The dominating initiating events were loss of feedwater and loss of condenser. Important factors affecting the core damage risk are assumptions related to common cause failures, manual depressurisation (TB) and recovery of fails in the containment spray system (system 322).

4.3.2 Scope of the present study

The present study has been issued in several phases. The latest issue is from 1999 and has been used in this comparison study.

The complete study includes both level 1 and 2 analyses, but level 2 PSA is documented separately.

The initiating events analysed are

- LOCAs inside containment
- LOCAs outside containment
- Transients
- Common cause initiators such as loss of support systems and spurious protection signals
- Fire and floodings (only a barrier analysis, i.e. core damage probability per each event analysed)
- External events (only a qualitative analysis).

Low power operating mode is not analysed.

The study is a complete revision of the previous 1986 PSA.

4.3.3 Results (level 1)

The core damage frequency is estimated to be (1999-02-03 report version):

Core damage category	Frequency
core damage due to failed shutdown	4.8E-6/year
core damage due to failed core cooling	1.3E-5/year
core damage due to failed residual heat removal	2.9E-5/year

In addition, the frequencies for the following end states are calculated: exceeding of safety limits (HTG = högsta tillåtna gränsvärden) regarding reactor pressure and depressurisation.

The following points are highlighted in the conclusions:

- CCFs have a great impact
- system success criterion for the residual heat removal function 322/721/712 1-out-of-4
- room cooling of 322-, 323- and 327-pump room
- CCF between batteries for back-up of DC-net (systems 672 and 673)
- small LOCA contributes 19% to core damage frequency
- LOCA outside of the containment has a negligible contribution.

5 Comparisons

The comparison covers both analysis methods and analysis processes. Major findings and conclusions are summarised in this section. The purpose is not to point out weaknesses or strengths in the studies. Therefore the plants and studies are labelled neutrally as A and B. The labels A and B may be switched between the chapters.

5.1 PSA-projects

5.1.1 Background

Both PSA-projects had quite similar background. The previous studies were from the middle of 1980's, and had not been updated since that. One reason for updating and completing the studies was the forthcoming ASAR-reviews. The ASAR-review set also the level of requirements for these studies from the authority point of view.

One significant difference was that the utility A had experience from using PSA for renewing the operating license of another unit. For that purpose, a detailed PSA-model was developed. The policy of the utility A is to have same level of scope and details in PSAs in order to be able to compare the units.

5.1.2 Goal and purpose

Generally, both plants had about the same goal for their studies: to have up-to-date level 1 and 2 PSA-studies covering all initiating events. Both had also the purpose to apply the study in the ASAR-review.

The utility A had an additional goal to have a similar model as had been done for another unit. This goal is explicitly defined in the study. The applications of PSA are also mentioned more explicitly in PSA A than in PSA B, e.g., safety verification of the plant, risk follow-up, optimisation of test intervals, and evaluation of proposed design modifications.

5.1.3 Scope

In PSA A, the level 2 PSA-study was separate from level 1. Concerning initiating events, the study includes all internal initiating events during the power operation mode. The area events, fire and flooding, have been analysed by a barrier analysis and external initiating events have been analysed only qualitatively. Low power operating modes have not been analysed.

In PSA B´, level 1 and 2 analyses are quite integrated. Concerning initiating events a difference from the PSA A is that neither area events nor external events were included in the PSA-project. Analysis of low power operating mode was also a separate project.

The reactor core was the only source of radioactive release considered in both studies.

Appendix 1 summarises the scope of the PSA-studies.

Table5. Comparison of scopes the PSA-studies.

Scope	PSA A	PSA B
PSA-levels • level 1 • level 2	 • yes • yes, separate from level 1	 • yes • yes
Source of radioactive release	• the reactor core	• the reactor core
Initiating events • internal initiating events • fires and floods • external events	 • yes • barrier analysis [1)] • qualitative analysis	 • yes • a separate study • no
Operating modes • power operation • low power and shutdown	 • yes • no	 • yes • a separate study

[1)] Analysis of conditional core damage probability of the area events

5.1.4 Resources

There is a significant difference in the spent resources. Plant A has used more than three times more man-power for the study. The difference can be seen in the detailness of documentation and model.

5.1.5 Time schedule

The PSA-project A has had several phases, beginning with the first phase in 1995, continuing at the moment with the fourth phase. The PSA-project B was initiated in the end of 1993 and completed in 1995.

The study A has been able to apply a newer version of the PSA-code, Risk Spectrum enabling quantification of larger models than previously. A more recent version of the Nordic reliability data book, T-book 4th edition (ref. 15), has also been available for PSA A.

5.1.6 Project organisation

The project organisations have been quite similar. The project leader has been in the power company, but consultants have done most of the analysis and modelling work. The plant technical and operational organisations have supported the analyses and reviewed the systems and event tree analyses. External consultants have reviewed the PSA-studies.

5.1.7 Quality assurance

The quality assurance routines have been quite similar. The project team first performed a control of reports and models. Reports and models (fault trees, event trees and other diagrams) were then distributed to the plant organisation that controlled the correctness and comprehensibility of the documents. Both studies have reviewed also by an independent review team.

The authority, SKI, has also reviewed the studies.

The difference between the PSA-projects is that PSA A has been carried out in several phases. After each phase the study has been reviewed and comments have been taken into account in the next phase.

PSA B was reviewed independently during the project so these comments are accounted in the version used in this comparison study. Review by SKI was performed after the project. The updating process is now going on, but a revised PSA was not available for this project.

5.1.8 Work process

The work processes have been different. The analysis process of PSA A has been carried out in several phases taking several years. A new version of the study has been released and reviewed in each phase.

The PSA-project B was carried out in one phase taking about 1.5 years. No major problems disturbed the project.

A big problem for PSA A was that the model was too large for the computer code. The solution was to divide the database into two parts. First now, in the phase four, it has been possible to merge the two model parts into one database.

Another significant development of the PSA-model A is concerned with the removal of conservative assumptions in the model, e.g., related to system success criteria and selection of common cause initiators. New analyses have been made to justify more realistic assumption. Therefore, if we had compared phase 1 version of PSA A with PSA B, the quantitative results had been remarkably more different than results of phase 3 of PSA A differ from PSA B.

5.2 Analysis of initiating events

The analysis of initiating events aims at identifying and defining initiating events to be taken into account in PSA. The analysis steps are:

1. identification of initiating events
2. categorisation of initiating events
3. estimation of initiating event frequencies.

5.2.1 Identification

Concerning the identification process, the difference is that the identification method is not explained in PSA A. PSA B has a method description and references are given. The impact of this difference is in the quality of the documentation.

5.2.2 Categorisation

The differences in the categorisation are summarised in Table6.

Table 6. Remarks regarding categorisation of initiating events.

