Unclassified **NEA/CSNI/R(2007)12**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

14-Nov-2007

English text only

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2007)12
Unclassified

USE AND DEVELOPMENT OF PROBABILISTIC SAFETY ASSESSMENT

CSNI WGRISK

English text only

JT03235946

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

* * *

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

– to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
– to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made of senior scientists and engineers, with broad responsibilities for safety technology and research programmes, and representatives from regulatory authorities. It was set up in 1973 to develop and co-ordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations.

The committee's purpose is to foster international co-operation in nuclear safety amongst the OECD member countries. The CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulatory organisations; to review operating experience and the state of knowledge on selected topics of nuclear safety technology and safety assessment; to initiate and conduct programmes to overcome discrepancies, develop improvements and research consensus on technical issues; to promote the co-ordination of work that serve maintaining competence in the nuclear safety matters, including the establishment of joint undertakings.

The committee shall focus primarily on existing power reactors and other nuclear installations; it shall also consider the safety implications of scientific and technical developments of new reactor designs.

In implementing its programme, the CSNI establishes co-operate mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA) responsible for the programme of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH), NEA's Radioactive Waste Management Committee (RWMC) and the NEA's Nuclear Science Committee (NSC) on matters of common interest.

The Use and Development of Probabilistic Safety Assessment

Executive Summary

Background

The CSNI WGRISK produced a report in July 2002 on "The Use and Development of Probabilistic Safety Assessment in NEA Member Countries". This provides a description of the PSA programmes in the member countries at the time that the report was produced. However, there have been significant developments in PSA since 2002. Consequently, a decision was made at the WGRISK meeting in October 2005 to produce an updated version of the report. This was agreed by CSNI at their meeting in December 2005.

Objective

The aim of the Task was to produce an updated, stand alone version of the report that presents an analysis of the position on the use and development of PSA in the WGRISK member countries as of spring 2006. The Task was carried out in cooperation with the IAEA. This has led to more information and will thus provide a better overview on PSA worldwide. The expected readers of the report are PSA professionals and generalists dealing with risk and safety management.

Process

A detailed questionnaire was circulated to WGRISK members and to the IAEA to ascertain the state of the art in PSA use and development at the end of 2006. Detailed responses were prepared by 20 countries totalling several hundred pages of information. After first compilation of information, an updating round was organized by showing to the countries all the answers and the summary made of them by a small group of experts. The process led to some clarifications and more consistency in the report. The collected information was finally analyzed and summarized to reach the conclusions presented below.

Separately, short summaries were prepared for each of the following sections of the report thus helping a reader to get an overview of those areas: PSA Framework and Environment; Numerical Safety Criteria; PSA Standards and Guidance; Status and Scope of PSA Programmes; PSA Methodology and Data; PSA Applications; Results and Insights from the PSAs; and Future Developments.

Conclusions

- The overall environment for the use of PSA in regulatory and licensee decision-making is quite positive in all countries that provided information. In most cases the regulatory system encourages the performance of PSAs to provide information to complement and support the defence in depth philosophy used by most regulatory bodies, and to aid in operational configuration decisions. PSA results and analyses can play a key role in developing new regulatory requirements.

- The performance of a PSA is a formal regulatory requirement in many countries. Most countries that require a Periodic Safety Review be conducted on operating plants as part of their regulatory system (in accordance with IAEA Safety Standards) also require that a PSA be performed as part of these Periodic Safety Reviews.

- The interval for major PSA updates varies from three to ten years. In countries where a formal Periodic Safety Review is not performed, updates are made as necessary or when the PSA is used to support a regulatory action. Small updates or PSA extensions are often made to support specific safety cases.

- There are differences in the status of the numerical safety criteria that have been defined in different countries, reflecting differences in regulatory systems. Some have been defined in law and are mandatory, some have been defined by the regulatory authority (which is the case in the majority of countries where numerical safety criteria have been defined), some have been defined by an authoritative body such as a Presidents Commission and some have been defined by plant operators or designers. The differences include: the status of the criteria – that is whether they are mandatory or provide formal or informal guidance only: the way that the risk metrics have been defined and how they would be calculated: whether the criteria have been defined as limits or objectives, and differences in the numerical values cited.

- The work carried out so far has not addressed technical basis for the way that the criteria have been defined and the other reasons for the differences. This will be addressed by a specific WGRISK Task Force which has been set up in 2006.

- All operating nuclear power plants in the reporting countries have been studied using PSA methods. A Level 1 internal events PSA has been performed on all plants. In many cases, this has been extended to a Level 1+ or Level 2 PSA. In several cases, the Level 2 PSA consists mainly in the determination of the Large Early Release Frequency (LERF), rather than a complete Level 2 analysis of plant damage states.

- In several cases, the Level 1 PSAs have been extended to consider low power and shutdown events. External events, such as earthquakes, high winds, floods, and internal fires and other external or area events, as necessary, depending on the site are being factored into the basic PSA analyses in several countries or have already been considered. Only a few level 3 PSAs have been performed. They have typically been used to develop insights into the societal risk of a class of plants.

- The main application of the PSA has been for design evaluation where the insights from the PSA have been used in combination with the insights from the deterministic analysis in a risk-informed approach. The PSA has mostly been used to: identify the dominant contributions to the risk (CDF and LERF); identify weaknesses in the design and operation of the plant, and to determine whether the design is balanced. This has been done at the design stage for new plants or during periodic safety reviews for existing plants.

- Other general applications areas of PSA are: event analysis with aid of PSA; evaluation of Technical Specifications; training of operators and plant staff; accident management; emergency planning; risk-informed in-service inspection; risk monitoring and configuration planning; risk informed decisions dealing with plant structures, systems and components, and risk-informed regulation.

- There are many instances of where the PSA has identified weaknesses where plant improvements have been made. It has also been used to compare the options for design or operational changes to determine the relative reductions in risk that they would give, to develop accident management strategies, as well as for operator training.

- While the PSA methodology is reasonably robust in most areas, additional research is needed and in progress in several areas. In some cases this research is conducted to improve the efficiency of the PSA process. In other cases, it is performed to reduce the uncertainties associated with PSA results, thus making it easier to use the results and analyses in a regulatory environment or to change operational practices.

- Key areas of research in progress include the following: human reliability analysis, digital instrumentation and control, fire and flood risk, earthquakes, external off-site hazards, level 2 PSA methods, data analyses, common cause failures, uncertainty analysis, aging, and reliability of passive systems.

- WGRISK will use the results of this report to monitor the conduct of its ongoing research activities, and to promote and implement new international collaborative efforts within the framework of the CSNI.

Foreword

This report is a product of a numerous persons from all the contributing countries, and they all deserve a very special expression of gratitude for their work. The country contact persons are listed at the end of this report in Appendix B.

Some individuals helped among the national officers to produce the executive summary and the summaries of each section. These persons are in alphabetical order Dr. Jeanne-Marie Lanore (FRA), Dr. Joseph A. Murphy (USA) an, Dr. Charles Shepherd (GBR).

The NEA responsible administrator was Dr. Pekka T. Pyy and the administrative assistant Mrs. Elisabeth Mauny.

Table of Contents

1 INTRODUCTION

1.1 General

WGRISK produced a report in July 2002 on “The Use and Development of Probabilistic Safety Assessment in NEA Member Countries” – NEA/CSNI/R(2002)18. The report is available on the NEA website at: http://home.nea.fr/html/nsd/docs/2002/csni-r2002-18.pdf, and it provides a description of the PSA programmes in the WGRISK member countries at that time. However, the presentations made at subsequent WGRISK meetings have indicated that there have been significant developments in PSA since then. Consequently, a decision was made at the Annual Meeting in October 2005 to produce an updated version of the report. This was agreed by CSNI at their meeting in December 2005.

1.2 Objective and Scope of the work

The aim of the Task was to produce an updated, stand alone version of the report that reflects the position on the use and development of PSA in the member countries as of spring 2006. The Task has been carried out in cooperation with IAEA to increase the information content and thus provide a better overview on PSA worldwide. The expected readers of the report are PSA professionals and generalists dealing with risk and safety management.

The scope of the new report and the information requested from the member countries is broadly the same as that required for the previous report NEA/CSNI/R(2002)18. However, to provide greater clarity in the presentation of the information, the new report will have additional sections dealing with: PSA standards and guidance; PSA methodology and data; results and insights from the PSA, and future developments.

This report addresses the PSAs for power reactors only. It is not intended to address the PSAs for research reactors or for non-reactor nuclear facilities such as nuclear fuel fabrication facilities, reprocessing facilities and radioactive waste storage facilities in this initial report.

The countries participating in the work by replying to the questionnaire were: USA, UK, Chinese Taipei (denoted consistently by acronym “Taiwan” later in this report), Switzerland, Sweden, Spain, Slovenia, Slovak Republic, The Netherlands, Mexico, Korea, Japan, Italy, Hungary, Germany, France, Finland, Czech Republic, Canada, Belgium. The overview situation of the national PSA studies is given in Appendix A and the contact persons in Appendix B.

1.3 Format of the report

To ensure that the information from the member countries is presented in the report in a consistent way and to a common level of detail, the section headings that authors should use in providing the information were given to them along with guidance on what information should be provided. This guidance (reporting template) is presented in Appendix C.

The information provided should have reflected the different types of reactors/ utilities/ sites/ etc. However, the principal aim was to determine what the current best practices are in the use and development of PSA. The information provided by authors should relate to the most recent developments and trends in their country. In order to achieve an overview of the situation, summaries were written for each section of the report. Respectively, the country replies are presented for each section in reverse alphabetical order. PSA and PRA are used as synonyms for in replies.

The set of section headings in the report is, consequently, thus as follows:

Executive summary
1. Introduction
2. PSA Framework and Environment
3. Numerical Safety Criteria
4. PSA Standards and Guidance
5. Status and Scope of PSA Programmes
6. PSA Methodology and Data
7. PSA Applications
8. Results and Insights from the PSAs
9. Future Developments
10. References

Appendix A: Overview of the Status of PSA Programmes
Appendix B: Contact information
Appendix C: Questionnaire and Guidance to authors

1.4 Process followed in the work

The request for information was the first step in producing the updated report. Member countries were asked to provide a description of the current position on the use and development of PSA in their country as of 2006. The information was provided in electronic form using the section headings given in Appendix C and to the level of detail indicated in this appendix. The number of replies was limited to one per country.

It is recognised that some of the information that was presented in NEA/CSNI/R(2002)18 still is current in many cases – for example, this may be the situation with regard to the sections relating to the regulatory framework, the need to produce a PSA and numerical safety criteria. However, the aim was to produce a stand alone report where the reader does not need to continually refer back to the earlier report. Hence, in preparing their replies, authors were requested to copy the information from the earlier report into the current report and edit it as necessary.

The member countries sent their information during the summer 2006. During the autumn 2006, summaries for various areas (sections) were prepared by experts and sent back to the countries with attached replies. This gave an opportunity to the countries to iterate their replies during the winter 2006-2007. Also, a discussion was organised during the 2006 and 2007 WGRISK annual meetings in order to draw the most important lessons and trends from the country replies and to correct potential biases.

2 PSA FRAMEWORK AND ENVIRONMENT

2.1 Summary

The overall environment for the use of PSA in regulatory decision-making is quite positive in all countries that provided information. In some countries, the performance of a PSA by a licensee has not been a legal requirement of the regulatory system for a specific regulatory action, e.g., France, USA. However, in most cases the regulatory system encourages the performance of PSAs to provide information to complement and support the defence-in-depth philosophy used by most regulatory bodies, and to aid in operational configuration decisions. In some cases, PSA results and analyses play a key role in developing new regulatory requirements even though they may be deterministic in nature or may arise from the continuing dialogue between the regulator and the plant operator. This is particularly the case in countries that use a “cost/benefit” or “As Low as Reasonably Practical” approach to develop new regulations. (Examples include the United Kingdom and the USA in this regard.) The availability of a PSA is often a considerable aid to the plant operators and to regulators interpreting operational configurations and the significance of actual operating events. In many cases, living PSA models are used by the plant staff and/or regulators, or simplified PSA models are used to make an initial assessment.

The performance of a PSA is a formal regulatory requirement in many countries. For many, this is done through the requirement that a Periodic Safety Review be conducted on operating plants as part of their regulatory system (in accordance with IAEA Safety Standards) and the companion requirement that a PSA be performed as part of these Periodic Safety Reviews. In other instances, the requirement for PSA analysis is an integral portion of the regulatory structure; e.g., Canada, United Kingdom. In some countries, the use of PSA by licensees seeking regulatory change is voluntary. However, once that choice is made, substantial guidance is available on the nature of the analysis required and acceptable analytical results (e.g., USA).

In some cases where the fleet of operating reactors is highly standardized, reference studies may have been used to represent a class of several nuclear power plants to some extent in these PSA studies, rather than specific studies of individual facilities. (Examples include France and Hungary.) For new plants, particularly those of advanced design, most countries are formally requiring that a PSA be performed.

Most of the completed PSAs and those PSAs in progress have been performed by the operators of the plants. However, several PSAs have been performed by the regulators (or their Technical Support Organizations (TSOs)) as projects to advance the state of the art, to identify weaknesses in design or operational practices, to support specific regulatory actions and to ensure the regulatory body has the requisite knowledge of the strengths and weaknesses of the methods used. In several cases, the PSA models are provided to the regulatory body (or their TSO), so that the regulator may become familiar with their use and be able to make independent assessments, as needed; e.g., Canada, Netherlands and Belgium. When the PSA is conducted by the regulatory body, considerable cooperation is required from the plant owner/operator or detailed design information and knowledge of operational practices. In some instances, the PSA is essentially a cooperative effort between the regulatory body and the plant owner/operator. Examples here include some of the PSA efforts in France and Taiwan.

2.2 Country replies

2.2.1 USA

The PRA Policy Statement

The U.S. Nuclear Regulatory Commission (NRC) has for many years developed and adapted methods for doing probabilistic safety assessments (PSAs) (generally referred to as probabilistic risk assessments - PRAs - in U.S. applications) to better understand risks from licensed activities. The NRC has supported development of the science, the calculation tools, the experimental results, and the guidance necessary and sufficient to provide a basis for risk-informed regulation. By the mid-1990s, the NRC had a sufficient basis to support a broad range of regulatory activities. The Commission's 1995 PRA Policy Statement provides the following guidance on risk-informing regulatory activities:

> "(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.
>
> (2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109[1] (Backfit Rule). Appropriate procedures for including PRA in the process for changing regulatory requirements should be developed and followed. It is, of course, understood that the intent of this policy is that existing rules and regulations shall be complied with unless these rules and regulations are revised.
>
> (3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.
>
> (4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plants licensees."

The Commission also said:

> "Given the dissimilarities in the nature and consequences of the use of nuclear materials in reactors, industrial situations, waste disposal facilities, and medical applications, the Commission recognizes that a single approach for incorporating risk analyses into the regulatory process is not appropriate. However, PRA methods and insights will be broadly applied to ensure that the best use is made of available techniques to foster consistency in NRC risk-based decision-making."

In issuing the policy statement, the Commission said it expected that implementation of the policy statement would improve the regulatory process in three ways: by incorporating PSA insights in regulatory decisions, by conserving agency resources, and by reducing unnecessary burden on licensees. The movement toward risk-informed regulation has indeed sharpened the agency's (and,

---

[1] Code of Federal Regulations, Title 10, Part 50.109, "Backfitting."

therefore, the licensees') focus on safety, reduced unnecessary regulatory burden, and an effective, efficient regulatory process. A collateral benefit is the opportunity to update the technical bases of the regulations to reflect advances in knowledge and methods and decades of operating experience. In line with the NRC's goal of increasing public confidence, the agency has developed its approach to risk-informed regulation openly, giving the public and the nuclear industry clear and accurate information and a meaningful role in the process.

Risk-informed Regulation

In 1998 the agency formally defined risk-informed regulation as an approach to regulatory decision making that uses risk insights as well as traditional considerations to focus regulatory and licensee attention on design and operational issues commensurate with their importance to health and safety. A risk-informed approach enhances the traditional approach by: (a) explicitly considering a broader range of safety challenges; (b) prioritizing these challenges on the basis of risk significance, operating experience, and/or engineering judgment; (c) considering a broader range of counter measures against these challenges; (d) explicitly identifying and quantifying uncertainties in analyses; and (e) testing the sensitivity of the results to key assumptions. A risk-informed regulatory approach can also be used to identify insufficient conservatism and provide a basis for additional requirements or regulatory actions.

Regulatory guidance documents have been written to address risk-informed applications that use PSA information. One specific regulatory guide (and its associated standard review plan) is Regulatory Guide (RG) 1.174 and Standard Review Plan (SRP) Chapter 19, which provide general guidance on applications that address changes to the licensing basis of an operating nuclear power plant. Key aspects of these documents are:

- They describe a "risk-informed integrated decision-making process" that characterizes how risk information is used. In particular, they state that such information is one element of the decision-making process. That is, decisions "are expected to be reached in an integrated fashion, considering traditional engineering and risk information, and may be based on qualitative factors as well as quantitative analyses and information."
- They reflect the NRC staff's recognition that the characteristics of the PSA needed to support regulatory decisions can vary, stating that the "scope, level of detail, and quality of the PSA is to be commensurate with the application for which it is intended and the role the PSA results play in the integrated decision process." For some applications and decisions, only particular parts of the PSA need to be used. In other applications, a full-scope PSA is needed. General guidance regarding scope, level of detail, and quality for a PSA is provided in the documents.
- While the documents are written in the context of one reactor regulatory activity (license amendments), the underlying philosophy and principles are applicable to a wide spectrum of reactor regulatory activities.

Guidance is provided in separate regulatory guides for such specific applications as in-service testing (RG 1.175), in-service inspection (RG 1.178), quality assurance (RG 1.176), and technical specifications (RG 1.177). SRP chapters were also prepared for each of the application-specific regulatory guides with the exception of quality assurance.

NRC has developed, or is developing risk-informed alternatives to certain requirements. For example, 10 CFR 50.69 provides an alternative, risk-informed approach to the special treatment requirements. This is discussed in detail in Section 7.US.

Much of NRC's work to date on risk-informed decision making has focused on applications for currently operating reactors. Regarding future reactors, the staff has developed and implemented a plan to develop a regulatory structure for new plant licensing. The objective is to provide an approach for the staff to enhance the effectiveness and efficiency of new plant licensing in the longer term. It is to be technology-neutral to accommodate different reactor technologies, risk-informed to identify the more likely safety issues and gauge their significance, performance-based to provide flexibility, and will include defense-in-depth to address uncertainties.

Requirements for a PSA

It should be noted that for the applications discussed in the previous section (which are focused on currently operating reactors), the adoption of a risk-informed approach is voluntary. There is no legal requirement for a licensee to develop a PSA for operating plants (see discussion below on the MSPI, however). However, if a licensee chooses to adopt a risk-informed approach, then a PSA is required as discussed, for example, in RG 1.174. A condition for using PSA results in a risk-informed regulatory application is that the PSA is of sufficient quality to support the specific decision. This is discussed further in Section 4.US.

Regarding future reactors, 10 CFR 52.47 requires that an application for standard design certification contain, among other things, a design-specific PSA. Similarly, 10 CFR 52.79 requires that an application for a combined license contain a design-specific PSA.

Development of PSAs

As discussed further in Section 5.US, most U.S. PSAs were developed by the licensees in response to Generic Letter (GL) 88-20 and to Supplement 4 of GL 88-20. GL 88-20 requested licensees to perform an Individual Plant Examination (IPE) for severe accident vulnerabilities associated with internal events (including internal flooding events but not internal fire events). Supplement 4 to GL 88-20 requested licensees to perform an Individual Plant Examination of External Events (IPEEE) for severe accident vulnerabilities associated with external events and internal fire events. More recently, as discussed in Regulatory Information Summary (RIS) 2006-07, the Mitigating Systems Performance Index (MSPI) was included as an element of the Reactor Oversight Program (ROP - see Section7.US). One of the conditions agreed to between industry and the NRC before adoption of the index was that all plants should participate. The development of the index requires a plant-specific PSA. Prior to the implementation of the MSPI, the licensees had to demonstrate that their PSA models were of sufficient quality to support the MSPI application.

The NRC has developed Standardized Plant Analysis Risk (SPAR) models for each plant and is in the process of benchmarking these models against licensee PSAs. These Level 1 PSAs are used by the NRC staff in a number of applications, for example: evaluation of the significance of inspection findings (phase 3 of the Significance Determination Process of the ROP); evaluation of the risk associated with accident precursors involving operational events and degraded conditions; identification and prioritization of modeling issues to support agency efforts to improve PSA quality; providing support for the resolution of generic safety issues; and providing support to risk-informed reviews of licensing applications. SECY-05-0192 discusses the status of the SPAR modeling program.

2.2.2 United Kingdom

The legal requirement in the UK is that the operators of nuclear plants should conform to the Health and Safety at Work etc. Act 1974 (HSW Act) which requires them, so far as is reasonably practicable, to ensure that their employees and members of the public are not exposed to risks to their health and safety. This means that measures to avert risk must be taken unless the cost of these measures, whether in money, time or trouble, is grossly disproportionate to the risk which would be averted. Hence, the risk should be reduced to a level which is as low as reasonably practicable – the ALARP principle. The term “reasonably practicable” is not defined in the legislation but has been established in the courts as a result of cases brought under the HSW Act.

The application of the ALARP principle requires that risk assessment is carried out which, for nuclear plants, involves assessments against both qualitative/ deterministic criteria and probabilistic safety criteria.

Probabilistic techniques and targets have been used in the UK since the early 1970s in the design of the Advanced Gas-cooled Reactors (AGRs). In particular, for Hartlepool and Heysham 1, a probabilistic analysis which looked at individual fault sequences was used to complement the deterministic approach that had been used until then. This was followed by Heysham 2 and Torness where Level 1 PSAs were carried out during the design process for internal initiating events.

For the PWR at Sizewell B, PSA was carried out throughout the design process. The initial Level 1 PSA at the Preliminary Safety Report (PSR) stage was followed by two PSAs at the Pre-construction Safety Report (PCSR) stage – a Level 1 PSA by the architect-engineer The National Nuclear Corporation (NNC) and a Level 3 PSA by the vendors (Westinghouse). For the Pre-Operational Safety Report (POSR), a full scope Level 3 PSA was produced which addressed all internal initiating events and all internal and external hazards, and covered all the modes of operation of the plant including full power operation, and low power and shutdown modes.

Since then, PSAs have been progressively carried out for the earlier reactors. These have been done as part of the Long Term Safety Reviews (LTSRs) carried out for the Magnox reactors and continued with the Periodic Safety Review (PSRs) which are now carried out every 10 years for all nuclear facilities. One of NII's requirements for the PSR is that it includes a plant specific PSA.

Requirement for a PSA:

PSAs are performed for all nuclear installations in the UK to evaluate the design of the plant and to demonstrate that the risk to workers and members of the public is both tolerable and as low as reasonably practicable (ALARP). The PSAs need to address the probabilistic criteria given in the Safety Assessment Principles for Nuclear Plants (SAPs) which relate to the individual risk of death to a worker, or member of the public.

The PSAs which currently exist have been produced or updated either as part of the design process for a new nuclear facility, or as part of a Periodic Safety Review for an existing plant. The production of the PSA is the responsibility of the licensee. However, it is usually the case that the detailed work is subcontracted to specialist PSA consultants. NII does not require licensees to use any specific analysis methods, models or data in their PSAs so that the licensees are free to carry out the analysis in any way they choose as long as it can be justified that they are suitable/ fit for purpose. Although there was a high degree of variability in the scope, level of detail and quality of the early analyses, there is now a relatively high level of uniformity in the PSAs currently being produced for power reactors.

All the PSAs produced are required to undergo an independent peer review by the licensees before they are submitted to NII. NII then carries out its own regulatory review of the PSA. There is no agreed standard procedure for carrying out the assessment of a PSA, for reactors the review usually involves a relatively detailed assessment carried out in-house often with the support of external consultants.

Guidance to NII assessors in carrying out an assessment of a PSA is given in the SAPs and the Technical Assessment Guides (TAGs) which give guidance on the interpretation of the SAPs and the specific topics that an assessor may need to address. They do not give formal acceptance criteria for safety case issues or the PSA; in the UK formal acceptance relies heavily on the judgement of the NII assessors who are carrying out the assessment.

In addition, the licensees are required to produce their own safety principles which provide the framework for their staff to produce safety cases and PSAs. For example, British Energy and the British Nuclear Group (formerly BNFL Magnox Generation) have both produced their own Nuclear

Safety Principles (NSPs) for their reactors which have been incorporated into the formal company standards. This provides a framework for assessing the level of safety of existing plants by applying both deterministic and probabilistic criteria together with specific advice to analysts on the quantitative aspects of performing ALARP arguments. Comparisons have been made between the SAPs and the licensees NSPs which have identified minor differences due solely to the different rational of the licensee and regulator.

2.2.3 Taiwan

The Taiwan Atomic Energy Council (TAEC), the nuclear regulatory agency in Taiwan, was founded in 1955 at the ministerial level under the Executive Yuan. Its original mission was to foster peaceful applications of atomic energy, and to coordinate international cooperation on nuclear energy. With the Taiwan's first reactor (a research reactor in National Tsing Hua University) reached its criticality in 1961, the Atomic Energy Law was enacted in 1968 and the Institute of Nuclear Energy Research (INER) was founded in the same year. Thirty-five years after, Presidential Decree promulgated the law of "Nuclear Reactor Facilities Act" on January 15, 2003. The Act is enacted to regulate nuclear reactor facilities in order to protect the public safety.

For the three operating nuclear power plants (NPPs), PSA was not formally requested by TAEC. Under the suggestions from the National Science Council, the development of first at-power PSA model for the operating nuclear power plants were organized by TAEC and executed by INER and Licensee, Taipower Company. Three PSAs were completed in 1985 (Kuosheng BWR-6)[1], 1987 (Maanshan, PWR)[2] and 1991 (Chinshan, BWR-4)[3]. The original at-power PSA models were released to Licensee. In 1995, those PSA models were updated to be living PSA models[4,5,6] by INER under contracts with the Licensee. Living shutdown PSAs[7,8,9] were also developed by INER and completed in 1996. Currently all PSAs both at power and during shutdown models are maintained by the INER.

Although there was no regulatory policy announced on PSA application in 90', some improvements inspired form the insight of PSA have been made on the operating NPPs. Examples of the improvements includes the addition of the 5th emergency diesel generator for each plant, the improvement of control room fragility against seismic (Chinshan), the upgrade of DC battery capacity from 8 hours to 24 hours (Kuosheng).

As for the Lungmen NPP which is under construction and scheduled to commercial operation in 2009, PSA was required and already included in PSAR. INER is now developing a living PSA model for Lungmen NPP. The scope includes at-power and shutdown Level 1 PSA and at-power LERF evaluation.

The study of risk-informed regulations and applications was initiated by INER since 1997. All PSAs had completed the peer review process in 2001. Then, TAEC approved on-line maintenance of RHR system in 2003. It is the first risk-informed application approved by TAEC. Another application approved by TAEC is the exemption of Chinshan cable tray fire wrapping in December of 2005.

Several projects were initiated for further risk-informed applications after the pilot study of 1997. The risk monitor (TIRM)[10] developed by INER and Licensee was first released in 1999. The second generation (TIRM-2)[11] was released in 2002 which includes the LERF evaluation with the enhancement of calculation speed and accuracy. The inspection tool (PRiSE)[12] which assists the resident inspector to evaluate the risk significance of inspection findings were released in 2004. It is a PSA model based evaluation tool by which the risk significance of inspection finding can be characterized with the associated increase level of CDF. The ΔCDF was calculated by resolving PSA model in less than one minute. Other ongoing and future projects include the risk-informed applications on in-service inspection, in-service test, online maintenance and maintenance rule.

2.2.4 Switzerland

The development of the first probabilistic safety assessment (PSA) for a Swiss nuclear power plant was started in 1983. This initiative was aimed at the development of a level 1 PSA for the Beznau nuclear power plant. Subsequently, in 1987, the Swiss Federal Nuclear Safety Inspectorate (HSK) required the utilities to perform full power level 1 and level 2 PSAs for all Swiss nuclear power plants. Four years later, HSK additionally required the licensees to develop plant-specific low power and shutdown PSAs, including external events.

In the meantime, PSAs for all Swiss nuclear power plants have been completed by licensees and independently assessed by HSK. The plant-specific PSAs include internal and external events such as fires, flooding, earthquakes, aircraft impacts and high winds. Level 1 PSAs have been developed for full power as well as for shutdown mode. Several intermediate updates of the PSAs have been performed. For every periodic safety review a fully updated plant-specific PSA has to be submitted to HSK by the licensees.

After the initial phase of development and review of various PSA models, HSK required the implementation of plant-specific "living PSA", in order to ensure that the PSAs are commensurate with important plant hardware and operational changes. Every licensee has prepared procedures that outline the utility process and policies applicable to maintaining their plant-specific "living PSA". The implementation of "living PSA" at all plants was completed in 2005.

In February 2005, a new Nuclear Energy Law and an accompanying ordinance were enacted in Switzerland. The ordinance now anchors the PSA into the law:

- For the construction permit of a new nuclear power plant, a PSA has to be carried out.
- Important changes in the PSA studies as well as unavailability of PSA-relevant components have to be reported on a regular basis.
- PSA is an integral part of every Periodic Safety Review.
- The risk impact of plant modifications, findings and events is to be assessed systematically.

In order to have a comprehensive, balanced and adequate decision-making process, HSK is implementing an integrated regulatory safety oversight process. Plant-specific PSA insights will be one element of the integrated regulatory safety oversight process.

Requirement for a PSA to Be Produced:

The initial applications of PSA concentrated on the determination of the overall plant safety level, the assessment of the balance of the plant safety concept and the identification of procedural and hardware improvements. Other applications have included the assessment of the risk impact of power uprate, risk implication of accident management alternatives, changes to technical specifications, and the selection of risk-significant components for the ageing surveillance programme. Recently, a procedure for the systematic performance of a probabilistic event analysis has been introduced.

Who Has Carried Out the PSAs:

The licensees conduct the PSA studies, which are then submitted to HSK. In general, the licensee PSA model forms the basis for any PSA applications.

The PSA studies have been extensively reviewed, resulting in continuous updates and improvements over the last 15 years. As a part of this periodic review process, HSK has developed independent plant-specific regulatory PSA models that are also kept up to date and consistent with changes introduced in their licensee counterparts. These regulatory PSA models enable HSK to perform independent confirmatory analyses, and to assess the risk implication of various safety issues and regulatory actions.

2.2.5 Sweden

During the 80:ies and 90:ies the Swedish PSA work was very much linked to the program of the domestic ASAR-programs (ASAR80 and ASAR90 programs) (ASAR = As Operated Safety Analysis Report). In the ASAR80 program, the licensees had to perform their LOCA and transient PSA level-1 studies. In the ASAR90 program, e.g., the PSA level-2 studies, CCIs, shutdown studies, was planned to be performed.

A PSA had also to be published and reported to the regulatory body SKI, every 8th -10th year and as an appendix to the respective ASAR report. The regulatory body SKI reviewed both the ASAR and the PSA reports and a recommendation was thereafter given to the Swedish government.

In 1998 SKI published the regulation “The Swedish Nuclear Power Inspectorate’s Regulations Concerning Safety in Certain Nuclear Facilities and General Recommendations Concerning the Application of the Swedish Nuclear Power Inspectorate’s Regulations”**,** the SKIFS 1998:1.

Since 2004, the requirements on the PSA are sharpened in the new regulations given in SKIFS 2004:01. PSA:s have to be performed for all operating modes and a systematic inventory of all initiators challenging the safety have to be done.

Domestic PSA:s are at the licensees planned to be updated on an annual bases, type living PSA:s. The SKI inspection and follow-up of the PSA-activities at the licensees are based on a process oriented inspection and review process, complemented by a random inspection of the detailed analysis. A big work is going on both at the SKI and at the licensees regarding the update of the Safety Analysis Reports, so that they are fulfilling the requirements on the SAR, given in the regulation. The PSA:s in Sweden have not fully met the requirements on the scope of safety studies, this yields especially on studies for low power operation.

The changeover to the new regulation has led to different transition stages on how the licensees can fulfil the regulation at different time periods. It is expected now that the domestic PSA:s include analysis of all operating modes till end of 2007 as well as of all safety important initiators.

The new regulation has also led to different transition stages regarding the fulfilment of safety analysis documented in the Safety Analysis Reports.

The purposes of the PSA:s that have to be are to identify week points in the present design, operational routines and instructions to support program for education and training.

In Sweden the PSA:s that have been produced so far, are mainly produced by domestic consultant companies, under the supervision of the PSA offices at the licensees. SKI do not produce any PSA:s, it is the strictly responsibility of the licensees to do that. The role of SKI is to review that the quality are as expected and that the studies give right answers when used in different kinds of decision making, in applications. Also, that the safety studies documented in the license documentation SAR, is verified by probabilistic analysis.

2.2.6 Spain

The PSA framework has been established in Spain in 1986 with the submittal by the CSN of the programme “Integrated Programme on Performance and Use of the PSA in Spain”(IP). This document has been the guidance document of the PSA activities carried out by the utilities and by the CSN. The aim of the document was to define the scope of the PSA activities and the use of the PSA in Spain. This document has been revised in 1998 as the second edition and issued by the CSN.

The first edition of the IP, contemplate in first instance the performance of the PSA and this was the more important objective. In the second edition the objectives were more related to the use of the PSA. With this second edition the mayor emphasis was on the PSA applications but also review of the remaining scope of the PSA was an activity. This remaining scope refers to the performance and review of some levels 2, low power and shutdown and others activities related to fire and flooding during shutdown and level 2. The PSA applications were directed to the internal applications performed by the CSN but also to the external applications submitted by the utilities and reviewed by the CSN.

2.2.7 Slovenia

In 1991 the Slovenian Nuclear Safety Administration (SNSA) issued a decision by which the Krško NPP (NEK) had to develop Probabilistic Safety Assessment (PSA). It was required:

- to perform full scope PSA level 1 analyses on the basis of IAEA and US NRC (NRC Generic Letter No. 88-20 and NRC NUREG – 1407) guidelines.
- to perform PSA level 2 analyses on the basis of IAEA and US NRC (NRC Generic Letter No. 88-20 and NRC NUREG – 1407) guidelines.
- that licensees must provide a written report of analyses and the PSA plant specific model in electronic form to the SNSA (living PSA).

As a consequence of decision, both the SNSA and the Krško NPP use the same PSA model. The Krško PSA is a comprehensive PSA model. It covers internal and external events such as fire, external flood, seismic and others, and events at power and shutdown events. Moreover, the PSA model quantifies plant CDF for all categories of events (including, in a simplified manner, the shutdown events). The PSA model is a Living PSA model and is based on the Krško NPP IPE/IPEEE study, which was performed in the period 1992-1994. The PSA model has undergone various revisions (pass over to RiskSpectrum program, modernization in the year 2000 when the steam generators were replaced, and reactor power uprated, fire protection action plan implementation, seismic hazard reevaluation) since then. The PSA model update is preformed once every fuel cycle to reflect plant configuration and SCC reliability/unavailability data changes. These changes generally affect the existing references to the PSA model, such as system drawings, procedures, Technical Specifications, USAR, various analyses which affect success criteria etc. They may also induce an issuance of some new documents which may become new references to the PSA model (for example, various safety studies which may be part of a design modification package).

Several peer reviews of the PSA have also been preformed by the IAEA missions (IPERS and IPSART) in the past years. The PSA was also reviewed in the scope of the first Periodic Safety Review (PSR), where the Krško NPP PSA level 1 and level 2 (to a limited extent) analyses for internal events at power were reviewed against the PSA technical elements per NEI/WOG/ASME guidance and standards.

The regulation that would explicitly address the PSA is still under preparation (the first draft has been prepared). It will include and determine PSA extent, quality and applicability. It will also give principles, commitments, requests and conditions for using PSA. Also the criteria for assessment of changes, uncertainty assessment, reporting requests and on-line maintenance requirements will be included.

2.2.8 Slovak Republic

The Slovak Republic has six WWER-440 type units in operation. There are four nuclear power plants (NPP): A1, V1, and V2 at the Jaslovske Bohunice site and the Mochovce NPP. The A1 NPP, equipped with a heavy water moderated and gas cooled reactor, is shutdown and under decommissioning. There are two units with WWER-440/V230 type reactors in the V1 NPP; gradual reconstruction of both units was finished in 1999 and 2000. First unit of Bohunice V1 NPP has been shut down since December 31, 2006; the shut down of second unit of Bohunice V1 NPP is scheduled to December 31, 2008. Another two units with WWER-440/V213 type reactors are in operation in the V2 NPP. Two units with WWER-440/V213 type reactors were given into operation in 1998, respectively 2000 at the Mochovce site.

The NPP operator has the responsibility that the facility is operated, tested and maintained to achieve a high level of safety. Active use of PSA is an important element of this process. The probabilistic frameworks and the PSA models provide useful tool to support operation, maintenance and plant management.

The Nuclear Regulatory Authority of Slovak Republic (UJD) as the national regulatory body has the primary responsibility to review and audit all aspects of design, construction and operation to ensure that an acceptable level of safety is maintained throughout the life of the nuclear power plants in Slovakia. The plant specific PSAs are expected to fulfil an important role in this process because they will facilitate consistent understanding and communication between the operators and regulator. The PSA models provide a common basis for examination of safety issues, operational events and regulatory concerns and for determining plant specific safety significance of various issues.

PSA is considered as a part of safety documentation. Requirements on the PSA performance, review, and update including scope and contents of PSA are specified in the national regulations No. 49/2006 on Periodic safety review and No. 58/2006 on Preparation of safety documentation for nuclear facilities. A concretisation of requirements of generally binding legal regulations is provided in the UJD guideline BNS I.4.2/2006 on Requirements for the performance of PSA studies and analyses. A guideline on PSA applications including risk informed regulation is under development.

The guidelines are not intended to be procedural guides for performing, review, and application of a PSA. Such procedures have been developed by IAEA and other organizations. These guidelines are intended to enhance standardization of PSA, supporting documentation, and applications. Thereby, providing a more useful and effective tool for operational and regulatory safety enhancement.

The UJD recognizes the PSA methodology and requires performing the internal event level 1 and level 2 PSA study (including internal fires and floods) for full power operation state for any nuclear power plant on the site. If relevant, external hazards (as seismic event, extreme temperatures, etc) must be incorporated into the PSA study. In addition to full power operation, low power and shutdown operation states, and the transfers between them are recommended considered in the PSA study.

The PSA represents depiction of the state of knowledge at the time of the study. As time passes number of inputs in the model may change. The changes can be design changes, procedural changes or changes in the state of knowledge about the plant which can influence the accepted assumptions. The PSA should involve the risk evaluation of all plant changes. Therefore, it must be periodically updated. The UJD requires five-year interval for updating PSA. However, the design and procedural changes should be incorporated before additional applications are performed in order to keep the PSA model current.

The PSAs for the Slovak NPPs are performed by RELKO Ltd. and VÚJE, Inc. UJD performs review of the PSA studies. In addition, IAEA experts are used to perform the IPSART type of review.