Initiating event category	PSA A	PSA B
LOCA inside containment	Two categories: large and medium LOCA. Small LOCA is included in medium LOCA to simplify the model. Secondary effects are not accounted. Reactor pressure vessel rupture is accounted. This has impact on the level 2 results.	Four major categories: large, medium top, medium bottom and small LOCA. These are further divided into 9 different LOCA event trees and 55 different LOCA-categories regarding secondary effects of LOCA. Reactor pressure vessel rupture is not accounted.
LOCA outside containment	Differences in systems taken into account. Exclusions are not explained. LOCAs outside containment are not dominating in level 1 results, but have impact on level 2.	
Transients	Loss of feedwater and loss of feedwater and condensor considered as two different initiating events/one initiating event category	
CCI: • loss of support systems • spurious signals	Many differences in systems taken into account. Exclusions are not explained. Generally, PSA B assumes more events as potential CCIs.	
Area events: • fires, floods, missiles	Not included	A barrier analysis has been made (conditional core damage probability given an area event).
External events: • weather phenomena, earthquake, man-induced events	Not included	A qualitative analysis has been made.

Reasons for different approaches are different degrees of conservatism chosen (CCIs), different ambitions in analysing systems success criteria (LOCAs), and some different assumptions concerning potential initiating events (e.g. CCIs and LOCAs outside containment).

The differences in the initiating event categories have a large impact on the end result. Firstly one of the studies has more initiating event categories than the other, and secondly this study has applied more specific system success criteria than the other one.

5.2.3 Estimation of frequencies

The differences in the estimation of frequencies are summarised in Table 7.

The reason for different approaches is that the analysis team A chose to utilise as much as possible the recently published initiating event frequency data book I-book (ref. 16). The analysis team B wanted to apply same methods as applied in their other study.

It cannot be said that one study has generally larger frequencies than the other. In some cases, the difference is quite large, e.g. frequencies for LOCAs and loss of certain support systems. The impact of different frequencies is that initiating events get different risk importance values.

Table 7. Remarks regarding estimation of initiating event frequencies.

Initiating event category	Remarks
LOCA inside containment	Both studies utilise WASH-1400 frequencies but interpret them differently. PSA A applies WASH-1400 frequencies directly. PSA B has made an inventory of pipe components, and divided WASH-1400 frequencies between the pipe components. Sum of the LOCA-frequencies differs.
LOCA outside containment	PSA B uses screening values. PSA A applies WASH-1400 frequencies or probability analysis for an interfacing LOCA.
Transients	Frequencies are based on operating experience, i.e., reactor scram statistics. Different estimation models have been applied.
CCI: • loss of support systems • spurious signals	PSA A uses fault tree analyses while PSA B applies screening values or engineering judgements.

5.3 Event tree analysis

We compared the following items in the event tree analysis:

- definition of end states (controlled end states, damage states),
- definition and analysis of system success criteria,
- event sequence modelling (event trees).

5.3.1 Definition of end states

In level 1 PSA, three types of end states can be defined: controlled end states (OK-states), core damage end states, other damage end states. The end state definitions are needed for the system success criteria analyses and as labels for sequences in event trees. Event sequences that are classified as core damages are further analysed in level 2 PSA.

A controlled end state is defined as successful safety functions with a certain mission time. The main difference between the studies is in the requirement for reactor

shutdown: subcritical reactor in cold conditions (20 °C) vs. subcritical reactor in warm xenon-free conditions.

A minor difference is that 20 hours vs. 24 hours mission times are applied.

Core damage states are grouped differently as summarised in Table8.

One reason for different definitions is that PSA A is an integrated level 1 and 2 study while the level 1 study is quite independent in PSA B. The differences between the studies make the comparison of final results difficult because the definition for core damage is not identical.

Table 8. Comparison of core damage state categories.

Failed safety function	PSA A	PSA B
Reactivity control	Core damage class A1	Core damage class B1
Reactor pressure control	Overpressurisation (analysed further)	Other damage state: Fast overpressurisation
Core cooling	Core damage class A1	Core damage class B2
Decay heat removal	Core damage class A2 or A3 depending on the available water source for core cooling	Core damage class B3
Protect containment overpressure	Not analysed in level 1	Core damage class B2
Water level regulation (failure leads to overfilling)	Not analysed	Other damage state: Slow overpressurisation
Depressurisation (failure is to need depressurisation)	OK-sequence	Other damage state: Depressurisation

5.3.2 Definition and analysis of system success criteria

Table 9 summarises the differences in system success criteria.

Reasons for different system success criteria are

- analysis resources for system success criteria (simpler to apply FSAR criteria)
- desire to have a detailed model vs. to have a comprehensible model
- definition for controlled end state (cold vs. warm subcritical reactor)
- the approach for the integration of level 1 and 2 studies (some issues can be treated first in level 2).

The differences between the studies are considerable and should be taken into account when the results are interpreted and compared.

Table 9. Remarks concerning system success criteria.

Safety function	Remarks
Reactivity control	Subcriticality required in cold/warm conditions. Boron injection system (manual action) is credited in the other study
Reactor pressure control (overpressure protection, reclosure of valves)	FSAR definition vs. new analysis applied for overpressure protection (10-out-of-16 / 1-out-of-16 valves must open). One study does not account for consequences of failed reclosure of safety relief valves in level 1.
Core cooling	Both studies apply the MAAP-code but use different fuel temperature criteria for core damage. One study has performed much more analyses than the other one and thus has more detailed system success criteria — more variation between initiating events and event sequences, e.g. failed reclosure of safety relief valves causes a variation. Availability of feedwater system in LOCA is interpreted differently. One study calculates that the main feedwater system can be used in long term only in very small LOCAs, and thus does not take credit for the system in LOCA. FSAR criterion vs. new analysis applied for depressurisation function (6-out-of-8 / 4-out-of-8 valves must open).
Decay heat removal	One study takes credit for more heat removal methods than the other one. This is based on the analysis of EOPs. One study has more specific system success criteria regarding event sequences.
Protect containment overpressure	Not analysed in level 1 in the other study.

5.3.3 Event sequence modelling

Both studies apply the so-called small event tree/large fault tree approach. The front line systems are modelled in a chronological order in the event trees. There is, however, a difference concerning the level of details of the models, which makes the event tree layouts quite different.

Concerning event tree models, in PSA A there is one event tree for each initiating event, and each event tree fits in one event tree page.

In PSA B, another approach has been chosen. The database has been divided into two parts because it was originally too large to be managed by the PSA-code. The fault trees related to reactivity control are handled in database #1 and the other parts in database #2.

The event trees of PSA B (database #2) have more headings than PSA A has. This is because of the more detailed system success criteria and more systems credited e.g. for decay heat removal. Several initiating events can share same event trees. Initiating event specific system success criteria are taken care by boundary conditions in the minimal

cut set analysis. Some event trees are divided into several pages to handle the complexity of event trees.

In order to clarify the event tree models for the reviewers, functional block diagrams have been applied in PSA B.