2.2.9 Netherlands

Nuclear Environment

Currently there is one operating Nuclear power plant in The Netherlands. The Borssele NPP is a Siemens/KWU designed PWR of 480 MWe in operation since 1973. In 1997 the Dodewaard NPP, a vintage small GE-BWR ceased operation. Also there are three research reactors in operation. Over the last few years, more emphasis has been placed on the safety of the High Flux Reactor, a 45 MWt tank in pool type research reactor. The reason that this reactor is mentioned in this report is the fact that due to the requirement to conduct a 10-yearly periodic safety review, a simplified level-3 PSA was made.

Prior the Chernobyl disaster The Netherlands intended to construct another new NPP. This intention was abruptly changed by that dramatic event. The nuclear energy option as a whole was re-evaluated. Also the safety of the two at that time operating NPPs was evaluated. PSAs played an important role in the evaluation and associated discussions. The decision to expand the nuclear energy option was postponed and; the option even became a taboo. Several years later the government even tried to close the Borssele NPP by the end of 2003 by imposing a special license condition in that respect. The utility of the plant lodged an appeal against this restriction. In 2000 the Council of State (highest administrative court in The Netherlands) revoked on formal grounds this license restriction. Since about 2004 this anti-nuclear attitude was changed by the newly elected government. Currently there is an agreement between the utility and the government that the plant can operate till 2033, provided that the plant will remain within the group of the safest NPPs in the world (top 25%). In the summer of 2006 the government sent a letter to the parliament regarding the boundary conditions of possible new NPPs and thereby continuation of the nuclear energy option in The Netherlands. In this letter a criterion for Total Core Damage Frequency (TCDF) was formulated to what a new NPP should meet.

Regulatory framework

Legal framework

Nuclear Energy Act.

The basic legislation governing nuclear activities is contained in the Nuclear Energy Act. The Nuclear Energy Act is designed as an integral act to cover both the use of nuclear energy and radioactive techniques, as well as to lay down rules for the protection of the public and the workers against the risks. However, through the years the law is gradually more focussing on protection of the public and workers than on the use of nuclear energy. The law sets out the basic rules on nuclear energy, makes provisions for radiation protection, designates the various competent authorities and outlines their responsibilities.

A number of decrees have also been issued containing additional regulations and continue to be updated to take care of ongoing developments. The most important decrees in relation to nuclear safety are:

- the Nuclear Installations, Fissionable Materials and Ores Decree;
- the Radiation Protection Decree;
- the Transport of Fissionable Materials, Ores and Radioactive Substances Decree.

The Nuclear Installations, Fissionable Materials and Ores Decree regulates all activities (including licensing) that involve fissionable materials and nuclear installations.

The Nuclear Installations, Fissionable Materials and Ores Decree (Bkse) sets out additional regulations in relation to a number of areas, including the procedure for applying for a license. These contain also the requirements for the application of a license. Amongst others, this Decree requires:

- a description of the measures to be taken either by or on behalf of the applicant so as to prevent harm or detriment or to reduce the risk for harm or detriment, including measures to prevent any harm or detriment caused outside the plant during normal operation, and to prevent any harm or detriment arising from the Postulated Initiating Events (PIEs) referred to in the description, as well as a radiological accident analysis concerning the harm or detriment caused outside the installation as a result of those events (Safety Analysis Report);

- *a risk analysis* concerning the harm or detriment caused outside the installation as a result of severe accidents (Probabilistic Safety Analyses).

The *Environmental Protection Act*, in conjunction with the Environmental Impact Assessment Decree, stipulates (in compliance with EU Council Directive 97/11/EC) that an Environmental Impact Assessment must be presented if an application is submitted for a license for a nuclear installation.

Normally (i.e. for non-nuclear installations) this Act regulates all conventional environmental issues (e.g. chemical substances, stench and noise), but in cases concerning nuclear installations the Nuclear Energy Act takes precedence and regulates also the aspects of such conventional environmental issues.

In compliance with this Act and the Environmental Impact Assessment Decree, the construction of a nuclear plant requires the drafting of an environmental impact assessment as part of the licensing procedure. In certain circumstances, an environmental impact assessment is also required if an existing plant is modified.

The public and interest groups often use environmental impact assessments as a means of commenting on and raising objections to decisions on nuclear activities. This clearly demonstrates the value of these documents for public debate and involvement.

In general, the numerical outcomes of a level-3 PSA play a large role in the description of the environmental impact of the proposed design or design-change. Also various alternatives of the proposed design or design-change including the respective risk impacts are discussed.

Nuclear Safety Rules

In the Nuclear Energy Act (Article 21.1), the basis is given for a system of more detailed safety regulations in the areas of the design, operation and quality assurance of nuclear power plants. The system is referred to as the Nuclear Safety Rules (NVR) and has been developed under the responsibility of the Minister of Housing, Spatial Planning and the Environment and the Minister of Social Affairs and Employment

The NVRs are based on the Requirements and Safety Guides of the IAEA Nuclear Safety Series (NUSS) programme, now referred to collectively as the IAEA Safety Standards Series (SSS). Using an agreed working method, the relevant SSS safety principles, requirements and guidelines were studied by a working group consisting of representatives from the KFD, licensees and others, to see how these SSS could be applied in The Netherlands. This procedure resulted in a series of amendments to the IAEA Codes and Safety Guides, which then became the draft NVRs. The amendments were formulated for various reasons: to allow to present a more precise choice from a range of different options, to give further guidance, to be more precise, to be more stringent, or to adapt the wording to specifically Dutch circumstances (e.g. with respect to the risk of flooding, population density, seismic activity and local industrial practices).

The license granted to the nuclear power plant includes specific conditions under which the NPP has to comply with the NVRs. It is this mechanism that allows the regulatory body to enforce the NVRs. At the Code level, the NVRs have to be followed in detail, as they are requirements. At the Safety Guides level, the NVRs are less stringent, i.e. they may be followed, but alternative methods could be used for achieving the same safety level.

Regulatory Body

KFD

The Nuclear Regulatory Body in The Netherlands is formed by two entities, SAS and KFD, both from the Ministry of Housing, Spatial Planning and the Environment. KFD is the organisation responsible for inspection, assessment and enforcement, whilst SAS is the policy department dealing with all the political interfaces. KFD closely cooperates with SAS as a kind of TSO regarding licensing and the establishment of regulations.

Before 2001, the KFD was part of another ministry. It had its own formal role in licensing and regulation. After, the transfer to the current ministry the actual content of the work for licensing and regulation remained the same (TSO function), but the formal responsibilities shifted to SAS. In this way, a more formal separation between rulemaking and oversight was created.

The KFD encompasses all major reactor safety, radiation protection, security and safeguards and emergency preparedness disciplines. For areas in which its competence is not sufficient or where a specific in-depth analysis is needed, the KFD has a budget at its disposal for contracting outside specialists. One of the basic policies of the KFD is that core disciplines should be available in-house, while the remaining work is subcontracted to third parties or technical safety organizations.

The total professional formation of the KFD, for all nuclear facilities is now 24,75 (3 managers, 6 administrative support, 4 inspectors, 2 security & safeguards and 12 experts for the various core disciplines).

The staffing of the KFD is an ever-ongoing concern as it is with any comparable organization, which consists of a great variety of highly specialized professionals. Unavoidably this issue has been discussed within the organization almost as long as the KFD has existed (30 years).

Build-up of staff started systematically by the mid 70s and continued well into the eighties. An almost complete coverage of disciplines was developed in principle by 1985 when there was advanced planning for the extension of the nuclear programme in The Netherlands. After the Chernobyl accident the extension of the nuclear energy option was put to a hold and even the continuation of the existing nuclear power plants was debated. As a consequence there was no need to extend the regulatory body. The present situation is essentially still the same. The KFD remains a fairly small organization of highly specialized professionals, which is vulnerable to "external" developments.

Directorate for Chemicals, Waste, Radiation Protection (SAS)

The main task of this Directorate is policy development, regulation and implementation in the field of radiation protection and nuclear safety in relation to the public and the environment. Therefore, SAS is responsible for developing legislation and for licensing nuclear installations and nuclear transports in general (all procedural aspects), as well as for all aspects concerning radiation protection and external safety.

Historic regulatory requirement for PSA to be developed

After the Chernobyl accident the decision to expand the nuclear power capacity in the Netherlands was postponed. The Dutch government decided to reconsider the nuclear option. Several studies were initiated to assist in this reorientation process. An important part of this reorientation process was the assessment of the beyond design capabilities and possible accident management measures of the at that time two operating Dutch nuclear power plants Borssele, a 480 MWe KWU-PWR, and Dodewaard, a 58 MWe GE-BWR. In 1997 the Dodewaard plant closed in 1997 and is transformed into a so-called safe enclosure. Because plant specific PSAs were not available at that time, generic PSA insights and lessons learned from other PSAs and deterministic analyses formed the basis for a regulatory accident management and backfitting strategy as it was felt necessary at that time. The German Institute for Reactor Safety (GRS) was asked by the Dutch regulatory body to assess the design weaknesses of both Dutch NPPs relying on their insights gained by performing the German Risk Study (DRS-B) and other deterministic assessments. The results of this study formed the basis of the position of the Dutch regulatory body regarding accident management and backfitting. One of the recommendations was to perform at least a level 1^+-PSA for identification of plant-specific weaknesses. Thus, to focus on identification of the 'weaknesses' and 'imbalance' in the design and operation features that could be improved (e.g. by backfitting, accident management or changes in the conceptual design). In other words, the PSA should give a clear picture of the various scenarios leading to core melt, the relative contribution to the core melt frequency of each initiating event group, and the spectrum of resulting plant damage states. The PSAs had to support the required modification programmes and/or give guidance to the development of possible risk reducing measures for preventing and/or reducing accident scenarios as well as for mitigating the consequences of accidents.

PSA development and objectives

PSAs for the two NPPs Borssele and Dodewaard

Both the licensees and the licensing authorities agreed with the GRS-proposal to conduct a level 1^+ PSA. This resulted in two bid specifications for a level-2 minus PSA. For Borssele this PSA-project was awarded to the combination KWU and NUS (currently Scientech Inc.), and for Dodewaard the project was awarded to Science Applications International Corp. (SAIC) from the USA and to KEMA (the supporting organization of electric utilities in areas of testing, certification, assessment, research and development).

The main objective of these PSAs was to identify and to assess the relative weak points in the design and operation of the power plants, in order to support the design of accident management measures, and to support backfitting [reference 1]. An assessment of source terms, public health risks, etc., was regarded as unnecessary at that time.

The regulatory requirements as well as the wishes of the licensees themselves regarding the objectives of the PSAs were translated by the licensees in their respective original bid specifications:

- To identify and analyse accident sequences, initiated by internal and area events that may contribute to core damage and quantify the frequency of core damage.
- To identify those components or plant systems whose unavailability most significantly contributes to core damage and to isolate the underlying causes for their significance.
- To identify weak spots in the operating, test, maintenance and emergency procedures, which contribute significantly to the core damage frequency.
- To identify any functional, spatial and human induced dependencies within the plant configuration, which contribute significantly to the core damage frequency.
- To rank the weak spots according their relative importance and to easily determine the effectiveness of potential plant modifications (both backfitting and accident management). See further reference 1 for a more detailed description of the PSA based backfitting and modifications going on at the Borssele and Dodewaard Nuclear Power Plant.
- To provide a computerized level -1 PSA to support other living PSA activities like optimisation of Tech Specs, Maintenance Planning, etc.
- To transfer technology and expertise to the licensee to make them fully capable to evaluate future changes in system design, operating procedures and to incorporate these changes in the 'Living' PSA.

At the same time large modification/backfitting programmes emerged, partly as a result of Chernobyl. A backfitting requirement was formulated for the existing NPPs. Although backfitting primarily addresses the design basis area, also the beyond design basis area and associated severe accident issues get their attention. This so-called backfitting rule involves the requirement of a periodic 10-yearly safety review. This requirement is included in the operating licence of both plants. An important part of these periodic 10-yearly safety reviews is a level-1 plus PSA.

Later it turned out that large modification programmes involve a licensing procedure. Due to this licensing procedure both plants had to submit an Environmental Impact Statement. A substantial part of this Environmental Impact Statement is a 'full scope' level-3 PSA, including an assessment of the influence of the proposed modifications. This meant an expansion of the scope of the ongoing studies. These studies were finished in the beginning of '94. The results of these studies were also communicated to the Dutch Parliament.

In one case, new and unplanned studies regarding the potential of design modification proposals had to be performed. This as a result of comparisons of the results with resp. level-1 and level-3 PSC. An overview of these expansions is given in the next paragraphs. Due to review processes, intermediate results of the PSA, changing 'state-of-the-art (e.g., assessment of the risks associated with low power and shut-down states) and expansion of the objectives, the scope of the PSAs expanded as well.

In the early nineties these level-1^+ PSAs were expanded to full scope level-3 PSAs, including: internal and external events, power and non-power plant operating states, human errors of omission and commission. The objectives of these expansions were partly due to the requirement that the studies should be 'state-of-the-art' (non-power plant operating states and human errors of commission), and partly due to the licensing requirements associated with the ongoing modification programmes (an Environmental Impact Assessment had to include a level-3 PSA). For the Borssele plant NUS/Scientech became the main and sole contractor.

As already indicated, an important reason for the original PSAs was to provide both licensees and regulatory body a better understanding of the hidden safety related weaknesses in operation and design. Other, less obvious reasons for regulatory input regarding the use of PSAs emerged as well:

- to have a common basis of understanding between licensee and regulatory body.

- stimulation of Living PSA applications at the plant

The regulatory body needs the current PSA as a common basis of understanding in discussions regarding plant modifications, backfitting, etc. In this case the PSA was not a replacement of the traditional regulatory work; it only assesses and guides this work.

After finishing these studies, the focus shifted towards "Living PSA" (LPSA) applications. Even the new licenses of the modified plants require the licensees to have an operational 'Living' PSA, without describing the concept and applicability of LPSA any further. The operator of the Borssele plant as installed a risk monitor for configuration control during outages, uses the PSA for optimisation of Technical Specifications, etc.

The current ongoing PSA applications like: support of backfitting measures, support of periodic safety reviews, licensing activities, prioritisation of inspection tasks, reliability centred maintenance, etc., will be continued and/or intensified.

PSA of the High Flux Reactor (HFR)

The existing license of the HFR was obsolete. It was issued before the Nuclear Energy Act in The Netherlands was established and revisions had a very fragmentary character. In the past the HFR received little attention by the Regulatory Body because prioritisation of the two Nuclear Power Plants at that time. This approach was supported by the low potential risk compared with the risk from the NPPs. Wishes of the KFD to update and modernise the license didn't get far. The Ministry of Economic Affairs, at that time the Secretariat of the competent authorities for licensing of nuclear installations, was very much programmatically and financially involved in the scientific program of ECN and the HFR in particular. In the late nineties two events caused a change:

1. due to the long-time negative attitude (both public and political) towards the option of installing new nuclear power plants in The Netherlands, the focal point for the Ministry of Economic Affairs shifted from nuclear research programs towards other energy research programs,
2. the ministry of Economic Affairs was no longer the Secretariat of the competent authorities for licensing.

These changes, together with the practice for NPPs to conduct every ten-year a complete safety re-evaluation, enabled the regulatory authorities to embark on a re-evaluation plan of the HFR and its license.

In discussions between the regulatory body and both the licensee (JRC-Petten) and operating organisation (NRG) the scope of work for this safety re-evaluation was agreed upon. First a new Reference Licensing Basis (RLB) had to be established to have a state-of-the-art yardstick for nuclear safety for comparison. Second, a risk scoping study should be conducted for the identification of technical weaknesses, which could be overlooked by the deterministic comparison with the RLB. A new set of safety analyses should be made based on a more complete set of Postulated Initiating Events (PIEs), including the assessment of fire, flooding and seismic events as well as ageing. Following recommendations from the analyses a new safety concept had to be established as well as a modification program to achieve this safety concept.

Because a full scale Probabilistic Safety Assessment (PSA), as conducted for a NPP, was initially assessed to be too costly for a research organisation, it was decided to embark on a limited PSA, a so-called Risk Scoping Study. Apart from that a full scope PSA for the HFR was considered very complicated due to the lack of reliable data for both component failure as for operator handling. Nevertheless, during its conduct the scope and level of detail expanded far beyond the initial intent. The objective was to provide assurance that in the deterministic safety analyses performed for the HFR no potential occurrences presenting a substantial risk to the public were overlooked. Both the current plant configuration with HEU fuel as the future plant configuration with LEU fuel and planned modifications had to be assessed. Because the initial objective was mainly the identification of weaknesses and not providing numbers, the scope of the PSA was restricted to include only hazards associated with the core. Plant internal initiators, including internal flooding and fire were selected to:

- identify those initiating events and sequences which contributed to core damage or unusual release of radioactivity and to estimate the core damage frequency (level-1),
- identify and assess the containment failure sequences and associated source terms (level-2),
- assess the off-site consequences in terms of public health risks of these source terms (level-3).

The first level of the Risk Scoping Study was reviewed via an IPSART-mission of the IAEA. The comments and remarks being made led to an upgrade of the study. A second review followed in 2002 with the emphasis on level-2 and level-3

An important part of the Risk Scoping Study was the assessment of internal flooding and fire. Both the design review concerning fire protection and the fire hazard analysis turned out to be very useful. Especially, a lot of unnecessary combustible loads were found to be present in the control room area such as filing cabinets. But also lack of spatial separation between redundant safety systems and a lack of fire detectors were identified.

Transition towards a more Risk Informed regulation

Because the regulatory body increasingly is confronted with design or operational changes which stem directly from, or are supported by arguments stemming from LPSA-applications at Borssele, which require approval of the KFD, the IAEA was asked to advice the KFD in order to support this process. Questions like:

> “Are the LPSA-applications at the Borssele plant state-of-the-art and sufficient, or should Borssele do more?”, “How should the KFD respond to these applications, given a small regulatory staff and possible short remaining lifetime of the Borssele plant?”, were the focal points of this review.

The main conclusions and recommendations were:

- Complete the implementation of the risk monitor with high priority in order for it to be used for maintenance scheduling, operating decisions and risk follow-up.

- Select those applications that can provide benefit to the plant in the near term. This selection could be based on criteria such as dose reduction, regulatory requirements, maintenance costs, refuelling outage duration, etc. Examples of such applications are risk-informed improvement of technical specifications, risk-informed increment of on-line maintenance activities.

- KFD was suggested to develop a framework for the use of risk information in regulatory decisions. This should include the identification of objectives, description of the decision-making process and acceptance criteria, and clarification of how risk-informed decision-making is to be incorporated in the existing regulations. Since developing such a framework may take considerable effort, they were suggested to review existing risk-informed frameworks, bearing in mind that acceptance criteria need to be developed for the specific situation in The Netherlands.

- The resources required for accomplishing risk-informed regulation depend on how much use will be made of this approach, however, the IAEA team suggested that, as a minimum, KFD should continue to allocate one person, having in-depth knowledge of the Borssele PSA, for PSA-related activities, and that all decision-makers should have some training in PSA.

- The IAEA team felt that if applications are requested by the KFD to Borssele NPP, these should be discussed with the plant to maximise mutual benefit. Also, the discussions raised the idea that perhaps the KFD and Borssele NPP could develop a consensus document to conduct and assess PSA applications.

- Finally, the KFD was suggested to use PSA to focus the regulatory inspection program on the more significant systems, components, and plant practices.

As a follow-up of this advice, the KFD cautiously defined a follow-up program/feasibility study in order to proceed towards a more risk-informed regulation. It was decided to take a step-by-step approach. The first step is to familiarise with risk-informed regulatory approaches in West-European countries, whilst the next steps are centred on a particular application, such as Technical Specification optimisation.

Follow-up program

The objective of this program is to come to a situation in which regulatory attention is more consistent with the risk importance of the equipment, events, and procedures to which the requirements apply, so that regulatory and licensee resources can be used in a more efficient way when making decisions with respect to ensuring the health and safety of the public. This objective implies that the regulatory requirements be commensurate with the risk contributions (i.e., regulations should be more stringent for risk important contributors, and less stringent for risk unimportant contributors). Therefore, provided risk informed regulatory criteria are appropriately developed, a systematic and efficient expenditure of resources are to be expected, while, simultaneously, a balance in overall plant safety can be achieved.