5.4 System analysis

System analysis consists of analysis of faults or other causes and their combinations that can result in an unavailable system with respect to defined system success criteria. The analysis has usually a qualitative part and a modelling part.

Essential parts of system analyses are human reliability analysis, and analysis of dependencies (CCI, CCF, electric power supply, actuation signals). These tasks are normally documented separately from the system analysis chapters.

5.4.1 Approach for qualitative systems analysis

The system analyses have been documented in system analysis reports that follow the system numbers. The major difference is that the study A applies failure mode and effects analyses (FMEA) to document the critical failure modes accounted in fault tree models. The study B describes modelling assumptions in free text.

PSA A has 53 system analysis chapters while PSA B has 29 chapters. One reason is that study A has included more systems in PSA, but another reason is that PSA B has more compound chapters, one system analysis chapter may include several systems. The analysis of the electrical power supply is an example.

5.4.2 Fault tree modelling and analysis

It should be noted that this comparison of fault tree models is *not* a complete review of the fault tree models. Instead we have made the following checks and, based on subsequent findings, we have studied further the following models:

- fault tree analyses of the main safety functions
- main features in the modelling of electric power supply
- signals modelled in the reactor protection system (516)
- modelling of maintenance.

Findings are summarised in Table 10 and Table 11.

Table 10. Remarks concerning system analyses of safety functions.

Function	Remarks
Reactivity control	The studies apply different system success criteria.
Reactor pressure control (314)	The studies apply different system success criteria.
Reclosure of safety relief valves (314)	Same system success criterion is applied. However, different assumptions regarding how many valves open (all sixteen valves open/eleven valves open)
Feedwater system	Very different models and assumptions. Also quantitative results differ.
Turbine condenser	Different modelling approaches: basic event/fault tree
Auxiliary feedwater system (327)	One study has sequence specific system success criteria. Differences in modelling of the level regulation. Most important basic events are same: CCFs between vital components.
Depressurisation (516TB)	A design difference: manual action not required at one plant. The studies apply different system success criteria.
Core spray system (323)	Differences in crediting operator actions.
Containment spray system (322/721/712)	One study has sequence specific system success criteria. Same CCFs dominate.
Shutdown cooling system (321/331)	The studies apply different system success criteria. Different methods credited. Operator actions modelled as one basic event/several basic events.

Table 11. Remarks concerning modelling of electric power supply, protection signals and maintenance.

Other items	Remarks
Electric power supply	Gas turbines not credited in one study, because they require manual actuation of gas turbine power supply. House turbine operation modelled by a basic event/fault tree. Unloading of diesel bus-bars due to station black-out modelled differently.
Reactor protection system signals	One study accounts consequences of spurious signals. Actuation conditions modelled in the other study
Planned and corrective maintenance	Some differences in systems included in the preventive maintenance packages. Can be a real difference between the plants. Reparation times according to Tech.Spec./T-book. Corrective maintenance of non-critical failures accounted in one study.

5.5 Human reliability analysis

On a general level, the scope of HRAs in both PSAs is relatively similar. Both PSAs follow the usual division of human error types:

- Type A: errors made before initiating event
- Type B: errors causing initiating events
- Type C: errors after initiating events.

The compared PSAs apply different HRA methods. PSA A applies a method based on the work of Swain and Guttmann (ref. 17), with some extensions to take factors related to disturbance observation, diagnosis and decision making into account. The quantitative probability estimates are based on values taken from a time-reliability curve, which are modified by certain performance shaping factors. The earlier version of the method was applied in the analysis of a plant at the same site, and the results obtained in that analysis were utilised in order to save analysis resources.

PSA B applies a method based on both SHARP-technique and above mentioned Swain & Guttmann approach. These approaches were combined to obtain a PSA-specific method.

Although both PSAs apply an HRA model based on performance shaping factors, these factors are not the same in the analyses. Another difference in the HRA models is the analysis of recoveries from erroneous human actions. PSA A includes in some case recoveries as a part of decision or action made by the operator. PSA B does not take recoveries into account. Basically, this difference is due to different decomposition of human actions.

In both PSAs, human error events are assumed to be independent on each other, e.g. erroneous ground states. In addition, PSA B assumes independence between failures to start manually redundant pumps. This leads to optimistic results.

Both of the methods in PSA A and B are basically developed by an analyst or external consultant who also made the HRA study. Since all HRA methods are generally leaning strongly on engineering judgement, the quantitative results are different in the compared PSAs.

The human error events included in the analyses differ rather significantly. In the case of type C human actions, only one of these differences is due to the actual differences between the plants; manual depressurisation is automated at the other plant. The other differences originate either from the principle of system model or modelling decisions.

The events considered as erroneous ground states (refers mainly to wrong state of valves) are different. PSA A has included in the model totally 407 events of this kind, while the corresponding number in PSA B is 229. Only 49 of these events are common to both PSAs. The events are identified in PSA A in the connection with FMEA of safety systems.

5.6 Common Cause Failures

The CCF analyses of both PSA follow the CCF modelling principles of the used PSA computer code (Risk Spectrum). In this code, CCF events are assumed for certain groups of (redundant) components, and CCF-probabilities are assigned for multiple failures of components belonging to same CCF-group. The quantitative CCF estimates are calculated according to the recommendations of the SUPER-ASAR-project using the alpha-factor model and basically the same values of CCF-model parameters. Thus, the main differences are due to the different CCF-groups.

The majority of the CCF-groups in both PSAs are the same. However PSA A has more CCF-groups, in some cases due to more detailed system models (especially regarding electrical systems). In quantitative analysis PSA A has separated the time independent and time dependent failures in order to use the model as ”Living PSA.” This has small impact on CCF-probabilities too.

Both PSAs take into account high redundant CCFs (more than four component). The most important systems affected by such failures are the reactor shutdown systems (221, 222, 354, 532, 516) and safety relief valves (314). The modelling principles are the same: so called extented common load model is used in both PSAs for systems 221 and 222, and alpha-factor model for other high redundant CCFs.

As a conclusion of comparison of CCF modelling one can say that the common PSA-computer code and the earlier studies (SUPER-ASAR) have led to rather similar CCF analyses. The differences are mainly due to differences in system models; in the other PSA the models are more detailed. The data for CCF-models is very similar in both PSAs. This is also due to recommendations from the SUPER-ASAR-project.

5.7 Failure data

The failure data in both PSAs come mainly from the Swedish operational experience, according to the models applied in different versions of T-book (ref. 15). T-book data can be applied in plant specific way, which has led to different numerical values due to obvious reasons. The compared PSAs have used different editions of T-book, which has also some impact on the results.

For repair times, PSA A has applied, instead of plant specific repair time data, the maximal allowed repair time according to technical specifications. This was made due to the comments made by the safety authority to an earlier PSA at the same site, according to which the plant specific repair time data was in some case non-conservative.