Examples of typical regulatory actions where risk-informed methods and requirements are thought to be helpful and therefore being investigated in the project, include:

- evaluation of the design and procedural adequacy;
- performance of periodic safety reviews;
- assessment of changes to the licensing basis, e.g. Technical Specification optimisation: surveillance test intervals, allowed outage times, limiting conditions of operation;
- assessment of operational practices or strategies on safety such as: plant systems configuration management, preventive and corrective maintenance prioritisation;
- prioritisation of regulatory inspection activities;
- evaluation of inspection findings;
- investigation of ageing effects;
- assessment of risk-based safety indicators;
- the need for regulatory action in response to an event at a plant;
- one-time exemptions from Technical Specifications and other licensing requirements; and
- assessment of utility proposals for modifications of the design or operational practices.

The development of risk-informed regulation in The Netherlands is bounded by the present limited nuclear power programme: one NPP (Borssele) in operation, and shutdown of this NPP eventually foreseen by 2033. There are no new reactors planned yet.

Currently the focus of future activities/events for Borssele NPP is governed by license requirements or external circumstances. It concerns initiation/continuation of:

- new 10-year periodic safety review, formally started in 2001;
- two-year operational safety review;
- monitoring of the plant safety culture during the expected plant staff reduction;
- deregulation of the electricity market;

Under these boundary conditions, emphasis of the development of risk-informed regulation will be in the operational and not in the design area. Also QA is assumed to focus on operational items, in this respect. The design area, however, cannot be ignored, as the plant configuration determines much of the plant safety characteristics.

As the application domain is limited, as is the available manpower within the KFD, the development of Risk-informed Regulation should be based on existing approaches elsewhere; no separate ‘Dutch’ RiR development is to be foreseen. Main vehicle could be the USNRC development, plus useful parts of the approaches in Spain, Switzerland, Sweden, Finland, Belgium and the UK. Where the sources are diverse, special care must be exercised to obtain a coherent and consistent product.

‘Deregulation’ is meant as a support to the utility to be and remain competitive on the electricity market. In practice, it means that active support will be given to activities aimed to decrease costs, as long as they do not compromise safety.

The main objectives of the RiR are therefore:

- support the above mentioned (bulleted) activities;
- focus KFD and plant resources on items relevant for risk; and
- eliminate unnecessary ‘regulatory burden’.

It is *not* the intention of the proposed RiR-project to generate formal revisions of the NVR-series Design, Operation and Quality Assurance. However, RiR-products will be documented and reviewed with industry.

Overall, the RiR products will be application-oriented. In some areas, fundamental aspects may be touched, where no written guidance can yet be formulated. In those cases, a conclusion must be reached how to proceed on a more ad-hoc basis.

A special aspect of this project is feasibility if the current oversight process can be transformed into a more risk-informed oversight process. This includes, the eventual use of safety significant performance indicators.

In order to get an approval of the higher administrative and political top of the ministry for this transition towards a more risk informed approach of the regulation, a letter was send to the minister of VROM explaining the objectives and foreseen benefits of this approach. In this letter it was stressed that RiR is a vehicle for achieving a continuous improvement of safety of the plant. Also this approach shows in a transparent way the temporary risk increases which are associated with changes of the installation to benefit the economic output (e.g., power increase) and are granted on the principle of justification. It warrants in such cases that those risk increases will be as small as reasonably achievable.

As a more formal start of this project the adaptation of US-NRC Regulatory Guide 1.174 with regard to the Dutch Safety Criteria is being prepared and to formalise it as a Dutch Nuclear Safety Guide.

2.2.10 Mexico

The Political Constitution of the Mexican United States, in its Article 27, establishes that nuclear energy must be only used for pacific applications and the utilization of nuclear fuels for the generation of nuclear energy corresponds to the Nation.

Mexico has committed itself to apply safety and health protection measures observed in the International Atomic Energy Agency (IAEA). Furthermore, from the beginning of the Laguna Verde project, governmental authorities decided to apply the regulatory standards of the country of origin of the steam supply system as well as those from the IAEA recommendations. For this reason, Title 10 “Energy” of the Code of Federal Regulations of the United States of America was established as a regulatory requirement as well as all industrial standards and guides deriving from such Title. In a similar manner, US Regulatory Guides issued by the Nuclear Regulatory Commission have been adopted.

The Mexican regulatory authority (CNSNS), following the USNRC generic letter 88-20, requested the utility to perform an Individual Plant Examination (IPE) of Laguna Verde NPP. The utility performed the front-end analysis of the IPE and The Instituto de Investigaciones Eléctricas (Electrical Research Institute) was commissioned by the utility to perform the back-end analysis of the IPE. The IPE involved a thorough examination of the plant design and operation to identify dominant severe accident sequences and their contributors as well as plant vulnerabilities, if any. In parallel the CNSNS began the development of their own PSA level 1 and 2 for regulatory applications.

After the IPE conclusion, the CNSNS began the adaptation of the NRC/RG 1.174 and 1.177 [1, 2] as part of their first effort to implement a risk informed regulatory framework and issued in 2005 its policy for the use of PSA in regulatory practices where feasible within the bounds of the state of the art in PRA methods and data to reduce unnecessary conservatism in a manner that complements the deterministic approach and supports traditional defense-in-depth philosophy.

2.2.11 Korea

The initiative to perform PSA was taken by the regulatory body to ensure operational safety of the nuclear power plants (NPPs) since the TMI-2 accident. In 1997, the Minister of Science and Technology (MOST) issued the "Nuclear Safety Policy Statement" consisting of five regulatory principles of nuclear safety to secure consistency, adequacy, and rationality of regulatory activities. The regulatory principles are developed for independence, openness, clarity, efficiency, and reliability. To quickly realize the safety culture and to have safety assurance declared in the policy statement, nuclear power plants in operation or under construction have to be supplemented with the regulatory requirements, taking into account the possibility of severe accidents.

The Korean Nuclear Safety Commission decided to introduce the Severe Accident Policy (SAP) in 2001, which prescribes comprehensive measures against severe accident, including PSA implementation. The main objective of the policy is to assure that the possibility of a severe accident occurrence is extremely low and its risk to the public is sufficiently reduced. The details of the policy are to do the following essential elements in Korea:

(1) Setting-up of probabilistic safety criteria;

(2) Implementing PSA in the design and operation;

(3) Providing capability for the mitigating and preventing features against severe accidents;

(4) Establishing of severe accident management program (SAMP).

These will be used to provide the means of safety improvement for nuclear facilities, to assure the consistency in the execution of PSA review, and to establish the basic guidelines to the technical requirements for the specific PSA areas. In terms of PSA implementation, the policy states as:

> *"PSAs should be performed in order to determine countermeasures such that the risk from the NPPs is reduced to as low as reasonably achievable. As for relatively high probability accident scenarios inadvertently going plant damage, available means for accident prevention and mitigation should be identified and implemented in the design and operating procedures of NPPs, through cost-benefit analysis."*

The PSAs in Korea have been carried out in many organizations: KEPRI (Korea Electric Power Research Institute) in charge of the utility (Korea Hydro and Nuclear Power Company; KHNP), KAERI (Korea Atomic Energy Research Institute), and KOPEC (Korea Power Electric Company). The overall activities are focused on the development of the PSA models and methods, the use of PSA in design, as well as the PSA applications for operational safety improvement. Regulatory reviews are in charge of the Korean regulatory body, KINS (Korea Institute of Nuclear Safety). Recently, an ambitious, integrated plan by KINS has been established in order to improve the regulatory decision making process utilizing risk insights provided by PSAs.

2.2.12 Japan

Methodology development and application of Probabilistic Safety Assessment (PSA) have been mainly performed by the following organizations.

- Utilities: Ten utility companies in Japan operate nuclear power plants and have performed PSA of their plants. Development of PSA methodologies were performed mainly by their cooperative projects for PWRs and/or BWRs and developed methodologies were applied to plants of each company.

- Japan Nuclear Energy Safety Organization (JNES)[2]: JNES develops PSA methodology and performs PSA for representative plants in assistance to the regulatory activities of Nuclear and Industrial Safety Agency (NISA) of the Ministry of Economy, Trade and Industry (METI).

- Japan Atomic Energy Agency (JAEA)[3]: The nuclear safety research centre of JAEA is conducting PSA research under the safety research plans of the nuclear safety commission (NSC) for the purpose of providing assistance to NSC and other regulatory organizations. JAEA has also PSA programs in its research centre for future nuclear system as part of the development of FBRs.

The safety of Nuclear Power Plants (NPPs) in Japan is secured by stringent safety regulations based on the deterministic method, minimizing the possibility of a severe accident to a technologically negligible level. Though PSA is recognized as the convincing tool of supplementing the deterministic method to discuss balanced design and procedures and examine accident management (AM) of NPPs, PSA itself is not required in the current regulatory procedures. With the progress of PSA technology and study of severe accident phenomenology, application area of PSA has been expanded as follows in Japan.

(1) Since 1992, AM strategy has been made based on PSA; namely AM measures have been extracted based on PSA results and the effectiveness of the AM implemented has been confirmed by PSA.

(2) Since 1992, in periodic safety review (PSR), PSAs for both full power and shutdown operations have been made to assess the current plant situation of safety every ten years.

(3) In conjunction with above activities, PSA procedures guides for PSA at full power operation and shutdown operation have been prepared by the Nuclear Safety Research Association (NSRA) and the Atomic Energy Society of Japan (AESJ), respectively.

(4) Regarding pipe rupture incident at Hamaoka Nuclear Power Station Unit-1 Ministry of Economy, Trade and Industry (METI) requested NUPEC to carry out a PSA study for evaluating the risk significance of incident and corrective actions taken or to be taken.

(5) Judging from the fact that the risk informed regulation is expected in future, a subcommittee of AESJ initiated activities to prepare a Procedures Guide for level 1 and 2 PSAs of NPPs during rated power operation in March 2003.

(6) Under these circumstances, in November 2003, NSC decided the basic policy to introduce the risk informed regulation (RIR) concept in nuclear regulation in Japan.

(7) In December 2003, NSC proposed safety goals. The objective of the safety goals is to reasonably limit the public risk posed by nuclear accidents.

(8) In response to the above NSC basic policy, NISA, in collaboration with JNES, established Basic Concepts for RIR after receiving the public comments in May 2005.

(9) NISA and JNES also issued a Near Term Implementation Plan in May 2005 to embody RIR.

(10) The performance goals for light water reactor (LWR) are discussed at the performance goals subcommittee of the safety goals committee of NSC.

(11) Subcommittees of AESJ initiated activities to prepare Standards for level 1 seismic PSA and level 3 PSA of NPPs in 2004 and the works expect completion in 2007.

(12) Japan Nuclear Technology Institute (JANTI) was established in March 2005 to promote

---

2 The Nuclear Power Engineering Corporation (NUPEC)'s activities were succeeded by the Japan Nuclear Energy Safety Organization (JNES) when it was established in October 2003.

3 Japan Atomic Energy Research Institute（JAERI）and Japan Nuclear Cycle Development Institute（JNC）have been unified and become JAEA on October 1st, 2005.

nuclear industry circles to improve self-driven activity for nuclear safety, to re-establish trust on nuclear industries and activate the nuclear industry.

(13) NISA established High-Level Guidelines and PSA Quality Guidelines for RIR in collaboration with JNES in April 2006.

(14) NSC issued the revision of the examination guide for seismic design of nuclear power reactor facilities on September 19, 2006, reflecting the significant technical advancements such as advancement of the technologies for the geological investigation for the active faults. The new guideline is applied to the regulation for the reactor construction in the future, but NISA required the utilities to make a review on the seismic safety of the existing nuclear facilities based on the new guideline and to report NISA the results of their reviews, including evaluation of the residual risk of the facilities by seismic PSA.

(15) Subcommittees of AESJ initiated activities to prepare Standard of Parameter Estimation for PSA and Risk Information Application Guideline, in October and November, 2004, respectively.

(16) A new inspection system will start in April, 2008 based on preservation programs, placing emphasis on inspection on the important items from the viewpoint of safety. The risk information will be used to define the importance of maintenance, safety significance for findings during inspection and so on.

(17) The Implementation Plan established in 2005 was revised in January, 2007 mainly because the new inspection system will adopt risk information in safety preservation activities, safety significance determination and so on.

2.2.13 Italy

In Italy there are no Nuclear Power Plants in operation - after the Chernobyl accident the Government took the decision to shutdown the operating nuclear power plants and stop the construction of new ones -.

As consequence the activity and the research related to PSA aspects underwent a significant reduction, the remaining activities were aimed principally at maintaining competences and skills, as well as R&D capabilities.

However in the nineties ENEL (Italian National Electric Utility), APAT (the National Agency for Environment Protection and for Technical Services acting as Nuclear Regulatory Body) and ENEA (Italian National Agency for New Technologies, Energy and the Environment, a national research body) have been involved in the safety assessment on the probabilistic standpoint of the so called Innovative Reactors, like SBWR, AP 600 and PIUS through a series of international collaborations with industries, utilities and research organisations.

2.2.14 Hungary

The Hungarian legislative framework of the peaceful application of the nuclear energy is defined by the Act No. CXVI/1996 on Atomic Energy and the subsequent Governmental Decrees No. 114/2003 (VII. 29.) and 89/2005 (V. 5.). None of these legal items contain explicit requirements on performing and/or application of probabilistic safety assessment for the safety evaluation of the nuclear power plant in Hungary.

Six volumes of Nuclear Safety Codes (NSC) were issued as appendices to the Governmental Decree No. 89/2005 (V. 5.) on the Nuclear Safety Requirements of the nuclear Installations and Related Regulatory Activities. These six volumes contain a very detailed set of technical requirements on nuclear safety. All requirements in the volumes of NSCs are obligatory to meet for both sides – the licensees and the regulatory body. The nuclear safety requirements are regularly updated and maintained at the state-of-the-art level of the international practice. In this the corresponding IAEA, OECD NEA and EU publications are taken into consideration and the practices of leading national regulatory bodies are followed.

Nuclear Safety Guidelines are issued by the Hungarian nuclear safety regulatory authority (Nuclear Safety Directorate of the Hungarian Atomic Energy Authority – HAEA NSD) to explain several areas of the nuclear safety requirements and to show pragmatic example on the way of fulfilment of the requirements. The guidelines by their legal status are not obligatory only recommended; the licensees may follow other means to meet the nuclear safety requirements.

The nuclear safety requirements related to a nuclear power plant are collected in the first four volumes of NSC. Volume 3 deals with the design requirements of a nuclear power plant and it contains several prescriptions in relation to the PSA. In its Chapter 3.4.5. Probabilistic Safety Assessment it contains requirements providing the framework of constructing a PSA model. Level 1 and 2 PSAs are required for a nuclear power plant covering all operational states, modes and initiating events. It is stated that in PSA analyses best estimate approach shall be followed and where it cannot be applied there reasonable assumptions shall be considered. General requirements are given related to the data, the human failure and common cause modelling applied in the PSA. According to the requirements uncertainty and sensitivity analysis of the results shall be performed. On the other hand no requirements are contained on the quality of PSA and on the use of PSA and its applications.

Nuclear Safety Guideline No 3.11 is to be issued in the very near future (2006 third quarter) on the PSA quality recommendations and on how to prepare PSA models and tools for all initiating events and operational states.

During the decision making in all of its regulatory areas the HAEA NSD follows deterministic principles, examines if rules and criteria derived from deterministic safety analyses performed with conservative assumptions are met. On the other hand the HAEA NSD has been referring since a long time in many articles of its safety policy to the application of PSA results, to the consistent consideration of risk aspects during the regulatory decision making. The HAEA NSD has decided to follow the good international practices, therefore an Implementation Plan has been produced to define the necessary steps towards the risk-informed regulation and to co-ordinate its realisation. Following the actions foreseen in the Implementation Plan a nation wide project has been launched for the time period 2003-2008, in which the technical support organisations in the area of PSA and the Paks NPP are involved as well.

2.2.15 Germany

The use of probabilistic methods for nuclear safety assessment has a long tradition in Germany. The first "Risk Study", in current terminology a "Level 3 PSA", has been published in 1979. This study and the second phase of this study, which was completed in 1989, had significant influence on the design and operation of German nuclear power plants (NPPs). Particularly, the installation of accident management measures - as a fourth level of defense - was initiated as a result of PSA insights.

Since 1989 "Periodic Safety Reviews" (PSR) have been performed for all operating NPPs in Germany. For most of them the PSR was performed voluntarily by the utilities. The PSR was made obligatory by the operating license only for six of the most recent plants (out of nineteen in total). From the beginning, a "Level 1+" PSA has been an essential part of the assessment for the PSR.

In the German PSA Guideline, first published in 1996, scope and methods of the PSA for the PSR have been described. The Level 1+ PSA was to be performed for full power states, not including internal area events (fire, flooding) and external events. The "+" in "Level 1+" indicates the fact that the active functions of the containment isolation are included in the analysis. A revised version of the German PSA Guideline for Level 1 (power operation, low power and shutdown states) and Level 2 (only power states) was published in 2005, including internal area events (fire, flooding) and external events.

Most of the Level 1 PSAs have been performed by KWU resp. FRAMATOME on behalf of the utilities and reviewed by expert organizations on behalf of the regulators. Level 1 PSA studies have been performed by GRS as research projects for several plants (Obrigheim, Biblis B, Gundremmingen (B and C), Neckarwestheim 2 and Philippsburg 1).

Since the amendment of the Atomic Energy Act in April 2002 probabilistic safety analyses are an obligatory part of the (Periodic) Safety Reviews (SR) mandatory to be performed for all NPPs in Germany at a time interval of ten years.

Level 2 PSA studies have been performed by GRS as research projects for several plants (BWR-1300, PWR-1300 Konvoi - Neckarwestheim 2 and BWR-900 type 69 - Philippsburg 1). Partly based on this experience, the German PSA Guideline has been amended (2005). It now covers PSA level 1 for full power and shutdown states, including internal and external initiating events, in particular a fire PSA and a seismic PSA, and PSA level 2 for full power states.

There is neither a formally issued regulatory policy on PSA, nor has a risk-informed approach formally been introduced. The objective of the PSA is mainly to confirm the robustness of the deterministic design of the NPPs, to identify design and/or operational weaknesses (if any), and to address these weaknesses if necessary. In that way, the deterministic and probabilistic approaches are used in a complementary way..

2.2.16 France

The safety of French nuclear reactors is based essentially on a deterministic approach. In the past years, PSA studies have been performed out of the regulatory framework. PSA was not required by the Safety Authority and was carried out as an aid for safety analysis.

It has to be noted that France holds a rather unique position with a large, highly standardized reactor fleet, built by a single constructor and operated by a single operator. This situation has provided favourable conditions for the application of PSAs to power reactors since the 80s, explaining also the rather not prescriptive regulation, which is more a continuous technical dialogue between the regulators and the operators.

On a voluntary basis, two level 1 PSA studies were completed in 1990, one for a standardised 900 MWe PWR and one for a 1300 MWe PWR, respectively by IRSN (Technical support of the Safet Authority) and by EDF (the operator).

Many applications of these studies have been performed, leading to important safety improvements and plant modifications and backfits. PSA is now recognised as an important tool for safety analysis.

Due to the increasing role of PSA in the regulatory process, the safety authority decided the redaction of a basic safety rule related to “Development and Utilisation of Probabilistic Safety Assessments” in France. The basic safety rule was issued on December 2002. The text of this safety rule can be read on the French Safety authority website: http://www.asn.gouv.fr/.

The Basic Safety Rule describes the acceptable PSA methods and applications which have already been used and validated. For that reason the scope is limited to PSA level 1 and internal initiating events, and will be extended in the future as appropriate.