Although the same data sources were used, the PSAs differ in the component reliability models. PSA A has aimed at Living PSA model, and it applies time dependent component unavailability models. This has led to many failure modes and parameters of the unavailability model. Since data for all failure modes are not directly given in T-book, various interpretations and judgements must have been made (e.g. assumptions on the rate of non-critical failures). Due to conservative repair times, differences in plant specific data and these assumptions, the unavailabilities of same type of components in the compared PSAs differ in some cases significantly. Basically, the unavailabilities in PSA A are higher that those in PSA B.

6 Discussion

6.1 Introduction

Forsmark 3 and Oskarshamn 3 PSA-studies have been approved internally by the plant and externally by the safety authorities. The studies are, however, quite different both concerning the contents and results.

It cannot be judged that one study is correct and the other one is incorrect. It is more a question about the use of different assumptions and boundary conditions in the studies. Because PSA is such a comprehensive and complicated analysis with lots of judgements, variability in the results is understandable. Is it acceptable or is there something we can or should do, are relevant questions, and will be discussed in this chapter.

The starting point is that both utilities have performed risk studies for their own plants, have identified and analysed risks to reactor safety. There are similar conclusions, for instance, concerning the importance of residual heat removal systems. On the other hand, there are differences, e.g., regarding the importance of various initiating events.

Both plants work continuously with the PSA-studies by updating and revising the analyses. In some issues, the studies have become closer to each other, partly because of information exchange. In some other issues, the PSA-teams have recognised differences but do not want to change their assumptions so that differences remain between the studies.

One important point to notice is that, in this review, we look at different versions of the study. Concerning Forsmark 3, it was the first release of the PSA-project, dated 1995. Concerning Oskarshamn 3, we reviewed the so-called phase 3 study released 1999. The O3-PSA had been revised twice after the first release. However, this is the reality for the user as well as for the reviewer of PSA that the PSA-studies are more or less living documents. The results presented and conclusions drawn in one version can be changed — even radically — to the next version. The history of the study and the status of the PSA-programme of the plant should be known when reviewing the study.

The practical reason for the lack of robustness of PSA-results is that a PSA-project has limited resources and deadlines to be followed. It is difficult to predict how much work is needed to obtain a satisfactory study. Typically, as for Oskarshamn 3 PSA, the first version is made by using conservative assumptions. Based on results, most conservative assumptions are replaced by more realistic assumptions in the next phase. Another continuous reason for model revisions is the identification of open questions. Since PSA covers main parts of the process and organisational factors of a nuclear power plant, it is evident that there will be open questions all the time. The review process plays important role in the identification and handling of open questions.

One lesson of this comparison study has been that results presented in a PSA-study should not be regarded as the best estimate of the core damage frequency of the plant. A PSA-study is never complete, and it is too much to require it. There are always open issues and things that have been excluded that can have great influence on the quantitative estimate of the accident frequency. A more reasonable way is to regard a

PSA-study as a document of the ongoing PSA-work at the plant. The scope of the study, conclusions and recommendations are the main issues, not the numerical results.

6.2 Presentation and interpretation of results of PSA

So far, the PSA-studies have been released as paper documents. To produce a user-friendly paper document is a laborious task and perhaps in future the resources should be allocated for the development of smart electronic documentation and presentation system.

The problem with the presentation of results of PSA is partly that PSA provide many kinds of results and partly that there are many kinds of users of PSA. Besides, the presentation of the whole study (scope, method, project) is as important as the results of the quantitative analyses. The documentation of the study should have a structure that supports the needs of different user groups. That could be realised in three levels:

1. Entry
2. Major descriptions of the study
3. Topical reports, analyses

The entry contains a summary of the study and instructions for the user (i.e. the reader) of the study. The reviewed studies had summaries but instructions for the user of PSA could be developed further. One thing to be considered whether several versions of summaries should be written for different user groups such as plant personnel, plant management, safety authorities, journalists, layman. Use of professional writers (e.g. journalists) is recommended to reach an appropriate terminology for layman.

The second level documents consist of

- Presentation and interpretation of results
- Project description
- Assumptions and limitations
- Scope
- Conclusions and recommendations
- Method descriptions, definitions, abbreviations.

Presentation of results should be extensive. Forsmark 3 and Oskarshamn 3 PSAs present results from many sides. If PSA will be updated frequently, it can be burdensome to update this chapter of PSA-documentation. The next stage would be to develop electronic result presentation methods.

Interpretation of results includes explanation of dominating initiating events, accident sequences, minimal cut sets, functions, systems and basic events. In addition, judgements should be made regarding significance of the results. Is the core damage frequency high? How dominating are the most important events, sequences, etc? Role of uncertainties should be discussed. Sensitivity studies and comparisons should be utilised in the interpretation of the results. The sensitivity studies in Forsmark 3 PSA are exemplary.

The PSA-project is usually described quite shortly in the PSA-documentation. A description of the PSA-history would be useful for the reader, as is provided in the beginning of the Oskarshamn 3 study. A description of the quality assurance procedure should be provided as well. The description of the quality assurance process was missing in the reviewed PSA-studies.

Main assumptions and limitations are important to know. We recommend that a summary of assumptions and limitations of each analysis phase is provided as a part of the PSA-documentation.

Scope could be presented in table form regarding which initiating events, operational stages and level of study (level 1 or 2 PSA) are included in the study. A tentative way to summarise the scope of a PSA-study is provided in Appendix 1.

Conclusions and recommendations should be based on presentation and interpretation of results. Since recommendations are intended for different decision-makers, it can be practical to write different versions of recommendations, e.g. one for the internal use at the plant and another one for the public version of the study.

Method descriptions, definitions and abbreviations should be documented separately from the analysis reports. This is the way it has been done in Forsmark 3 and Oskarshamn 3 PSAs.

The third level documents consist of rest of the analysis reports: analysis of initiating events, analysis of system success criteria, systems analyses, data analysis, human reliability analysis, etc.

6.3 Reasons for differences

PSA is a complex and comprehensive analysis. Therefore to explain reasons for various choices made in the analysis is a complicated task. We have chosen the following factors:

- Purpose of the PSA
- Scope of the study
- Methods used
- Use of knowledge regarding systems, functions, phenomena.

In addition, the actual differences between the plants should be accounted. The identification of actual technical and organisational differences between plants is the prerequisite for a comparison of PSA-studies. In this comparison study, the actual differences had significance for human interactions to be credited in the study.

6.3.1 Purpose

The purpose of the study described in the PSA-documentation is usually rather general. Even in this case, the purpose is defined about the same way: to have an up-to-date level 1 (and level 2) study applicable for various living PSA applications. To satisfy the requirements of the safety authority is naturally a very important purpose.

There was one significant difference between the two studies: the one study has a goal to have a similar study as the other unit of the same site. This purpose is significant concerning the choice of methods, scope and level of details in the PSA-model. The other study did not have this kind of reference study.

One lesson in this comparison study is that more detailed purposes or goals for PSA can be found out from documents like decisions made by the plant before the project, documents related to the bidding process, the project plan, evaluation report of the project, utility's PSA-related instructions and PSA-policy documents.

To enhance understanding of the PSA, the chapter describing the purposes should be elaborated as specific as possible. It would be useful to know the background of the project, planned PSA-applications, areas of emphasis and possible couplings with other projects. Typically there are some issues in a PSA-study that have received a lot of attention and detailed analyses have been made in order to resolve the questions, perhaps parallel with the PSA-project. Spin-off effects of these studies should be mentioned.

6.3.2 Scope

Perhaps the most important aspect to be known of PSA is the scope. Differences in the scope always lead to differences in the results. From PSA-documentation one can find lists of initiating events, operating modes, systems credited, manual actions credited. Main assumptions and limitations of the study are usually listed briefly.

There are, however, potential to improve the description of the scope. More specific descriptions would help the comparison of the studies and would help in the evaluation of application areas for a study. Methods to describe the level of details and level of realism of a PSA-study should be developed.

By level of details we mean the resolution level in the model regarding event sequences and fault trees, which issues are modelled as basic events of their own or are represented by joint basic events. Proper descriptions of methods play a key role. Another way to clarify the level of details is to compare with a reference guide, e.g., IAEA guidelines for PSA (ref. 18). More attention should be paid to explaining the exclusions in the study.

Realism is related to the choice of system success criteria, crediting human actions and the choice of failure data. To give an overview of the level of realism may be impossible, but it should be commented in connection with each item in the study, e.g. "this failure probability is based on plant operating experience and that one is a (conservative) screening value".

The scope is rather established for a basic PSA (level 1 analysis of internal initiating events). That's why we did not notice major differences between the studies. We would have presumably identified more differences in a comparison of e.g. analysis of external initiating event or analysis of low power operating modes.

6.3.3 Method

PSA is an integration of several analysis methods. Many methods and tools are standardised and applied in nearly all studies, e.g. event tree-fault tree modelling, and reliability models for the basic events. There are however many areas with methodological differences, such as:

- physical analyses (different codes)
- human reliability analysis (generally)
- systems analysis regarding the level of details
- reliability data estimation (e.g. initiating events)
- integration of level 1 and 2 PSA.

Choice of particular methods should be seen in historical perspective. The influence of SUPER-ASAR work can be seen in these studies compared with the PSAs from 1980's. Both teams chose analyses and data developed in the beginning of 1990's, e.g. for initiating events (ref. 16) and for high-redundant CCFs (ref. 5). However, the study that was performed later revised the method for estimation of initiating event frequencies. The lesson is that not only models but also methods "live" in the PSA-process.

The impact of the method can be difficult to analyse since it can require laborious benchmarking evaluations. In this comparison study, we have compared the two studies mainly qualitatively. Differences were noticed in the methods used for human reliability analysis and for system analyses. These differences have presumably minor importance for the core damage frequency since the related accident sequences are not dominating.

In order to facilitate a review of PSA or a comparison of studies, the methods used should be described precisely. Preferably, clearly defined references should be applied, like internationally published PSA-guidelines and standards.

An area for further studies and development work is the integration of different analyses and models in PSA. Examples of cases where methods need to be integrated is interactions between level 1 and 2 analyses and interactions between HRA and analysis of system success criteria. As in this case, the integration of sub-analyses is not well documented.

6.3.4 Use of knowledge

Knowledge about processes, phenomenon and interactions between them depends on the experience of the analysis team (and supporting plant organisation) as well as resources to be spent for PSA.

Differences in facts can be identified quite easily in a comparison of PSA-studies. A recommendation is to compare PSA-studies and communicate between the plants and analysis teams. This kind of experience exchange can be a valuable addition for the quality of the PSA-study. Experience exchange can, for instance, take place in connection with the peer reviews made by visiting PSA-experts from other plants. This positive side effect of PSA-reviews has been recognised in the PSA quality certifications in USA.

In Sweden, SKI can have a role in experience exchange. In this case, however, Forsmark 3 and Oskarshamn 3 PSA-studies were not reviewed in a comparative manner (Forsmark 3 was reviewed before Oskarshamn 3). SKI's policy has been to review each study as such.

One reason for experience exchange is to save resources in the physical analyses. The compared studies have in practice identical FSARs and thus the deterministic basis for the studies is same.

Concerning the use of FSAR or other previous references there are two things to be decided by the analysis teams. One question is whether to rely on previous assumptions or to check their validity. Another question is to decide in which items it is worth removing conservatism identified in the previous assumptions. It is often an economical question how much resource is put to resolve the issues. A recommendation is that this decision making process is documented including motives for choosing or rejecting various references since it is valuable for the further generations.

In this comparison study, we find differences in assumptions concerning Common Cause Initiators and system success criteria. The other team made more studies concerning systems success criteria for core cooling and residual heat removal. During the PSA-project, the analysis teams did not co-operate, and only few information exchange took place. The natural reason for this was that the Forsmark 3 study was finished before the Oskarshamn 3 PSA-project was initiated. The project teams have discussed differences later and this had led to modifications in the studies.

6.4 Harmonisation of the methodology

Harmonisation of the PSA-methodology has benefits but also drawbacks. The main benefits are to facilitate the review of studies and to facilitate the comparison of the studies. The drawback is that a harmonisation may suppress the development of the methodology. Needs for harmonisation should be discussed together with needs for development.

Based on this comparison study, we recommend harmonisation in the presentation and documentation of PSA-studies as well as harmonisation of certain key definitions. These are:

- Presentation of results. There should be some general guidelines how to present the main results of a PSA-study.
- Presentation of methods, scope, main limitations and assumptions.
- Definitions of end states, above all for core damage.
- Definitions of initiating events (this was not a problem in this comparison study).
- Definitions of common cause failures. How to assume common cause failures is a generic problem and the PSA-community should seek for a common view on the subject.

One point in the harmonisation is that at which level it is made. The highest level is an international consensus on principles and methods. At the national or regional level (e.g. European Community) some harmonisation is natural due to regulatory requirements. On the other hand, utilities can agree about the level of scope and details. Besides the

regulatory requirements, the harmonisation process is voluntary for the utilities and depends on the attitude in the utility, i.e., is following whether the state-of-the-art methodology and PSA-standards are seen important or not.

The lowest level of harmonisation takes place within a utility. This goal was clearly defined for the other utility in this comparison study. The benefit with this harmonisation is that the utility can compare the units with the aid of PSA.

Harmonisation should follow the experience from the use of studies and results from the research and development work.