An important point is that the Basic Safety Rule introduces the notion of “Reference PSA”, developed by the operator for each plant series and reviewed by the regulators. A summary of the reference PSA results has to be included in the Safety Report.

In parallel to PSA applications, EDF and IRSN are still working on PSA developments. These developments concern updating of existing studies (based on plant modifications, new data and new knowledge), extension of the scope of the studies (level 2, internal and external hazards), PSA for 1450 MWe PWR and other designs (EPR), and methodology improvement.

2.2.17 Finland

The essence of the risk informed regulation and safety management is that the Living PSA works as an interactive communication platform between the licensee and STUK. Accordingly a PSA model, performed by the licensee and reviewed by STUK, is used for resolution of safety issues by both parties. For this purpose the licensees provide STUK with the PSA model in electronic form and regularly maintain and update it. There is no conflict of interest between STUK and the licensees on how to use PSA for the risk informed regulation (STUK) and safety management (the Licensee) because both are using the same PSA models which have been accepted by STUK after a thorough review process. In the regulatory process the deterministic and probabilistic approaches work in parallel. In addition the deterministic and probabilistic approaches interact. First of all the results of deterministic assessment provide necessary input for models and data used in PSA. Secondly PSA provides insights on adequacy of design requirements and design basis and thirdly PSA provides assessment on the need to improve the reliability of safety functions and plant systems.

In the course of the years the use of risk information has been evolved and experiences accumulated and today the use of PSA is aimed at running through the design, construction and operation phases. Accordingly a plant specific, design phase level 1 and 2 PSA is required as a prerequisite for issuing the construction licence for a new NPP designs and a complete level 1 and 2 PSA for issuing the operating licence as stated in the regulatory guide YVL2.8. The plant specific level 1 and 2 PSA includes internal initiators, fires, flooding, harsh weather conditions and seismic events for full power operation mode and for low power and shutdown mode. The regulatory guide YVL 2.8 includes general guidelines for ensuring the quality of PSA. STUK will review the PSAs and makes an assessment of the acceptability of the design phase PSA/ construction phase PSA prior to giving a statement about the construction licence/operating licence application. This approach is used in the licensing process of OL 3 EPR plant unit.

2.2.18 Czech Republic

There is not any legal requirement to perform PSA studies by licensee in the Czech Republic. Regulatory body is still building up its own position in this field and therefore PSA activities are mainly initiated by utility based on NPP needs, experience of other countries and taking into account regulatory recommendations. The PSA performance is conducted completely on voluntary basis by the plant operator to enhance the safety level of the plant operation in the frame of existing safety culture environment.

In the Czech Republic there are two WWER sites (Dukovany /4 x WWER 440/213/ and Temelin /2x WWER 1000/320/).

A basic PSA study as a first step of typical PSA programme, was for NPP Dukovany unit 1 completed in 1995 /initial version in 1993/. The study was performed for internal initiators and full power operation. Since that milestone a “Living” PSA programme has come into force at the site.

Temelin NPP basic PSA study was completed in 1996 for all operating modes and internal and external events and updated in 2002.

The PSAs are being performed by teams consist of NPP staff and technical support organisations experts.

Main purpose of the studies that have been produced was identification of weak points and start to build up a base for further PSA applications. The aims of PSA studies and models have been changed with time and the main present role is a support in adequate way of risk informed applications and decisions making which are complementary to deterministic ones.

QA systems implemented within the studies include internal and external reviews. The regulatory review was performed for both PSAs by external consultant company in 2005 with aim to confirm applicability of studies and models for PSA applications. Both PSA studies have also been reviewed by IAEA IPSART teams.

2.2.19 Canada

The Canadian regulator, namely the Canadian Nuclear Safety Commission (CNSC), has the mandate to manage the risk in the public's interest as defined in the Nuclear Safety Control Act and regulations [1].

The CNSC published back in April 2005 the Regulatory Policy P-299 "Regulatory Fundamentals" [2] that contains those principles that govern the regulatory approach to regulating the Canadian nuclear industry. The considerations of risk are clearly described in this document that states that the CNSC:

- regulates persons, organizations and activities that are subject to the Act and regulations in a manner that is consistent with the risk posed by the regulated activity;
- recognizes that the risk must be considered in the context of the CNSC's mandate under the Act; and
- makes regulatory decisions and allocates resources for regulatory activities.

Consistent with the intent of this policy, the CNSC is in full process of risk informing the decision making process. As part of this process, the CNSC produced a set of documents aimed to define and apply the risk informed approach within the nuclear power reactor activities. In this approach, the PSA is recognized as a valuable instrument in the Risk-Informed Decision Making (RIDM) process, bringing insights that complement the traditional safety approach. Over the last years, the two safety assessment methods, probabilistic and deterministic, have been used increasingly, as their strengths, limits, and complementary values are better understood.

As a result of the PSA's increasing role in the decision making process as practiced by both the regulator (CNSC) and the nuclear industry, the PSA Level 2 has become a regulatory requirement included in the Regulatory Standard S-294 [2], published in April 2005. This regulatory document will be part of the licence of each of the licensees once the term of renewal arrives (more details are presented in Section 4).

The CNSC does not develop PSAs. Nevertheless, all the PSAs received from the licensees are converted on CNSC PSA specific computer codes (i.e., Saphire, Risk Spectrum, Cafta). The effort to make the conversion depends on the PSA models. For instance, one of the early PSAs (BBRA) required re-work of the event trees and the associated modification for integration with fault trees [3] to fit into Saphire.

Over the last two decades the licensees with multi-unit Canadian nuclear power plants have developed Level 3 PSAs (see Figure 1). Depending on the study, the PSA has been either developed within the organization that owns the PSA with the support of contractors, or performed by the contractors as leads. In general, the major work for operating plants is produced by the same contractors (e.g., NSS/NNC, and AECL).

In the past, the CNSC performed only off-line reviews of the PSAs. In the last years, the situation has changed. The remaining PSAs for operating plants (e.g., Gentilly-2, and Point Lepreau) and new design (Advanced Candu Reactor - ACR) are being reviewed on-line by CNSC.

2.2.20 Belgium

The legislative and regulatory framework has been put progressively in place since 1955. The law of 15 April 1994, replacing the law of 29 March 1958, very generally outlines the protection of the population and the environment against the dangers of ionising radiation. The detailed stipulations are given in the Royal Decree (R.D.) of 20 July 2001, replacing the R.D. of 28 February 1963, "providing the General Regulations regarding protection of the population, workers, and environment against the dangers of ionising radiation".

In 1975, when the decision was taken to build four more nuclear units (Doel 3-Tihange 2 and Doel 4-Tihange 3), the Belgian Nuclear Safety Commission decided that the American nuclear safety rules would be applied, and this according to a schedule consistent with their date of issue, and that a number of external accidents be considered in a deterministic manner (crash of civil or military aircraft, gas explosion, toxic cloud, large fire, ...). The whole safety analysis of these units was conducted on these bases, applying the USNRC regulation and guidance. Deviations, if accepted, were documented.

For the existing nuclear power plants (NPPs), a periodic safety revaluation (PSR) has to be performed every ten years. In this context, a plant specific PSA has been performed for each plant. Also the PSA update of scope and methodologies will be linked to the periodic safety reviews, while updates of models will be done on a continuous way are also foreseen. More information on the integration of PSA in the PSR projects can be found in a recent paper presented at PSAM7.

For future NPPs, a PSA will be required from the licensing phase on.

There is no formally issued regulatory policy on PSA, nor has a risk-informed approach formally been introduced.

The objective of the PSAs is mainly to confirm the robustness of the deterministic design of the NPPs, to identify design and/or operational weaknesses (if any), and to address these weaknesses if necessary. In that way, the deterministic and probabilistic approaches are used in a complementary way.

The PSAs for the Doel and Tihange plants are performed by Tractebel Engineering (TE), the architect-engineer of these plants, on behalf of the utility Electrabel. AVN, as regulatory organisation, is performing an on-line review of the development and the updating of the PSA models. This means that technical documents (e.g. proposed methodologies, documents describing event tree construction, system reliability studies, etc.) are transmitted continuously to AVN for review. They are discussed with TE and the utility on an interactive basis. At the end of the project (after publication by TE of the final report) AVN establishes a PSA evaluation report.

3 NUMERICAL SAFETY CRITERIA

3.1 Summary

Status of the Numerical Safety Criteria

There are differences in the status of the numerical safety criteria that have been defined in different countries. Some have been defined in law and are mandatory, some have been defined by the regulatory authority (which is the case in the majority of countries where numerical safety criteria have been defined), some have been defined by an authoritative body such as a Presidents Commission and some have been defined by plant operators or designers. Hence there is a difference in the status of the numerical safety criteria which range from mandatory requirements that need to be addressed in law to informal criteria that have been proposed by plant operators or designers for guidance only.

There are a variety of reasons for defining the criteria which includes:

- a change in the law to introduce risk management into the environmental policy,
- the need to define an acceptable level of safety for nuclear power plants following an accident,
- a recommendation from a public enquiry to build a new plant, and
- the need for guidance for improving old plants or designing new ones.

In some countries, high level qualitative and quantitative guidance has been defined and has been used to derive lower level or surrogate criteria than are easier to address and are sufficient to demonstrate that the higher level criteria are met.

In some countries, criteria have been defined for existing plants and for new plants. In general, the expectation is that the target/ objective for the level of risk from a new plant should be about an order of magnitude lower than for existing plants.

In a number of countries no numerical safety criteria have been defined. However, there is a general requirement that the level of risk should be comparable to (or lower than) the risk from existing plants for which a PSA is available.

Framework for Defining the Numerical Safety Criteria

In most of the countries in which numerical safety criteria have been defined they have been defined as a “target”, an “objective” or a “goal” where the recommendation is that the risk should be lower than the prescribed value with no guidance given on what action needs to be taken if it is exceeded.

However, in the UK, a comprehensive framework has been defined for managing the risk arising from a nuclear power plant (or any industrial activity). This identifies three levels of risk: an unacceptably high level of risk where operation of the plant would not normally be allowed; a very low level of risk which is broadly acceptable and below which the regulatory authority would not seek further improvements to be made to reduce the risk; and an intermediate level where the risk would need to be reduced to a level that was as low as reasonably practicable (ALARP). For each of the risk measures addressed two numerical values are defined: a Basic Safety Limit (BSL) above which the risk would be unacceptably high; and a Basic Safety Objective (BSO) below which the risk is broadly acceptable.

Metrics for Defining the Numerical Safety Criteria

The way that the safety criteria have been defined ranges from high level qualitative and quantitative requirements relating to individual and societal risk for members of the public to lower level criteria relating to core damage, a large release or a large early release of radioactivity to the environment, and radiation doses to an individual living near the plant.

The high level qualitative criteria state that the additional health effects to the public from operation of the nuclear power plant should not lead to a significant increase in the risk of death of members of the public. The high level quantitative goals state that the level of increase should be less than about 0.1% of the existing risks.

In some countries the risk criteria are defined for individual members of the public and for societal risks involving 10 or 100 members of the public. The societal risks are sometimes defined as acute fatalities that occur in a short time after the accident or in the longer term.

The most common metrics used are core damage frequency (CDF) and large release frequency (LRF) or large early release frequency (LERF). In some cases these criteria have been defined as surrogates for higher level metrics and some cases they have been defined in their own right.

Societal Risk Criteria

Societal risk criteria have been defined in the UK and the Netherlands as shown in Table 3-1. These have been defined in terms of the number of fatalities.

TABLE 3-1: Summary of numerical criteria defined for societal risk [1]

Country	**Organisation**	**Risk metric**	**Frequency**	**Limit/ objective**
UK	Regulator	100 deaths	10^{-5} /yr 10^{-7} /yr	Limit Objective
Netherlands	Law	10 deaths 100 deaths [2]	10^{-5} /yr 10^{-7} /yr	Limit Limit

[1] Some countries like Japan also consider the impact to the whole society such as economical effects or land contamination

[2] The frequency at which 10 fatalities occurs should be less than 10^{-5} /yr. If the number of fatalities is increased by a factor n then the frequency should decrease by a factor n^2.

In both cases the frequency for 100 deaths is given as 10^{-7} /yr. However the definition of the two criteria is quite different as follows.

UK	**Netherlands**
Objective which may be exceeded if the risk can be shown to be ALARP	Limit
Early or late deaths	Acute deaths (within a few weeks)
Calculated over 100 years	Long term effects not included
Includes on- and off-site fatalities; relates to UK population only	Off-site fatalities
Credit taken for short and long term countermeasures including food bans	No countermeasures

In the USA, the qualitative criterion has been defined that the risk to society from generating electricity using nuclear power should be comparable with that from generating electricity by other sources and should not be a significant addition to other societal risks, and the quantitative criterion that the risk of death should be <0.1% of the sum of cancer fatalities from other sources. Similar quantitative criterion have also been defined in Korea.

Individual Risk Criteria

A criterion for the risk of death for an individual member of the public has been defined in a number of countries. This is summarised in Table 3-2.

TABLE 3-2: Summary of numerical criteria defined for individual risk

Country	Organisation	Frequency	Limit/ objective	Notes
UK	Regulator	10^{-4} /yr 10^{-6} /yr	Limit Objective	Credit can be taken for countermeasures Does not specify early or late deaths
Netherlands		10^{-5} /yr 10^{-6} /yr	Limit, all sources Limit, single source	Early or late death, no countermeasures
Japan	NSC	10^{-6} /yr	Objective	Acute fatality in the vicinity of the site boundary
		10^{-6} /yr	Objective	Late fatality within a certain distance of the site
Canada	Licensee	10^{-4} /yr 10^{-5} /yr	Limit for existing plants Objective for existing plants	Late fatality

In the USA, the qualitative criterion has been defined that there should be no significant increase in the risk of death for individual members of the public and the quantitative criterion that the risk of prompt death should be <0.1% of the risk of death from other types of accidents. The quantitative criterion has also been defined in Korea relating to prompt fatality.

There are differences in the way that these criteria have been defined depending on whether the criteria relate to: acute effects leading to early death or late effects leading to eventual death; whether the consequences should take account of countermeasures such as sheltering, taking stable iodine tablets and evacuation; and whether the numerical values defined are limits or objectives.

Core Damage Frequency

The numerical criteria defined for CDF are summarised in the Table 3-3.

TABLE 3-3: Summary of numerical criteria defined for core damage frequency

Country	**Organisation**	**Frequency**	**Notes**
USA	Regulator	10^{-4} /yr	Objective
UK [1]	Regulator	10^{-4} /yr 10^{-5} /yr	Limit Objective
Taiwan	Licensee	10^{-5} /yr	Limit
Switzerland	Law	10^{-5} /yr	Limit for new plants Objective for existing plants
Sweden	Licensee	10^{-5} /yr – level 1 studies	Objective This is a criteria or safety goal established by the licensees, for CDF from level 1 PSA:s.
Sweden	Licensee	10^{-5} /yr	Objective
Slovak Rep	Regulator	10^{-4} /yr	Objective
Netherlands	Regulator	10^{-4} /yr 10^{-6} /yr	Limit for existing plants Limit for new plants
Japan	Regulator	10^{-4} /yr	Objective
Italy	Regulator	10^{-5} to 10^{-6} /yr	Objective
Hungary	Regulator	10^{-5} /yr	Objective
France/ Germany	Designers of EPR	10^{-6} /yr	Objective
Finland	Regulator	10^{-5} /yr	Objective
Czech Rep	Licensee	10^{-4} /yr 10^{-5} /yr	Objective for existing plants Objective for new plants
Canada	Licensee	10^{-4} /yr 10^{-5} /yr 10^{-5} /yr	Limit for existing plants Objective for existing plants Objective for new plants

[1] This numerical safety criterion was defined in the Safety Assessment Principles published in 1992 but does not appear in the revised version of the document to be published in 2006.

There are differences in the way that these safety criteria have been defined as follows: some of the criteria have been defined in law, some have been defined by the regulatory authority and some have been defined by the licensees; some of the criteria have been defined as limits and some as objectives; some of the criteria differentiate between existing plants and new plants.

In some countries, no numerical value has been set but the overall requirement given than the CDF should be comparable with, or lower than, published values for comparable plants.

Large Early Release Frequency

The numerical criteria defined for LRF/ LERF are summarised in the Table 3-4.

TABLE 3-4: Summary of numerical criteria defined for large (early) release frequency				
Country	**Organisation**	**Risk metric**	**Frequency**	
UK	Regulator	10^4 TBq I_{131}, or 200 Tbq Cs_{137} or other isotopes	10^{-5} /yr 10^{-7} /yr	Limit Objective
Taiwan	Licensee	Not defined	10^{-6} /yr	Objective
Sweden	Licensee	>0.1% of core inventory	10^{-7} /yr	Objective This is a criteria or safety goal established by the licensees, for L(E)RF from level 2 PSA:s.
Sweden	Licensee	>0.1% of core inventory	10^{-7} /yr	Objective
Slovak Rep	Regulator	Not defined	10^{-5} /yr	Limit
Japan	Regulator	Containment failure	10^{-5} /yr	Objective
France	Regulator	Unacceptable consequences	10^{-6} /yr	Objective
France/ Germany	Designer of EPR	Not defined	Neg [2]	Objective
Finland	Regulator	100 TBq Cs_{137}	$5x10^{-7}$ /yr	Objective
Czech Rep	Licensee	Not defined	10^{-5} /yr 10^{-6} /yr	Objective for existing plants Objective for new plants
Canada	Licensee	>1% Cs_{137} >1% Cs_{137} 100 TBq Cs_{137}	10^{-5} /yr 10^{-6} /yr 10^{-6} /yr	Limit for existing plants Objective for existing plants Objective for new plants

[1] This numerical safety criterion was defined in the Safety Assessment Principles published in 1992 but does not appear in the revised version of the document to be published in 2006.

[2] The aim is that the sequences that lead to a large early release should be “practically eliminated”.

There are differences in the way that the metric for large release has been defined. This includes: quantities of particular radioactive isotopes; percentage of particular radioactive isotopes in the core; unacceptable consequences, and containment failure.

Some of the criteria relate to a large early release and some to a large early release. It is unclear from the information provide what is meant by “early”.

Other criteria

In one country, criteria relating to the risk to workers from accidents has been defined. This defines a limit and an objective for the risk of death and for the risk of receiving a dose in one on four dose bands.

Risk increases

Numerical criteria have been defined in some counties for the acceptable increases in risk from plant changes or outages during maintenance and repair. These follow the guidance given in Regulatory Guige 1.174.

Way Forward

There are differences in the numerical safety criteria that have been defined in the countries included in the survey. These differences include:

- the status of the criteria – that is whether they are mandatory or provide formal or informal guidance only,
- the way that the risk metrics have been defined and how they would be calculated,
- whether the criteria have been defined as limits or objectives, and
- differences in the numerical values cited.

The work carried out so far has not addressed the reasons for the way that the criteria have been defined and the reasons for the differences. This will be addressed by the WGRISK Task Group which has been set up.

3.2 Country replies

3.2.1 USA

As a result of the recommendations from the President's Commission on the Accident at Three Mile Island, the NRC issued a safety goals policy statement for nuclear power plants in 1986. This policy statement expressed safety policy using both qualitative and quantitative methods. The policy statement was not a regulation, but influenced various regulatory actions, primarily the development of the Regulatory Analysis Guidelines used to backfit analyses and the guidance developed for risk-informing reactor regulatory activities. The reactor Safety Goals broadly define an acceptable level of radiological risk and apply to reactor accidents and do not address environmental considerations, worker protection, routine operation, sabotage, non-reactor activities, or safeguards matters.