6.5 Review of PSA

Review of PSA takes place in three stages: 1) internal review of the project, 2) independent review by the client (the utility), and 3) review by the safety authorities. The content of each stage varies between PSA-projects and countries. These QA-activities should be specified in the QA programme for PSA so that they are taken into account in the planning and accomplishment of the PSA-project.

The objectives and basis for the review must be specified. By objectives we mean that the reviewers need to know what is expected from the review. The basis defines the parts of PSA to be reviewed. For instance, it can be specified that, at certain stage, FMEAs and minimal cut sets are reviewed but not fault trees. This is important information for the next review stages. At any review stage, the reviewer should have access to same material as the PSA-analysts.

The problem with present PSA-studies is that they are so complex and detailed that a thorough review of a study is a laborious task. The developed PSA review standards can be applied for a general validation of a study (peer review) (ref. 19, 20, 21), but that is not enough. The resource spent for quality review should be in relation with work spent for the study itself.

The two compared PSA-projects had slightly different approaches regarding use of independent reviewers. In one project, the independent reviewer gave comments during the project. In the other project, reviews were made between different project phases. In any case, our impression is that the studies of this comparison study could have been reviewed more closely since we found several errors in the studies. Typical errors found are inconsistencies in the documentation and model, and the natural reason for this type of errors is the living analysis process.

7 Recommendations

7.1 Performance of PSA

Performance of PSA is directed in regulatory requirements and in state-of-the-art PSA-guidelines. There is general understanding what should be included in a level 1 and 2 PSA, but there are also open items, e.g., related to area events and external events. These questions are related to overall requirements for safety analyses for a nuclear power plant, and they are not discussed in this context.

The recommendation here is that the analysis team and the future user of the study (the power plant) should carefully plan the end product in the beginning of the project. Forsmark 3 and Oskarshamn 3 PSAs have good features but improvements can be made. See also discussion in the chapter 0 concerning presentation of the study. One important stage is the release of the study, and resources should be allocated for introducing the new/updated study for the plant personnel.

Regarding the work methods and analysis methods, the recommendation is to follow clearly defined references. The advantage with this is to facilitate the review process as well as to reduce the need for documentation. Naturally own development work can be needed in specific issues, and that should be encouraged. However, established definitions should be used.

An important question is the level of realism and details that should be required. The trend is to try to have as realistic PSAs as possible, which is even formulated as required by SKI (ref. 7). This kind of goal has increased the complexity of PSA-studies by the natural reason that nuclear power plant processes are complex. The problem is that the performance of PSA costs more, it is more difficult to review and validate the study and it is more difficult to understand the results. A recommendation is that the requirement concerning realism and details of a PSA-study should be elaborated and specified. A detailed study need not be more realistic than a less detailed study, e.g., because there may be no data for the estimation of probabilities of various failure modes.

We compared two basic level 1 PSAs. A recommendation is to compare level 2 PSAs, analyses of area events and low power PSAs. These comparisons would presumably rise other types of methodological questions than our comparison of basic PSAs.

7.2 Presentation and interpretation of results of PSA

In Section 0, we outlined a structure for the documentation of PSA. A recommendation is that electronic documentation methods should be developed for the management and use of PSA-documents.

An electronic documentation system could also facilitate versatile presentation of results. For instance, the user can choose type of lists and diagrams from a set of alternatives. To some extent, present PSA computer codes provide possibilities for various presentations, but development and perhaps other tools, dedicated for result presentation, are needed.

We recommend certain harmonisation for the presentation of the results. It helps comparison of studies. The following items should be a part of the result presentation:

- Goal and purpose with the study
- Status of the study (revision number and date, history)
- Scope (initiating events, operational states, consequences, systems credited, human actions analysed)
- Main results (core damage frequencies per initiating events and per core damage category, safety margins i.e. conditional core damage probability given an initiating event, initiating event frequencies)
- Dominating minimal cut sets, sequences, initiating events, human errors

- Risk importance measures for basic events, systems and human errors
- Analysis of uncertainties and sensitivities
- Discussion (interpretation of the results)
- Conclusions and recommendations.

Appendix 1 provides examples of summarising the scope of PSA. A question for the reader of this report is whether he/she can understand the differences between the compared studies based on the tables in appendix 1. Another question is whether the table can give a rough guidance on areas to be developed in the next phase of the PSA-project.

One recommendation for harmonisation is definitions for initiating events and core damage categories. Forsmark 3 and Oskarshamn 3 have categorised core damages differently, which makes the comparison of the results difficult.

Interpretation of the results should include explanation of dominating initiating events, sequences, cut sets and basic events in plain text. Comparison against safety goals and discussion about uncertainties in the analysis should be made. For instance, if the core damage frequency is higher than 1E-5/reactor-year, then why. Do conservative assumptions contribute to core damage frequency and how much? Have some initiating events or operational states been excluded? Have operator recoveries been accounted?

Figures and diagrams are illustrative. However, one should choose carefully appropriate scales and forms of diagram. The relative importance between the presented items looks in an absolute scale totally different from the logarithmic scale.

7.3 Use of PSA

Methods for validation of PSA for different application areas should be developed. The development of various standards (ASME, BWR Owner's Group, etc.) aims at this purpose. However, it is also emphasised that a review based on a standard can provide just a general quality grade for a PSA. The real feasibility of PSA can be evaluated only after experience from numerous applications.

Based on this comparison study, it can be said that in any application consultation with the expert of the specific study is needed. For a person that has not participated in a PSA-project, is usually difficult understand all features that should be accounted for in a PSA-application. The document and model are seldom good enough but discussion with the analysts is needed. The analysts need feedback from the users of PSA.

One important question is whether we should use probabilistic safety goals. One problem with these goals is that the scope and level of realism differ between the studies. If we define a safety goal “core damage frequency less than 1E-5/year”, should external initiating events and area events (fire) be included in this evaluation? How about core damage risk for low operating mode? One alternative is to define criteria for comparisons, e.g. for the evaluation of plant modifications. There is still the same problem with the scope of the study.

Because of the present state of the art of PSA, the use of probabilistic safety goals should be restricted to discuss the results of PSA made for internal initiating events (LOCA and transients). Analysis of area events and external events include

considerably more uncertainties which are handled partly by using conservative assumptions partly by excluding issues from the study. Status of those PSAs is not yet mature to be compared with PSA for internal initiating events.

8 Conclusions

The comparison of the two PSA-studies shows that comparison of PSA results from different plants is normally not meaningful. It takes a very deep knowledge of the PSA studies to make a comparison of the results and usually one has to ensure that the compared studies have the same scope and are based on the same analysis methods.

PSA is an enormous mathematical model based on technical descriptions of systems, experience and data, interpretations of data, engineering judgements and use of various physical models. The analysis process is sensitive to many factors, not all controllable for the analysis team.