There is a level of safety that is referred to as "adequate protection." This is the level that must be assured without regard to cost and, thus, without invoking the procedures required by the NRC's Backfit Rule (10 CFR 50.109). Beyond adequate protection, if the NRC decides to consider enhancements to safety, costs must be considered, and the cost-benefit analysis required by the Backfit Rule must be performed. The Safety Goals, on the other hand, are silent on the issue of cost but do provide a definition of "how safe is safe enough" that should be seen as guidance on how far to go when proposing safety enhancements, including those to be considered under the Backfit Rule.

The Commission has established two qualitative safety goals, which are supported by two quantitative objectives. These two supporting objectives are based on the principle that nuclear risks should not be a significant addition to other societal risks.

The qualitative safety goals are as follows:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.
- The following quantitative objectives are to be used in determining achievement of the above safety goals:
- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1%) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.
- The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1%) of the sum of cancer fatality risks resulting from all other causes.

The Commission believes that this ratio of 0.1% appropriately reflects both of the qualitative goals to provide that individuals and society bear no significant additional risk. However, this does not necessarily mean that an additional risk that exceeds 0.1% would by itself constitute a significant additional risk. The 0.1% ratio to other risks is low enough to support an expectation that people living and working near nuclear power plants would have no special concern due to the plant's proximity.

In addition to the quantitative objectives discussed above, the NRC also identified a subsidiary objective on core damage frequency of 10^{-4} /reactor year. Subsequently a number of quantitative guidelines have been developed based on the quantitative objectives and the subsidiary objective for use in its regulatory activities. These include:

- The Regulatory Analysis Guidelines, NUREG/BR-0058, provide quantitative criteria on core damage frequency (CDF) and conditional containment failure probability to give guidance on whether to proceed with value-impact analysis for development of changes to the regulations.

- Regulatory Guide (RG) 1.174 introduces acceptance guidelines on CDF and changes in CDF, (Δ CDF) and large early release frequency (LERF) and changes in LERF (Δ LERF) for license amendments. (Regulatory guides provide guidance for licensees on an acceptable approach, but are not in themselves requirements.)

- Commission guidance on licensing new reactors introduces large release frequency (LRF) and conditional containment failure probability (CCFP) metrics and associated goals.

- NRC Management Directive (MD) 8.3 uses risk criteria to aid in determining the extent of follow up inspection activities for plant events.

- The Reactor Oversight Process (ROP), described in NUREG-1649, uses quantitative criteria to determine the risk significance of performance deficiencies as indicated by performance indicators or inspection findings.

3.2.2 United Kingdom

Tolerability of Risk from Nuclear Power Stations

Following a recommendation of the Sizewell B Public Inquiry that the HSE should "formulate and publish guidelines on the tolerability of levels of individual and societal risk to workers and the public from nuclear power stations", a document entitled "*The Tolerability of Risk from Nuclear Power Stations*" (TOR) was produced and issued for comment in February 1988, with the final version being issued in October 1992.

This specified a framework for defining the risk criteria which identified three regions of risk as follows:

- *unacceptable high* where the risk is regarded as intolerable and cannot be justified in any ordinary circumstances,
- *tolerable* where the nuclear plant would be allowed to operate provided that the associated risks have been reduced to a level that is as low as reasonably practicable (ALARP) such that the costs of further improvement would be grossly disproportionate to the reduction in the risk, and
- *low or broadly acceptable* where the risk is so small that the regulator need not seek further improvements provided that they are satisfied that these low levels are attained in practice.

Regarding the levels of risk which define these three regions, TOR proposed the following:

- 10^{-4} per year as the limit of tolerability for the risk of death for a worker on a nuclear plant,
- 10^{-5} per year as the benchmark for the risk of death for a member of the public from a new nuclear power plant, and
- 10^{-6} per year for the broadly acceptable level of risk of death for a member of the public,

and these numerical values were used as the basis of the accident frequency criteria given in the SAPs.

This was updated in 2001 in the publication *"Reducing Risks, Protecting People; HSE's Decision-Making Process"* which sets out an overall framework for decision taking by HSE which would ensure consistency and coherence across the full range of risks falling within the scope of the HSW Act. This framework is based on the approach described in TOR for nuclear power plants.

This report emphasises the role of Risk Assessment, both quantitative and qualitative, in the decision-making process and expands on the role of good practice in determining the control measures that must be put in place for addressing hazards.

Accident frequency criteria

The framework defined in TOR has been used as the basis for defining the numerical accident frequency criteria given in the NII Safety Assessment Principles (SAPs) (first published in 1988, revised in 1992 and 2006). The concept of a limit of tolerability has been translated into a *Basic Safety Limit* (BSL) so that the risk from the plant must be below this limit before it can be considered for licensing. In addition, a *Basic Safety Objective* (BSO) is defined which is the point beyond which the risk is so small that assessors need not seek further safety improvements. However, the licensee of the plant is still legally required to make further improvements where reasonably practicable.

Following the publications of the SAPs, the nuclear power plant operators updated their own Nuclear Safety Principles which are now formal company standards. They include numerical accident frequency criteria which are broadly equivalent to those defined in the SAPs.

SAPs Numerical Criteria (1992)

The 1992 revision of the SAPs chose to address the risks discussed in TOR supplemented by the consideration of societal effects of lesser accidents, and to emphasise defence in depth. A guiding aim was to focus assessment on the design and operation of the plant and to minimise the extent to which judgments on the safety of the plant depend on the numbers of people who live and work in the vicinity of the site. Hence, the risks of offsite consequences of accidents were not addressed directly, but rather via surrogate measures related to the plant so that a Level 3 PSA is not formally required. The numerical criteria defined, and still in use at the time of writing, are:

P42 Doses to the public: The total predicted frequencies of accidents on the plant, which would give doses to a person outside the site, should be less than the values given in the following table:

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	BSL	BSO
0.1 - 1	1	10^{-2}
1 - 10	10^{-1}	10^{-3}
10 - 100	10^{-2}	10^{-4}
100 - 1000	10^{-3}	10^{-5}
> 1000	10^{-4}	10^{-6}

Note. A subsidiary aim should be for no single class of accident to contribute more than about one tenth of the total frequency in any dose band, to avoid placing excessive reliance on particular features of the plant or on particular assumptions in the analysis.

The measure chosen to represent the severity of the accident is the maximum effective dose which would be received by a person at the nearest habitation which is typically 1 km downwind from the plant. This is considered to be a generally adequate surrogate for the whole range of offsite effects which an accident can lead to including the individual risk of death (prompt and delayed) and of other health effects to local people, contamination of land, disruption of people's lives from the application of countermeasures such as evacuation, fear and alarm in the general public, economic loss etc.

When account is taken of the variability of wind and weather conditions, a plant which just met the BSLs/ BSOs would give a maximum individual risk of death to a person outside the site of about 10^{-5} per year/ 10^{-7} per year respectively which meet the criteria given in TOR.

P43 Risk to workers: The total predicted individual risk of death (early or delayed) to any worker on the plant attributable to doses of radiation from accidents should be less than:

BSL	BSO
10^{-4} per year	10^{-6} per year

Note 1. It is recognised that the calculation of individual risk to workers may be difficult and hence only a broad estimate will normally be required, sufficient to show that the BSL is very unlikely to be exceeded and that ALARP has been appropriately applied.

Note 2. This principle is not intended to apply to personnel returning to perform recovery actions after an accident.

The risk of death to workers on the plant from accidents does not involve consideration of offsite effects, and so the individual risk is used directly. To maintain consistency with ICRP, the major part of the tolerable level of risk is allocated to normal operation, and hence the BSL for accidents in P43 is set out at 10^{-4} per year. The BSO value is chosen as 10^{-6} per year as being reasonably consistent with the broadly acceptable level of 10^{-6} per year in TOR, bearing in mind that, while the latter includes normal operation, it is directed principally at members of the public.

P44 Large release: The total predicted frequency of accidents on the plant with the potential to give a release to the environment of more than:

	10 000 TBq of Iodine 131
or	200 TBq of Caesium 137
or	quantities of any other isotope or mixture of isotopes which would lead to similar consequences to either of these

should be less than:

BSL	BSO
10^{-5} per year	10^{-7} per year

For a major accident, the dose to a person close to the plant may be into the range which would cause prompt death, so the particular level of dose is no longer an appropriate measure of its severity. In this situation the number of people affected and the land contamination become dominant concerns. A more appropriate surrogate for these effects, but one which is still related to the design and operation of the plant, is the quantity of radioactive material released in the accident.

The quantities or radioactive material chosen are consistent with the definition of a major accident given in TOR and in line with international thinking on large releases. The BSL frequency is consistent with the value proposed in the Barnes report for Hinkley Point C.

P45 - Plant damage: The total predicted frequency with which the plant suffers damage and a significant quantity of radioactive material is permitted to escape from its designed point of residence or confinement, in circumstances which pose a threat to the integrity of the next physical barrier to its release, should be less than:

BSL	BSO
10^{-4} per year	10^{-5} per year

Note. Such plant damage is interpreted as a degraded core in the case of a reactor. For other plant, it would include a major breach of vessel pipework etc, together with the potential for events such as fire, explosion, or aggressive chemical attack which might lead to degradation of the containing cell or its ventilation/ filtration system even though there may be a safety system provided to prevent such degradation.

This principle is included to reinforce the objective of defence-in-depth which looks for a series of physical barriers to a release of radioactive material. The safety of the plant should not rely predominantly on the integrity of the final barrier to the release: there should be sufficient reliability in each of the barriers to make a challenge to the final barrier very unlikely.

The BSL frequency is set at 10^{-4} per year on the basis of a judgement that a higher frequency would be intolerable in terms of the alarm, concern and loss of confidence that would be caused by such an accident, even without a release, and because it would indicate an intolerable weakness in the design of the plant or laxity in the control of its operation. The BSO frequency of 10^{-5} per year is that given in the same report as the goal for future plants.

P46 - Criticality incidents: The total predicted frequency of an accidental criticality excursion on a plant other than a nuclear reactor should be less than:

BSL	BSO
10^{-3} per year	10^{-4} per year

This principle also applies to plants handling or storing fissile material outside the reactor core on a nuclear power station.

This principle is included by analogy with P45 to address defence-in-depth for the protection of workers against radiation from accidental criticality incidents, which are an important concern on some non-reactor plants. Such an incident would represent a loss of control and might impose a challenge to the shielding and to the emergency arrangements for personnel protection. The potential consequences, however, are more limited than those of plant damage and so the BSL and BSO frequencies are set a factor of ten higher.

SAPs Numerical Criteria (2006)

Since their last review in 1992, experience in the use of the SAPs and developments in the field of nuclear safety, both internationally and in the UK, has led the NII to undertake a further thorough revision of all the principles including benchmarking against the current IAEA standards. This revision resulted in an updated version of the SAPs being issued for public consultation in April 2006. This new revision of the SAPs, whilst remaining applicable to all new nuclear facilities, makes greater provision for the decommissioning and radioactive waste management activities of the industry, and is also clearer in its application to submissions related to existing facilities.

The targets and legal limits presented in the revised SAPs (see below) are for normal operations, design basis analysis, individual risk and societal risk. The targets are not mandatory. Those few examples of levels that are derived directly from regulations are called legal limits, which are mandatory. While the targets are not legal limits, they are indicative figures that can guide assessors in judging whether there is a need for a more detailed analysis to demonstrate that risks have been reduced ALARP.

Risk to persons on-site

Target 5: The targets for the individual risk of death to a person on the site, from all on-site accidents that result in exposure to ionising radiation, are:

BSL:	10^{-4} per year
BSO:	10^{-6} per year

The majority of the tolerable level of risk to persons on-site is allocated to normal operation, and hence the BSL for accidents in Target 5 is set at 10^{-4} per year. The BSO value is chosen as 10^{-6} per year as being reasonably consistent with the broadly acceptable level in R2P2. The estimation of individual risk is, however, subject to assumptions regarding occupancy, shift-working etc and also does not clearly emphasise the importance of prevention rather than mitigation. Hence, assessors will also consider, particularly where estimated risks are low because of such factors, whether the event incidence is ALARP. (Note, Target 5 of 2006 SAPs is directly analogous to P43 of 1992 SAPs.)

Target 6 sets reasonable expectations for event frequency against dose, where it is assumed a worker could be present. Provided sufficient controls and/or alarms are in place, assessors take into account plausible countermeasures. This target also provides some measure of safety for groups of workers who might be affected in a single incident.

Target 6: The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person on the site, are:

Effective dose (mSv)	*Total predicted frequency (per year)*	
	BSL	BSO
2 – 20	10^{-1}	10^{-3}
20 - 200	10^{-2}	10^{-4}
200 - 2000	10^{-3}	10^{-5}
> 2000	10^{-4}	10^{-6}

For a given fault sequence, the maximum effective dose is the predicted dose to the worker who could potentially be most exposed to ionising radiation. The dose may be calculated using a best estimate approach. Where this is not practicable, reasonably conservative assumptions may be made. Simple assumptions about the radiation source(s), the location where the maximum potential exposure occurs, the exposure pathways and the exposure times, are used to give reasonable dose estimates. The effects of any mitigating action that can be justified may also be taken into account. For each fault sequence, the risk of death is determined using appropriate dose risk conversion factors and by taking account of the probability that an employee will be in the location where the potential exposure is greatest. The total predicted risk of death to a worker from accidents in a facility is the sum of the risks for all fault sequences associated with the facility.

Checks are made to ensure that the overall BSL level of 10^{-4} per year in Target 5 is not exceeded, particularly if there are dose bands where the predicted frequencies approach the BSL levels. In determining the risk to the most exposed worker on site, due account is taken of risk contributions from other facilities, where appropriate. It is acknowledged that the risk calculated in this way is likely to be greater than the risk to any particular individual worker in the facility or on site. Alternative methods and data, including the choice of dose/frequency bands, may be used to determine worker risks where they can be justified. This principle is not intended to include the risks associated with personnel returning to perform recovery actions after a radiation accident or emergency.

Risk to person off-site

Target 7: The targets for the individual risk of death to a person off the site, from all on-site accidents that result in exposure to ionising radiation, are:

BSL:	10^{-4} per year
BSO:	10^{-6} per year

The basis of Target 7 is that the individual risk to people off-site from accidents on the site should be considered. This requirement is supported by Target 8, which is facility-based, in the form of a dose ladder. The facility-based target allows consideration of safety submissions where the overall effect on the risk from the site is small. The individual risk levels in R2P2 include the risks arising from normal operational doses. To estimate the individual risk to a person outside the site, it is necessary to take account of a wide range of parameters such as the probability that a hypothetical person will receive the dose, given that the accident has occurred, allowing for the variability of wind and weather conditions and the effect of countermeasures. A particular issue is the physical position of the hypothetical person.

The dose ladder in Target 8 is based on the generally accepted premise that the larger the potential consequences of an accident, the smaller should be its frequency. The severity of the accident is represented by the effective dose that would be received by a hypothetical person. This can also be related to the countermeasures that may be needed.

Target 8: The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site, are:

Effective dose (mSv)	Total predicted frequency (per year)	
	BSL	BSO
0.1 - 1	1	10^{-2}
1 – 10	10^{-1}	10^{-3}
10 - 100	10^{-2}	10^{-4}
100 - 1000	10^{-3}	10^{-5}
> 1000	10^{-4}	10^{-6}

The facility's safety should be shown to be balanced, thus no single class of accident should make a disproportionate contribution to the overall risk, i.e. give rise to more than about one tenth of the frequency in each dose band. Also that as doses increase above about 1000 mSv then deterministic effects, including the possibility of prompt death, will start to become important. At a sufficiently high dose, deterministic effects will become more important in comparison with the risk of death from stochastic effects and for such accidents, societal risk levels should be considered as these could be the dominant targets.

The risks and frequencies in these numerical targets should, to the extent possible, be realistic estimates for the specified accidents occurring on the facility Whilst radiological analysis to evaluate maximum effective dose in PSA are carried out for a hypothetical person located at the distance of the nearest habitation or one km from the facility, whichever is nearer, or at the point of greatest dose if that is further away and that the person should be assumed to remain directly downwind of the release point for the duration of the release, also that the best estimate dose should be calculated as the expected value over the possible weather conditions. (Note, Target 8 of 2006 SAPs is directly analogous to P42 of 1992 SAPs.)

Societal Risk

As a measure of the societal concerns that would result from major accident, a target based on a representative accident leading to multiple fatalities is defined. The nature of the radiological effects of a major accident at a nuclear site will inevitably mean that long term, large distance stochastic effects are important, and the effect of weather must be considered. For this reason, the societal risk targets are based on the TOR considerations, though it is consistent with the R2P2 targets. These targets should be taken as indicative and do not replace the need for a detailed analysis to show that risks have been reduced 'so far as is reasonably practicable'.

Target 9: The targets for the total risk of 100 or more fatalities, either immediate or eventual, from all on-site accidents that result in exposure to ionising radiation, are:

BSL:	10^{-5} per year
BSO:	10^{-7} per year

The safety case should identify all accidents that result in source terms that can cause 100 or more deaths. The total risk is calculated taking account of the frequency distribution of the source terms together with probabilistic weather conditions. In estimating the risks all fatalities both on site and off site should be included. It is expected that a significant proportion of the fatalities resulting from these accidents will involve stochastic deaths, which are typically estimated using collective dose calculations. Based on advice from the Health Protection Agency (HPA), the integration of these effects should be over 100 years and restricted to the UK population. These assumptions are implicit in the targets.

Weather conditions are based on meteorological data appropriate to the site. Population data is based on current demography, but reasonable expectations for changes in the future are considered by sensitivity analyses. The ability to implement off-site countermeasures, particularly food bans, is taken into consideration in estimating the consequences. They should be based on current HPA advice and the ability to implement them should be justified.

Notwithstanding the target, to determine the effects on society from accidents on a site, the safety case must consider all accidents that can cause adverse health and safety effects. These should be included in an ALARP demonstration, together with the measures taken to reduce the effects on health and safety following the accidents, using if appropriate a Cost Benefit Analysis approach, to show that implementing further safety measures would not be reasonably practicable. (Note, Target 9 of 2006 SAPs is analogous to P44 of 1992 SAPs.)

It summary whilst the 1992 revision of the SAPs chose to focus the assessment on the design and operation of the plant and to minimise the extent to which judgments on the safety of the plant depend on the numbers of people who live and work in the vicinity of the site. The 2006 revision now directly addresses the risks of offsite consequences of accidents so that a Level 3 PSA is required.

Short Term Risks - Time at Risk

The above risk targets are given as frequencies based on annual averages, however it is recognised that for certain periods of time the use of annualised frequency targets may be unrealistic. These are generally where the risk exists for periods much shorter than a year and when risk is elevated for this period and a decision as to whether this is excessive and ALARP is maintained, or additional safety measures are needed, has to be made. In assessing such situations important factors are the:

- independence between the initiating event and the activity or operation being undertaken;
- the degree of control that the duty holder has over the initiating event and the activity or operations; and
- the degree to which the risk only arises due to the activity being undertaken (e.g. lifting operations).

Any period in which the risk is elevated (e.g. due to equipment unavailability or occupancy of hazardous areas) must be subject to a specific demonstration that risks are controlled ALARP. The period of elevated risk should be as short as reasonably practicable. The safety case is neither allowed to rely solely on numerical risk estimates or averaging risk over a longer period of time. The role of good engineering and operational practices must be prominent in the case. Sufficient protection based on engineering and operational considerations must be retained. If this is not reasonably practicable, adequate substitution arrangements have to be considered. The extent of protection is required to be commensurate with the level of risk at the time that it is present.

Any reasonably practicable step that can be taken to eliminate or mitigate a hazard should normally be taken irrespective of ‘time based’ arguments. During operations which impose a planned short term risk, means for monitoring the actual facility state must be in place to ensure that the mode of operation and the time during which it persists meet the assumptions in the case. Where possible, means to reverse the process are required to be in place in the event that it becomes apparent that assumptions of the safety case are not being met. Where reasonably practicable, contingencies should be identified that could cope if the situation deteriorates further, including accident management arrangements.

High risks that, if evaluated as continuous risks would exceed BSLs, should be avoided except in special circumstances. These circumstances are required to be rigorously justified in advance. They may include situations not originally foreseen in the design of the facility, or which are unavoidable because of the need to increase risks for a short time to reach a safer state in the long term. The extent of the time for which the risk is increased can not be argued as the sole argument for acceptability that a situation is ALARP. (Note, Short Term Risks and Time at Risk considerations are a new addition to 2006 SAPs, neither having been explicitly mentioned within the 1992 SAPs.)

3.2.3 Taiwan

There are 6 units in operation and 2 units under construction in Taiwan. No probabilistic safety criteria have been defined to evaluate the safety of the operating NPPs. For Lungman NPP which is now under construction, the Licensee has committed to TAEC that the plant design will meet the safety criteria with CDF <10^{-5} per year and LERF <10^{-6} per year. Thus, to obtain the operation licensee from TAEC, the Licensee should demonstrate in FSAR that the new built plant meets the safety criteria.

3.2.4 Switzerland

In February 2005, a new Nuclear Energy Law and an accompanying ordinance were enacted in Switzerland. The ordinance anchors PSA applications into the law and defines fundamental directions for the decision-making process relevant to PSA as follows:

- For the construction permit of new nuclear power plant, the applicants need to demonstrate that the estimated core damage frequency (CDF) is less than 10^{-5} per reactor-year. To the extent that is feasible and reasonably achievable, this CDF criterion is also expected to be met by the operating plants.
- The new Swiss nuclear energy act requires that sufficient preventive and mitigative measures shall be considered in order to ensure the safety of nuclear power plants in Switzerland. In order to demonstrate that sufficient measures have been considered, dose limits are defined according to the accident frequencies (see Section 7). It is outlined that, to the extent possible, the determination of the accident frequencies shall be based on the results of plant-specific PSAs.
- The risk impact of plant modifications, findings and events shall be assessed systematically using plant-specific PSAs.

This new ordinance requires the development of a guideline on PSA scope and quality and a guideline on PSA applications (see Section 4). For the assessment of the operational safety using plant-specific PSAs, additional numerical criteria will be developed as part of the guideline on PSA applications.

3.2.5 Sweden

The outcome of a probabilistic safety assessment (PSA) for a nuclear power plant is a combination of qualitative and quantitative results. Quantitative results are typically presented as Core Damage Frequency (CDF) and Large Early Release Frequency (LERF). In order to judge on the acceptability of results, various criteria for interpretation of results and assessment of their acceptability need to be defined. In Sweden, the goals have been set by the nuclear utilities.

In the USA, the NRC has issued Regulatory Guides defining target values for cases when a licensee wants to use PSA results as a basis for deviating from deterministic requirements. The interpretations of these criteria are most probably fetched from USA at the time when 10CFR50 was created and the born of civil use of nuclear power technology. The legal status of these criteria are indirectly accepted as a part of the design of domestic nuclear power plants, ones upon the time accepted by former SKI. The SKI interpretations of these criteria are that they are more guidelines, than requirements.

- The use of new developed safety criteria today and targets for them are part of the interpretation of the modern regulation in force in Sweden. It is a natural part of the interpretation of new regulations to test functional solutions by deterministic calculations. The possibilities to fulfil requirements may end up in new safety criteria.
- The SKI has not formally defined any numerical safety criteria. The reason for this is that SKI has promoted a "living safety concept" since the early beginning of the nuclear business in Sweden. With that SKI intend that safety in all the aspects have to be developed and maintained to better solutions and numbers, not that this process can stop when a certain goal is achieved.

The IAEA has issued a number of publications dealing with PSA and judgement of PSA results. The exact levels of the safety goals differ from organisation to organisation and between different countries. There may also be differences in the definition of the safety goal. Ultimately, these safety goals are intended to define acceptable levels of risk from operation of commercial nuclear power plants.

Safety demonstration of Swedish Nuclear Power Plants relies on deterministic principles and requirements documented in the Safety Analysis Reports of the individual NPPs. PSA is a supporting decision tool, used in complement with the deterministic approach.

The numerical safety criteria

At present there are quantitative safety goals / limits established at the Swedish NPPs, and they are as follows:

- The overall objectives are expressed in terms of "unacceptable consequences", but these "unacceptable consequences" are not specified by legislation or in regulations of SKI in terms of exact annual frequencies of occurrence.

However, SKI appraises this as a god way of working with safety and safety matters in general. The licensees have expressed safety goals to be followed for their own quality assurance of their own safety work, and they are;

The 10^{-5} /year value is an objective for the BWR and PWR plants, for the overall CDF frequency. Safe shutdown has to be demonstrated for this level. The 10^{-7} /year values for the BWR and PWR plants are for unplanned release of core inventory larger than 0.1% of the total core inventory exclusive noble gas. Such measures are given high priority at the licensees, to be able reach this established safety goals.

The dominating sequences to the total CDF shall not diverge more than a factor 10, from each other.

Some of the risk metrics used are :

- Level 1, core damage frequency (CDF)
- Level 2, large early / late release (LERF, LRF)
- Shutdown, refuelling, start-up modes, core damage frequency (CDF)
- Area events (fire, flooding), impact on core damage frequency (CDF)
- External events, their impact on the core damage frequency (CDF)
- Offsite doses, the risk metrics used are the amount of release of radioactive noble gases from the primary system. The amount accepted by the society is up to 0.1% of release products (e.g., CsI, CS, BAO, MoO2, noble gases) from the former Barsebäck 1 reactor

Other notices; In a research project recently started by the Nordic PSA Group (NPSAG) and SKI, in the so called "Validity of Safety Goals", the definitions and the history behind the safety goals used by licensees, regulators, PSA developers, practitioners etc, are investigated. The expected result from this project is to have a clearer picture of the validity and the interpretation of safety goals used today. In 2007, a SKI Report will be published on results from the phase 1 in this project.

3.2.6 Spain

No quantitative safety guidelines have been officially used in Spain. PSA results within the usual range of published results all over the world were intended and, in many cases, this intention was the basis for plant modifications. A legal goal might also have made the objective of the analysis to derive from identifying and making safety improvements to just trying to demonstrate the goal achievement.

However, for PSA applications quantitative acceptance criteria have been established in the Regulatory Guide (G.S. 1.14) for Core Damage Frequency (CDF) increase as well for Large Release Frequency (LRF) increases. For these LRF two types of risk increase has been defined, Large Early Release Frequency (LERF) and Large Late Release Frequency (LLRF) depending on the time of the release after the accident initiation. The LERF include the releases that have release fractions of volatile fission products equal o greater than 3% of the core inventory 12 hours after the accident initiation and the LLRF during 24 hours after the accident initiation. The risk increase criteria are similar to those established by the USNRC in the R.G. 1.174.

Also, cost benefit analysis is being applied in certain cases where the risk acceptance criteria are close to the risk increase limits.

3.2.7 Slovenia

Selected numerical safety criteria will be formally defined and come into operation when the update of the legislation has been completed. Now, on-line maintenance numerical criteria based on PSA are being used (as agreed between SNSA and the Krško NPP).

3.2.8 Slovak Republic

The guideline defines the PSA safety criteria on the level of safety system failure probability, core damage frequency (CDF), and large early release frequency (LERF). The failure probability of the safety system is considered to be unacceptable if it is higher than 10^{-3}. In case of reactor protection system the failure probability is unacceptable if it is higher than 10^{-5}. The baseline values of CDF and LERF are calculated from PSA models. The safety goal for them is 10^{-4} /year and 10^{-5}/year respectively.

The changes in CDF are considered non-risk significant:

- If the changes in CDF are less than 10^{-4} /year and their cumulative effect do not cause the safety goals to be exceeded; changes in the CDF greater than 10^{-4} /year are considered unacceptable.
- If the changes in LERF are less than 10^{-5} /year and their cumulative effect do not cause the safety goals to be exceeded; changes in the LERF greater than 10^{-5} /year are considered unacceptable.

3.2.9 Netherlands

The concept of risk management and risk assessment was first introduced in environmental policy in the 1986-1990 Long-term Programme for Environmental Management. This concept was reassessed following debates in parliament. As part of the Dutch National Environmental Policy Plan [Lower House of the States General, 1988-1989 session, 21137, Nos. 1-2, The Hague 1989], the Minister of Housing, Spatial Planning and the Environment, the Minister of Economic Affairs, the Minister of Agriculture, Nature Management and Fisheries, and the Minister of Transport, Public Works and Water Management set out a renewed risk management policy in a document called ‘Premises for Risk Management; Risk Limits in the Context of Environmental Policy’ [Lower House of the States General, 1988-1989 session, 21137, No. 5, The Hague 1989]. In the following year, a separate document was issued dealing with the risk associated with radiation: ‘Radiation Protection and Risk Management; Dutch Policy on the Protection of the Public and Workers against Ionising Radiation’ [Lower House of the States General, 1989-1990 session, 21483, No. 1, The Hague 1990]. These two documents still form the basis for government policy on risk management.

Numerical Safety Criteria included in Nuclear Energy Act.

The Nuclear Installations, Fissionable Materials and Ores Decree (Part of the Nuclear Energy Act) has recently been amended to incorporate this risk policy in the licensing process for nuclear installations. Risk criteria are explicitly included as assessment principles for licenses to be granted to nuclear power plants. The outcomes of a level-3 PSA must be compared with these risk criteria and objectives.

This concept of environmental risk management has the following objectives and steps:

- Verifying that pre-set criteria and objectives for individual and societal risk have been met. This includes identifying, quantifying and assessing the risk.
- Reducing the risk, where feasible, until an optimum level is reached (i.e. based on the ALARA principle).
- Maintaining the risk at this optimum level.

Normal operation

The dose limit due to normal operation of installations consists of a maximum total individual dose of 1 mSv in any year for the consequences of all anthropogenic sources of ionising radiation (i.e. NPPs, isotope laboratories, sealed sources, X-ray machines, etc). For a single source, the maximum individual dose has been set at 0.1 mSv per year. In addition, as a first step in the ALARA process, a general dose constraint for any single source has been prescribed at 0.04 mSv per year.

Design basis accidents

The public health risks due to incidents or accidents in the design basis area are also bound to the criteria of the individual risk concept. However, a conservative deterministic analysis of the respective design basis accidents is more effective than a PSA, which is based on a probabilistic approach, for the purpose of ensuring that the engineered safety features of a particular NPP are adequate. There are a number of reasons why a conservative, deterministic approach has certain advantages over a probabilistic approach:

Design basis accidents are postulated to encompass a whole range of related possible initiating events that can challenge the plant in a similar way. These other related initiating events do not therefore need to be analysed separately.

It is much easier to introduce the required conservatism. With a probabilistic approach, uncertainty analyses need to be performed to calculate confidence levels.

By definition, design basis accidents are events that are controlled successfully by the engineered safety features. Hence, they do not result in core melt scenarios, and are considered in a PSA as being ‘success sequences’. The related radioactive releases are negligible compared with the uncontrolled large releases associated with some of the beyond-design basis accidents. In other words, a general ‘state-of-the-art’ PSA, which focuses primarily on core melt scenarios and associated large off-site releases, does not take account of the consequences of design basis accidents.

Clearly, the above dose and risk criteria are not suitable for use as rigid criteria in the conservative and deterministic approach used in traditional accident analyses. A separate set of safety criteria was therefore formulated, as is prescribed by NVR 1.1, §1201. This set, which is part of the amended Nuclear Installations, Fissionable Materials and Ores Decree, are as follows:

Frequency of event (per year)	*Effective dose (H_{eff}, 50 years)*	
	Adult	Child (1 year old)
$F \geq 10^{-1}$	0.1 mSv	0.04 mSv
$10^{-1} > F \geq 10^{-2}$	1 mSv	0.4 mSv
$10^{-2} > F \geq 10^{-4}$	10 mSv	4 mSv
$F < 10^{-4}$	100 mSv	40 mSv

An additional limit of 500 mSv thyroid dose (H_{th}) must be observed in all cases.

Correspondingly the provisions concerning the dose related to normal operation as a first step in the ALARA process, a general dose constraint has been prescribed at values of 40% of the above mentioned.

Major accidents

For the prevention of major accidents, the maximum permissible level for the individual mortality risk (i.e. acute and/or late death) has been set at 10^{-5} per year for all sources together and 10^{-6} per year for a single source.

As far as major accidents are concerned, both the individual mortality risk and the group risk (societal risk) must be taken into account. In order to avoid large-scale disruptions to society, the probability of an accident in which at least 10 people suffer acute death is restricted to a level of 10^{-5} per year. If the number of fatalities increases by a factor of n, the probability should decrease by a factor of n^2. Acute death means death within a few weeks; long-term effects are not included in the group risk.

In demonstrating compliance with the risk criteria, one has to assume that only the usual forms of preventive action (i.e. fire brigades, hospitals, etc.) have been taken. Therefore risk reduction by evacuation, iodine prophylaxis and sheltering may not be included in these assumptions.

This risk management concept is used in licensing procedures for nuclear installations and all other applications of radiation sources. Guidelines for the calculation of the various risk levels have been drafted for all sources and situations. In principle, the calculations must be as realistic as possible (i.e. they should be 'best estimates').

For NPPs, this means that the level-3 PSA plays a leading role in the verification process. Specific procedure guides have therefore been drafted in The Netherlands for performing full-scope PSAs. The level-1 PSA guide is an amended version of the IAEA Safety Practice: 'Procedures for conducting level-1 PSAs' (Safety Series No. 50-P-4) and the level-2 guide is based on the IAEA Safety Practice: 'Procedures for conducting level-2 PSAs (Safety Series No. 50-P-8).

The procedure guide for level-3 PSAs is a specifically Dutch initiative, in which the COSYMA code for atmospheric dispersion and deposition is used. It gives instructions on the pathways which should be considered, the individuals (i.e. critical groups) for whom the risks should be assessed and the type of calculations which should be performed. It also describes how the results should be presented.

Since it has been recognised that PSAs produce figures that can be used as a yardstick in safety decisions, a number of countries have developed probabilistic safety criteria for PSA-level-1 applications. The regulatory body in The Netherlands has taken note of the INSAG-3 safety objective, i.e. the maximum acceptable frequency for core damage is 10^{-5} per year for new NPPs and 10^{-4} per year for existing NPPs. Recently this 10^{-5}/year figure for new NPPs was revised. In a recent letter to the Dutch parliament (September 2006) the government formulated boundary conditions for new NPPs. (Conditions for installing new nuclear power plants in The Netherlands; Lower House of the States General, 2006-2007session, 30000 No. 40, September 28, 2006) These boundary conditions were in the area of safety, environmental impact, radioactive waste, security and safeguards, environmental aspects of uranium mining and enrichment, knowledge infrastructure in The Netherlands and social aspects. Regarding safety several criteria were formulated.

- TCDF < 1.10^{-6}/year
- Provisions to prevent containment attack by the corium after core melt, e.g. a core-catcher
- Containment shall be able to withstand high containment pressures and the crash of a large airplane
- No preventive measures in the vicinity of the NPP necessary.

These boundary conditions are formulated with regard to the current state-of-the-art of NPP designs (generation III and III+). Every five to ten years these boundary conditions shall be re-evaluated with respect to the state-of-the-art at that time.

In addition, the objective of accident management strategies should be that the majority of potential accident releases will not require any immediate off-site action such as sheltering, iodine prophylaxis or evacuation. This means that the dose to which members of the public are exposed in the first 24 hours after the start of the release should not exceed 5 mSv. The PSA can help in fixing these figures. For example, the limit of 5 mSv was used as an acceptance criterion in the design of the containment emergency venting filter for the Borssele NPP.

Numerical Safety Criteria used by the licensee for operational decisions, AOT optimisation, configuration control etc.

In order:

- to master simultaneous component outages,
- to be able to reschedule component outages with high TCDF impact in a certain Plant Operating State to another refuelling operating state where the component outage has a lower impact, and
- to reduce the component outage duration during the refuelling outage by shifting to on-line maintenance,

the licensee of the Borssele plant has defined several numerical safety criteria as performance indicators (PIs). Evaluation of historic output of the Risk Monitor was used as a basis for these PIs. KFD has welcomed these criteria and will incorporate these in its policy plan on Risk Informed Regulation.

The PI for power operation:

- Total cumulative TCDF increase caused by planned as well as unplanned component outages should be <5%. The cumulative TCDF increase caused by planned component outages shall be <2%.
- [2]The PI for all operating states:
- Instantaneous TCDF shall never exceed the value of 10^{-4} /year.
- For optimisation of AOTs the licensee has adopted a value of $5x10^{-8}$ for ΔTCDF x AOT and ΔTCDF always <10^{-4} /year.

3.2.10 Mexico

Once the Individual Plant Examination for Laguna Verde was reviewed and approved by the CNSNS, and further based on the recommendations of the review team, it has been subject to an updating and improvement process. This will lead to a living PSA model that can be used to support different applications related with changes to the licensing basis, technical specifications and operational and maintenance activities.

The CNSNS initiated a project aimed at developing an adequate framework to evaluate the above applications. Based on the USNRC regulatory guides, the CNSNS has adapted and issued for trial purposes two Regulatory Guides, similar to the NRC/RG 1.174 and 1.177, which formally defines an approved methodology for using probabilistic safety assessment in risk informed decisions on permanent plant-specific changes to the licensing basis for Laguna Verde and for Technical Specifications changes. These regulatory guides establish numerical safety criteria as in the NRC guides.

For permanent changes, the risk acceptance guidelines established the rejection of applications that result in an increase in CDF above 10^{-5} per reactor year, and to accept those applications with a calculated CDF increase in the range of 10^{-6} to 10^{-5} per reactor year if it can be reasonably shown that the total CDF is less than 10^{-4} per reactor year. When the calculated increase in CDF is very small, less than 10^{-6} per reactor year, the change is acceptable regardless of whether there is a calculation or not of the total CDF, except in those cases when there is indication that the total CDF may be considerable higher than 10^{-4} per reactor year.

Regarding the large early release frequency, the applications are not acceptable if they result in an increase in LERF above 10^{-6} per reactor year. When the LERF calculated increase is in the range of 10^{-7} to 10^{-6} per reactor year the applications are accepted if it can be reasonably shown that the total LERF is less than 10^{-5} per reactor year. When the calculated increase in LERF is very small, less than 10^{-7} per reactor year, the change is accepted regardless of whether there is a calculation or not of the total LERF, except in those cases when there is indication that the LERF may be considerable higher than 10^{-5} per reactor year.

These guidelines are intended for comparison with a full-scope PSA, including internal events, external events, full power, low power, and shutdown, assessment of the change in CDF and LERF, and when necessary, as discussed above, the baseline value of this risk metrics.

3.2.11 Korea

No quantitative safety guidelines have been officially used in Korea. In some cases, e.g., in designing APR1400, the licensee adopted a design philosophy which ensures that the accident occurrence frequency is significantly reduced compared to that of the existing NPPs by maintaining the high reliability level of safety significant structures, systems, and components (SSCs). It was also required that core damage frequency, conditional containment failure probability, and offsite large radiological release frequency be maintained at a lower value to a practical extent, and any accident sequence or design feature not be greatly contributable to the overall plant risk with imbalance. Following these licensee's requirements, the regulatory interim guidelines for assuring adequate safety goals were issued:

- Criteria for setting up the safety goal shall be established to achieve the acceptable risk-tolerance and engineering conditions.
- Reference safety goals shall include core damage frequency, large off-site release frequency, and public health objectives in establishing safety limits or design acceptance criteria. While the safety goals can be selected for each area, such as full power and low power/shutdown, internal and external events according to the related accident conditions, consistency shall be maintained in selecting acceptance criteria.
- The safety goals can be established with consideration of uncertainty, and the adequacy of the confidence level shall be checked.