A PSA-study is never complete. There are always open issues and things that have been excluded that can have great influence on the quantitative estimate of the accident frequency. The results presented and conclusions drawn in one version can be changed to the next version. The history of the study and the status of the PSA-programme of the plant should be known when reviewing the study. Therefore the results presented should not be regarded as the best estimate of the core damage frequency of the plant. A more reasonable way is to regard the PSA-study as a document of the ongoing PSA-work at the plant. The scope of the study, conclusions and recommendations are the main issues, not the numerical results.

There are several areas in the PSA-methodology that should be harmonised. This would facilitate the review of the studies as well as comparison of the studies. Thus it would lead to better quality. Such areas are e.g. presentation of results, presentation of methods, scope, main limitations and assumptions, definitions for end states (core damage categories), definitions of initiating events, definitions of common cause failures. Harmonisation should follow the experience from the use of studies and results from the research and development work.

Methods for validation of PSA for different application areas should be developed. The developed PSA review standards can be applied for a general validation of a study. However, the present PSA-studies are so complex that quality reviews should be detailed.

The most important way to evaluate the real feasibility of PSA can take place only with practical applications, such as

- evaluation of allowed outage times and test intervals in the Safety Technical Specifications
- analysis of operating experience (occurred safety-related events)
- analysis of plant design modifications.

In any application consultation with the PSA-expert is needed. For a person that has not participated in a PSA-project, it is usually difficult to understand all features that should be taken into account in a PSA-application. The document and model are seldom good enough but discussion with the analysts is needed. Even then, the PSA-documentation

and models can be developed to facilitate the communication between PSA-experts and users.

Another important aspect in the applications is the role of PSA together with other analyses such as deterministic safety analysis and analysis of man-machine-organisation aspects. Again the communication between different views plays the key role as well as the pedagogic presentation of basis, methods, data and results in each approach.

Many real uncertainties can be identified by comparing PSAs. Generally, comparisons are recommended as a method to review the quality of a PSA-study and as a method to analyse uncertainties of the study.

9 References

1 Reactor Safety Study, An Assessment of Accident Risks In U.S. Commerical Nuclear Power Plants. Report WASH-1400 (NUREG-75/014), U.S. Nuclear Regulatory Commission, Washington D.C., 1975.

2 ASAR 90 — SKI-direktiv. SKI-UA-014/90, 1991-03-27. (In Swedish)

3 Projekt SUPER-ASAR. Slutrapport FAS I. Report SKI TR-90:3, Stockholm, 1990. (In Swedish)

4 Projekt SUPER-ASAR. Slutrapport FAS II. Report SKI TR-90:4, Stockholm, 1990. (In Swedish)

5 Mankamo, T., Björe, S., Olsson, L. CCF Analysis of High Redundancy Systems. Safety/relief Valve Data Analysis and Reference BWR Applications. Report SKI 91:6, Stockholm, 1992.

6 ASAR 80 — SKI-direktiv. Enligt SKIs anslagsframställan 1983/84, 1982-08-20. (In Swedish)

7 Statens kärnkraftinspektions föreskrift om säkerhet i vissa kärntekniska anläggningar, SKIFS 1998:01. (In Swedish)

8 Säkerhetsstudie Forsmark 3. Report Ds I 1978:3, Industridepartementet, Energikommissionen, 1977. (In Swedish)

9 Forsmark 3 — säkerhetsstudie. Report PK-15/87, Vattenfall, 1987. (In Swedish)

10 Forsmark 3 — Säkerhetsstudie — Effektdrift. Report R-dok 950-PSA, FKA, 1995. (In Swedish)

11 Forsmark 3. Riskanalys/redovisning avseende yttre händelser. Report GES 43/96. Vattenfall Energisystem, 1996. (In Swedish)

12 Forsmark 3. Säkerhet under avställningar. Förstudie för ned-/uppgång samt kall avställd reaktor. Report NTC 94-181, ABB Atom, 1995. (In Swedish)

13 OKG - STA - OIII. Systematisk tillförlitlighetsanalys. Lägesrapport 1984. OKG, 1984. (In Swedish)

14 Systematisk tillförlitlighetsanalys Oskarshamnverket 3 1986. OKG, 1986.

15 T-book. Reliability Data of Components in Nordic Nuclear Power Plants. 4th edition. The TUD Office, Vattenfall Energisystem AB, 1996.

16 I-book. Initiating events at the Nordic Nuclear Power Plants. 2nd edition. SKI report 94:12. Stockholm, 1994. (In Swedish)

17 Swain, A.D. & Guttmann, H. E. 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Sandia National Laboratories, USA.

18 IAEA Safety Series No. 50-P-4, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)

19 PSA Applications Guide. Report EPRI TR-105395, Palo Alto, CA, USA, 1995.

20 A framework for a quality assurance programme for PSA. Report IAEA-TECDOC-1101, Vienna, 1999.

21 Standard for probabilistic safety assessment for nuclear power plant applications. A proposed American National Standard (ANS), Rev 12 May 30, 2000.

APPENDIX 1. Presentation of the scope of the compared PSA-studies

Plant A, level 1 PSA for internal initiating events

Sources of radioactive materials	Core
Operational states	Power operation • Full power, normal configuration, reactor-year = 337 days Planned shutdown analysed as one transient category
Accident end states	Core damage categories • Failed shutdown • Loss of core cooling • Loss of residual heat removal Other accident end states • Cold overpressurisation (overfilling) of RPV • Overpressurisation (fast) of RPV • Depressurisation of RPV
Initiating events	
Identification and categorisation	Internal LOCA: • DN>50mm (system 354 DN>25mm) in RCPB • 1) Large 2) Medium, top, 3) Medium, bottom, 4) Small LOCA • secondary and dynamic effects External LOCA: Systems 311, 312, 321/331, 354 Interfacing system LOCA: No system identified Transients: based on SUPER-ASAR recommendations Common Cause Initiators: 1) spurious reactor protection signals 2) loss of support systems, 3) loss of offsite power, 4) spurious process measurement signals (no CCI identified), 5) loss of electrical systems
Frequencies	Internal LOCA: WASH-1400 frequencies distributed between components External LOCA: screening values Transients: plant operating experience Common Cause Initiators: • support systems: screening values • spurious signals: screening values • loss of offsite power: plant operating experience • electrical systems: fault tree analysis with T-book data

System success criteria	
Controlled end state	20 hours mission time, cold subcritical reactor
Analyses made for PSA (rest from FSAR)	Reactivity control regarding control rods Reactor pressure control (BISON), except regarding overfilling of RPV (FSAR) Core cooling (MAAP) Decay heat removal regarding 322/712/721 (MAAP)
Systems analyses	
Front systems (system numbers in parentheses)	Reactivity control: control rods (221/222), boron system (351), hydraulic scram (354), screw insertion (532), recirculation pumps (649/313) Reactor pressure control: safety relief valves (314), condenser (461), steam lines regarding protection of overfilling of reactor vessel (311) Core cooling: feedwater system (312/463), auxiliary feedwater system (327), core spray system/depressurisation (323/314) Decay heat removal: condensation system (316), shutdown cooling system (321/331), containment vessel spray system (322), secondary feedwater system (328), firefighting water system (322O/861), containment filtered venting (362), condenser (461/462/463)
Support systems (system numbers in parentheses)	I&C: reactor protection system (516) Electrical systems: house turbine operation, general 10 kV, 660V, 380V systems (641, 643. 644, 645, 646), diesel-generator and its support system (653) diesel-backed systems (661, 662, 663, 666), DC systems (671, 672, 673), battery-backed AC system (677) Support system for turbine condenser and feedwater system: 421, 424, 441, 452 Cooling and service water systems: 712, 713, 714, 721, 722, 723, 724, 735, 861 Room ventilation: 727 Compressed air and nitrogen systems: 751, 753, 754
Human reliability analysis	
Actions before initiating events	Erroneous ground states Unavailability caused by reparation, test and reparation
Actions causing initiating events	Excluded
Actions after initiating events	Errors of omission and recoveries, actions identified in the survey of EOPs
Human error probabilities	Expert judgements based on the method
Common Cause Failures	
Assumptions	Identical active components in redundant trains of a same system Spurious stop of pumps and diesel-generators
Data	SUPER-ASAR regarding low-redundant systems Analysis of LERs and SKI research project regarding high-redundant systems
Failure data	
Component failure rates	T-book version 4 Tillgänglighetsstudien i Forsmark 1979 IEEE, 1993
Repair time of critical failures	AOT
Repair time of non-critical failures	failure rate = failure rate for critical failures repair time = AOT
Planned maintenance outages	AOT

Plant B, level 1 PSA for internal initiating events

Sources of radioactive materials	Core
Operational states	Power operation • Full power, normal configuration Planned shutdown analysed as one transient category
Accident end states	Core damage categories • Failed shutdown or loss of core cooling • Loss of residual heat removal with feedwater from condensation pool Other accident end states • Loss of residual heat removal with feedwater from external source • Overpressurisation of the reactor pressure vessel, analysed further
Initiating events	
Identification and categorisation	Internal LOCA: • Based on I-book: 1) Large 2) Medium or small LOCA, 3) RPV rupture External LOCA: Systems 311, 312, 321, 323, 327 Interfacing system LOCA: System 321 Transients: based on SUPER-ASAR recommendations Common Cause Initiators: 1) loss of water level measurement in RPV (not modelled), 2) loss of support systems, 3) loss of electrical systems, 4) loss of offsite power (included in Transients)
Frequencies	Internal LOCA: WASH-1400 frequencies distributed between components External LOCA: WASH-1400 Interfacing system LOCA: systems analysis Transients: plant operating experience (I-book) Common Cause Initiators: • support systems: fault tree analysis with T-book data • loss of offsite power: plant operating experience
System success criteria	
Controlled end state	24 hours mission time, subcritical reactor in warm, xenon-free conditions
Analyses made for PSA (rest from FSAR)	Reactivity control regarding control rods (POLCA) Core cooling (MAAP), except regarding 314-depressurisation (FSAR) 733/735 water inventory for feedwater system in LOCA H-room cooling
Systems analyses	
Front systems (system numbers in parentheses)	Reactivity control: control rods (221/222), hydraulic scram (354), screw insertion (532), recirculation pumps (649/313) Reactor pressure control: safety relief valves (314), condenser (461) Core cooling: feedwater system (312/463), auxiliary feedwater system (327), core spray system/depressurisation (323/314) Decay heat removal: condensation system (316), shutdown cooling system (321/331), containment vessel spray system (322), condenser (461/462/463)
Support systems (system numbers in parentheses)	I&C: reactor protection system (516) Electrical systems: house turbine operation, gas turbine, general 10 kV, 660V, 380V systems (641, 643. 644, 645, 646), diesel-generator and its support system (653) diesel-backed systems (661, 662, 663, 666), DC systems (671, 672, 673), battery-backed AC system (677) Cooling and service water systems: 712, 713, 714, 721, 722, 723, 724, 733, 735 Room ventilation: 727 Compressed air and nitrogen systems: 751, 753, 754

Human reliability analysis	
Actions before initiating events	Erroneous ground states Unavailability caused by reparation, test and reparation
Actions causing initiating events	Excluded
Actions after initiating events	Errors of omission
Human error probabilities	Expert judgements based on the method
Common Cause Failures	
Assumptions	Identical active components in redundant trains of a same system
Data	SUPER-ASAR regarding low-redundant systems SKI research project regarding high-redundant systems
Failure data	
Component failure rates	T-book version 3
Repair time of critical failures	T-book repair times
Repair time of non-critical failures	Excluded
Planned maintenance outages	AOT

Bibliographic Data Sheet **NKS-36**

Title	Experience from the comparison of two PSA-studies
Author(s)	Jan Holmberg & Urho Pulkkinen
Affiliation(s)	VTT Automation
ISBN	87-7893-087-1
Date	March 2001
Project	NKS/SOS-2.3
No. of pages	40 + appendix 4
No. of tables	11
No. of references	21

Abstract

Two probabilistic safety assessments (PSA) made for nearly identical reactors units (Forsmark 3 and Oskarshamn 3) have been compared. Two different analysis teams made the PSAs, and the analyses became quite different. The goal of the study is to identify, clarify and explain differences between PSA-studies. The purpose is to understand limitations and uncertainties in PSA, to explain reasons for differences between PSA-studies, and to give recommendations for comparison of PSA-studies and for improving the PSA-methodology.

The reviews have been made by reading PSA-documentation, using the computer model and interviewing persons involved in the projects. The method and findings have been discussed within the project group. Both the PSA-projects and various parts in the PSA-model have been reviewed. A major finding was that the two projects had different purposes and thus had different resources, scope and even methods in their study.

The study shows that comparison of PSA results from different plants is normally not meaningful. It takes a very deep knowledge of the PSA studies to make a comparison of the results and usually one has to ensure that the compared studies have the same scope and are based on the same analysis methods.

Harmonisation of the PSA-methodology is recommended in the presentation of results, presentation of methods, scope, main limitations and assumptions, and definitions for end states, initiating events and common cause failures. This would facilitate the comparison of the studies.

Methods for validation of PSA for different application areas should be developed. The developed PSA review standards can be applied for a general validation of a study. The most important way to evaluate the real feasibility of PSA can take place only with practical applications.

The PSA-documentation and models can be developed to facilitate the communication between PSA-experts and users. In any application consultation with the PSA-expert is however needed.

Many real uncertainties can be identified by comparing PSAs. Generally, comparisons are recommended as a method to review the quality of a PSA-study and as a method to analyse uncertainties of the study.

Key words Review of PSA, quality of risk analysis, uncertainty analysis

Available on request from the NKS Secretariat, P.O.Box 30, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@catscience.dk, www.nks.org.