The SAP addresses the primary quantitative safety goals:

> *"The prompt fatality risk resulting from the accidents to an average individual in the vicinity of a NPP should not exceed one-tenth of one percent of the sum of those risks resulting from other accidents which members of the population might generally be encountered. In addition, the cancer fatality risk resulting from nuclear power plant operation to the population in the area near a NPP of cancer fatalities that might should not exceed one-tenth of one percent of the sum of cancer fatality risks resulting from all other causes."*

In order to practically introduce the above goals to NPPs, substantial safety goals in terms of risk should be imposed in near future in order to prevent core damage and to mitigate the risk of fission product release. KINS prepared the performance goals for preventing the damage of reactor core and reducing the radioactive materials release by the containment. These goals might be finalized when insights from domestic PSAs are completely gained.

3.2.12 Japan

Safety Goal

NSC stated in the White Paper on Nuclear Safety published in March, 1999, that NSC promotes the discussion on the establishment of safety goals from a comprehensive point of view, taking into consideration international trends and outcomes from various PSA studies.

In February 2001, NSC set up the special committee on safety goals and started discussion to establish safety goals and, in August 2003, the committee presented an interim report about the discussion until that time to NSC. The interim report proposed qualitative and quantitative safety goals and future efforts to investigate performance goals for each field of utilization of nuclear energy. In parallel with the activities of the committee, NSC held panel discussion meetings in several cities for communications with the public on safety goals. NSC placed the interim report for public comments for three months from September 5 to December 4 and finalized the report in January 2004.

The interim report defined the role of the safety goal as the quantitative definition of the level to which the risks of the utilization of nuclear energy are required to be controlled under the regulatory activities by the government. The proposed safety goals are common to all the nuclear facilities and activities that have potential adverse effects of radiation dose to the public. However the timings of applications of the safety goals to various types of activities are to be determined based on considerations of specific nature of risks and maturity of risk assessment technology for each type of activities.

The proposed safety goals consist of one qualitative goal and two quantitative goals as follows.

Qualitative Safety Goal:

The possibility of occurrence of release of radiation or release of radioactive material that lead to health effects to the public caused by utilization of nuclear energy should be limited to the level not to cause a meaningful increase in the public risk.

Quantitative Goals:

(i) The average risk of acute fatality due to nuclear accidents, which is posed to individuals of the public who live in the vicinity of the site boundary, should be less than the probability of approximately 10^{-6} per year.

(ii) The average risk of latent fatality by cancer due to nuclear accidents, which is posed to individuals of the public who live within a certain distance from the facility, should be less than the probability of approximately 10^{-6} per year.

Here the ‘nuclear accidents’ include ones not only caused by internal events but also caused by external events except for intentional man-made events. The precise definitions of ‘vicinity of the site boundary’ and ‘within a certain distance from the facility’ are not made yet. These goals will be applied to various safety issues as trial usage and will be finalized when their applicability is assured.

Of course compared with the quantitative goals are always risks evaluated for individual facilities. At present, however, the goals will not be used for direct judgment on whether individual facilities are safe enough but be used to judge the adequacy of the regulation referring to the risk numbers of these facilities. When risks of some facilities exceed the goals and those of other facilities do not, NSC and NISA will analyze and identify the reasons that resulted in such a difference. Then these organizations will consider possible revision of the regulatory rules and the safety of the individual facilities would be judged by revised rules. In this sense, the quantitative goals are reference levels with which adequate regulatory policies are discussed.

The reason why the quantitative goals are expressed by the 'approximate' numbers is to take into account the variability of PSA results for individual facilities due to the uncertainties in PSA and the variability in reasonably practicable safety measures at individual facilities. Even in the case where risks evaluated for some facilities are slightly larger (factor 2 will be used in the trial usage period.) than the quantitative goals, it does not automatically mean that the regulatory rules applied to those facilities are inadequate but can be adequate provided that reasonable safety measures are taken in those facilities.

Performance Goals

Safety performance objectives, which are compatible to the quantitative goals, are sought for every type of nuclear facilities and activities, e.g. nuclear power plants, reprocessing plants, high level radioactive waste disposal, etc., since direct application of health effect goals is not always easy.

The discussions to determine the performance goals for LWRs were started in September 2004 at the performance goals subcommittee of the special committee on safety goals. The subcommittee discussed various issues, including the appropriate parameters to be used as a measure of performance goals, the procedure to derive the values of performance goals from the safety goals, treatment of external events, treatment of multi-unit sites, and the areas for averaging the individual risks. In April 2006 the following parameters and parameter values were established as performance goals for NPPs.

Parameter Value 1. CDF : approximately 10^{-4} /year, and

Parameter Value 2. CFF : approximately 10^{-5} /year

where CDF is core damage frequency and CFF is containment failure frequency including bypass and isolation failure scenarios. These are for all types of initiating events including internal and external events but excluding intentional man-made hazards. The reason for using CFF and not using LERF (large early release frequency) is that, although the LERF has closer relationship to individual risks, the CFF gives more conservative assessment when the same value is taken for CFF and LERF and it is a way to cope with the uncertainties in the quantification of source terms and the effectiveness of emergency protective measures, etc.

The process of derivation of the parameter value for the CFF compatible to the health effect goal was as follows. Firstly the conditional probabilities of acute and cancer death fatality were calculated by a probabilistic consequence assessment methodology used for level 3 PSA of NPPs for a series of very large source terms (up to 20% of Caesium and Iodine inventory of 1100 MWe class LWR). Conservative assumptions were made on the effectiveness of emergency protection measures. The calculated average conditional probabilities of acute and cancer fatality of individuals in the vicinity of the NPP were less than 0.1. Secondly the conservatism of the upper limit value of 0.1 was confirmed by the results from level 3 PSAs for representative plant and site conditions in Japan. Using the value of 0.1 as the upper limit of conditional probability of fatality, the CFF value compatible to the health effect goal was determined as 10^{-5} /year.

Although the condition for CFF is sufficient to achieve the two health effect goals, the parameter value for CDF was determined as 10^{-4} /year so that proper priority is given to prevention of core damage.

For a multi-unit site, the total risk for units in the site has to be smaller than the health effect goals.

3.2.13 Italy

The general design criteria for PWR NPP issued in eighties in Italy defined the following objectives to be verified by Probabilistic Safety Study:

- for each single sequence the annual probability of exceeding the core coolability limits shall not be higher than $10^{-6} – 10^{-7}$
- the annual overall probability of exceeding the above mentioned coolability limits shall not be higher than $10^{-5} – 10^{-6}$

3.2.14 Hungary

Presently no numerical criteria are in use in the Hungarian nuclear safety regulation. One Probabilistic Safety Goal (PSG) is stated in the NSC Volume 3: the total CDF value shall not exceed 10^{-5} $1/y_{reactor}$ considering all initiating events and all operational states. This PSG is a very challenging one and in the reality it is far from being met by the Paks NPP, which is a VVER-440/V-213 type reactor built to earlier standards.

Some other numerical criteria are given in Volume 3, which serve basically for ranking initiating events and for exclusion of initiating events from the scope of assessments:

> 3.023. The assumed (design) emergency means a rarely occurring event which is caused by failure of systems, system elements, adverse external effects and/or incorrect/erroneous human intervention. During the event the safety functions shall operate as planned and it is not allowed the event to result in a radiation exposure of the operating personnel and the population which is higher than the value specified by the authority. Frequency of the assumed (design) emergencies is lower than the value of 10^{-2}/year.
>
> 3.025. It is allowed the following events to be eliminated from initial events included in the design basis an internal event occurring due to failure of systems, system elements and human error, if its frequency is lower than 10^{-5}/year. Such events originating from external human activities typical of the site frequency of which is lower than 10^{-7}/year, or if the hazard point is far enough and it can be certified that normally it does not have any anticipated effect on the nuclear power plant.
>
> 3.030. The emergencies exceeding the design basis, i.e. accidents mean those events during which the active core might damage and/or radioactive material release of the nuclear power plant probably exceeds the limit values prescribed. The nuclear power plant's design basis shall ensure that it is possible such events to occur under a frequency of 10^{-5}/year at the outmost. Within the concept of accident, a separate class is constituted by those hypothetical events, the so-called severe accidents, which result in core damage and/or during which the quantity of releasing radioactive material so high that dose exposures exceeding the authorial limit values concerning the assumed design emergencies occur, or might occur, within the scope of the operating personnel and the population.
>
> 4.101. It shall be demonstrated for all potential hazard points that the principles determined on the basis of structural design, analysis and probability assessment, that is requirements of the design specification, have been appropriately satisfied. Only those hazards are allowed to be filtered out without further analysis with respect to which it is possible to certify that frequency of the event is lower than 10^{-7} /year, or, since the hazard point is sufficiently far, it is reasonably not expected that it affects the nuclear power plant. Furthermore, the scope of initial events originating from the hazard points shall be investigated also by means of deterministic devices in order to determine whether the assumed initial events filtered out on the basis of the occurrence frequency might represent a real danger, and whether it shall be included in the design basis of the facility.

4.102. In case of natural phenomena, as external hazard points, it is allowed initial events having a frequency of lower than 10^{-4} /year to be filtered out of further analysis. However, the scope of natural phenomena, as initial events originating from external hazard points, shall be analysed also by means of deterministic methods in order to establish whether assumed initial events filtered out represent a real danger and whether it shall be considered in the design basis of the facility.

4.107. In accordance with provisions included in the item 4.103, the value of design basis earthquake, which is relevant from the safety point of view, shall be determined. The maximum design basis earthquake is the highest one during which safety of the nuclear power plant shall be still guaranteed. The earthquake occurring at a frequency of 10^{-4} events/year at the site shall be considered as the maximum design basis earthquake for the whole operating time of the nuclear power plant.

3.2.15 Germany

No probabilistic safety criteria have been defined in Germany to evaluate the safety of the operating nuclear power plants. Therefore, the results of the PSAs are not used to show compliance with any criteria.

Up to now, the PSAs have neither been used for quantified cost/benefit analysis, nor is it foreseen in the near future.

3.2.16 France

In 1977, during the examination of the major technical options for the 1300 MWe plants, the Safety Authority set an overall probabilistic objective expressed as follows:

- "In general terms, the design of a plant which includes a pressurized water nuclear reactor should be such that the overall probability that the plant could be the source of unacceptable consequences should not exceed 10^{-6} per year.
- This implies that, whenever a probabilistic approach is used to assess whether a family of events must be taken into account in the reactor design, the family must effectively be taken into account if its probability to lead to unacceptable consequences exceeds 10^{-7} per year".

It has to be noted that:

The overall objective is stipulated in terms of «unacceptable consequences», but these are not specified by legislation or regulation.

- The 10^{-6} value is an "objective" for a PWR plant, but EDF is not required to demonstrate that this objective has been achieved.
- The 10^{-7} per year value is more practical for operational uses and is used in the approach to determine the risks generated by external hazards; for example, the value is applied to several families of aircraft crash events.

During the PSA applications, the acceptability of the utility proposals are not based on formal criteria, but some orientation values (relative or absolute) can be given case by case. Some examples are the following:

- A probabilistic target of 10^{-6} per reactor year for the CDF related to shutdown conditions was set by the Safety Authority (considering in particular that during shutdown containment integrity is not guaranteed).

- In the framework of the 900 MWe series third Periodic Safety Review, each individual core melt sequence of the PSA 900 with a CDF $>10^{-8}$ per year was analysed, in order to investigate the interest and the feasibility of plant improvements. Particular attention was paid to sequences potentially resulting in early containment failure.
- A probabilistic analysis of operating events is carried out in France since 1994. The aim of the quantitative analysis is to assess the risk increase (in term of core damage probability) due to the incident. An incident is considered as a precursor if the risk increase is higher than 10^{-6} per event.
- The Safety Authority required to take particular measures if the risk increase is higher than 10^{-4}, and to assess the benefit of these measures.
- For the French-German project EPR (European Pressurized Reactor), the French and German Safety Authorities gave the following very general probabilistic objectives: a reduced CDF compared to existing plants and the "practical elimination" of sequences with potential for large early releases.

In order to fulfil these objectives, the designers have proposed probabilistic safety objectives as orientation values which give useful guidance but are not strict limits and do not correspond to a requirement of the Safety Authorities. Examples of these probabilistic objectives are a value of 10^{-6} per year for the CDF due to internal events, respectively for power states and for shutdown states.

Generally speaking, the French Safety Authority (ASN) considers PSA as a fruitful tool, notably for improving the safety of French PWRs by identifying where design and operating modifications are worthwhile, and for ranking problems in order of importance. However, they are not in favour of setting probabilistic criteria.

ASN's policy is to regularly increase safety, not only to maintain it. For that purpose ASN considers that Safety Objectives have not to be defined in probabilistic terms, since the compliance is very difficult to demonstrate and moreover they could have a negative effect by limiting the safety efforts when the objectives are met, even if an improvement could be carried out at a low cost.

Nevertheless ASN considers that probabilistic objectives could be used as orientation values but not as regulatory limits. This is done in particular for the EPR project.

3.2.17 Finland

A level 1 and 2 design phase PSA is required to support an application for a Construction License of the new designs and the construction phase level 1 and 2 PSA is required in context of application for an Operating License. Regulatory Guide YVL 2.8 "Probabilistic safety analysis in safety management of nuclear power plants" specifies the following probabilistic design objectives:

- mean value of the core damage frequency, as estimated from a comprehensive Level 1 PSA, is less than 10^{-5}/year
- mean value of a large radioactive release frequency (more than 100 TBq Cs-137), as estimated from a comprehensive level 2 PSA, is less than $5x10^{-7}$/year.

The design of a NPP unit under construction has to be improved if these objectives are not met in terms of a design Phase PSA. The design phase PSA has to be completed during the construction of the plant when detailed design is available. If new risk factors are identified after issuing a Construction License and the safety objectives are not still met, sufficient efforts have to be taken to reduce the risk.

3.2.18 Czech Republic

The safety criteria or safety goals adopted by the operator are based upon the IAEA INSAG target value recommendations for CDF and LERF. No regulatory probabilistic safety criteria are required to be met by the operator as there is no legal requirement to conduct PSA at all. As a direct consequence, the results of the basic PSAs are not used to demonstrate to regulatory body compliance with any criteria. There is only regulatory body recommendation to comply with IAEA probabilistic safety criteria (INSAG-12).

For the risk informed applications the risk increase criteria from US NRC RG. 1.174 is to be applied.

3.2.19 Canada

The CNSC regulations include the quantitative criteria for the unavailability of Special Safety Systems. There are no other quantitative criteria in CNSC regulatory documents with regard to PRAs.

However, the CNSC seeks to define the Policy on Safety Goals for Nuclear Power Plant (P-324). The document yet to be issued is supposed to only state high level qualitative objectives, while the quantitative surrogates are to be included in a standard. The qualitative safety goals are consistent with the IAEA standard NS-R-1, which identifies the radiation protection, and technical safety objectives. Associated with these two objectives, CNSC deems to use three safety goals which include the traditional two used by most regulators, namely (1) frequency of Severe Core Damage, and (2) frequency of Large Releases. The third safety goal would be the Small Releases triggering the evacuation of the public. The third goal is related to the limited damage of the core with containment impairment where the release would be low enough to not-permanently contaminate, but nevertheless results in severe disruption of public life. The CNSC is considering the option to specify the releases of radioactive material in absolute quantities. However, no decision has been made on the safety goals. The work is still in progress.

The industry is using the safety goals consistent with the ones defined by the owner of one of the multi-unit Candu plants, namely Ontario Power Generation (OPG). OPG and Bruce Power (following its formation as a separate company) have for many years been using risk-based safety goals to assess the adequacy of plant design and operation. The current version of these goals is given in Table 3-5. These are applicable to the operating plants and the refurbishment project for the single unit of Point Lepreau.

TABLE 3-5: Safety goals defined by Ontario Power generation

Safety goal (application)	**Average risk (per year)**		**Instantaneous risk (per year)**
	Target	Limit	Limit [1]
Latent Effects [2] (per site)	10^{-5}	10^{-4}	N/A
Large Release [3] (per unit)	10^{-6}	10^{-5}	3×10^{-5}
Severe Core Damage (per unit)	10^{-5}	10^{-4}	3×10^{-4}

[1] Bruce Power has an identical set of values as OPG except that the instantaneous risk values are interpreted as threshold values instead of limits.

[2] Latent effects refer to delayed fatality.

[3] Defined as release of > 1% of core inventory of Cs_{137}.

For the new designs like ACR, the safety goals are the following:

- The summed severe core damage frequency is less than 10^{-5} /reactor year
- The summed large release frequency (LRF) is less than 10^{-6} /plant year. The magnitude of the LRF is 100 TBq of Cs_{137}.
- The severe core damage frequency for individual event sequences is less than 10^{-7} /year

3.2.20 Belgium

Except for the evaluation of the required protection against external events (where the probabilistic criteria of the USNRC SRP section 2.2.3 are used), no probabilistic safety criteria have been defined in Belgium to evaluate the safety of the operating nuclear power plants. As a direct consequence, the results of the PSAs are not used to show compliance with any criteria.

Until now, the PSAs were not used for quantified cost/benefit analysis.

4 PSA STANDARDS AND GUIDANCE

4.1 Summary

The position in the respondent countries is that there is an increasing move towards a risk informed approach to making decisions on plant safety issues and carrying out regulatory activities. This has let to a greater need for the PSAs being produced to be of a sufficient quality to support a wide range of applications. This includes the scope, methodology and data used in the analysis. In addition, in the Member Countries with a number of power plants, there is a need to ensure that the set of PSAs being produced are consistent. This has led to PSA Standards and Guidance being developed in a number of the Member Countries.

In the USA, PSA standards and guidance are being developed and this activity is being supported by professional societies, the industry and the Regulatory Authority. The PSA Standards and Guidance being produced is as follows:

- Standard for Level 1 PSA (for core damage frequency) and limited Level 2 PSA (for large early release frequency) for full power operation that covers internal initiating events and internal flood – being produced by the American Society of Mechanical Engineers (ASME).
- Peer review guidance for the same scope of PSA as the ASME standard – being produced by the Nuclear Energy Institute (NEI).
- Standards for: external hazards, low power and shutdown modes, internal fires, Level 2 PSA and Level 3 PSA - being produced by the American Nuclear Society (ANS).

NRC staff is working with the industry to incorporate risk insights into codes and standards applicable to various activities at nuclear power plants such as in–service inspection and testing. In addition, a phased approach is being developed between NRC and the industry for the production of better, more complete PSAs that are suitable for current, or anticipated, applications.

In Japan, fundamental guidelines on the use of risk information in the safety regulation of nuclear power plants and PSA quality guidelines have been developed by the Nuclear and Industrial Safety Authority (NISA) and the Japan Nuclear Energy Safety Organisation (JNES) and issued for trial use. In particular, the guidelines for PSA quality gives the requirements for: the scope of PSA for risk-informed applications; the adequacy of the PSA models and data; and the adequacy of the analysis and evaluation of the results.

In addition, standards and guidance has been produced by academic societies or industry which will be endorsed by NISA. This includes the PSA Procedure Guide produced by Nuclear Safety Research Organisation (NSRA) and the PSA Standard being produced by Atomic Energy Society of Japan (AESJ) which addresses:

- Level 1 PSA for internal events during shutdown.
- Level 1 PSA for internal events during power operation.
- Level 2 PSA for internal events during power operation.
- PSA for seismic events during power operation.
- Level 3 PSA.

In Canada, the Regulatory Authority, the Canadian Nuclear Safety Commission (CNSC), has produced a Standard on PSA for nuclear power plants and is in the process of producing the associated Guidance on the PSA requirements for specific applications. In addition, the plant operators, Ontario Power Generation (OPG) and Bruce Power (BP), have produced their own PSA Standards and Guides that are included as part of the company’s management system. The scope of the Standard and Guidance that has been produced relates to carrying out the PSA, maintaining it as a

Living PSA and using it as part of a risk-informed decision making process, and provides guidance to practitioners on each of the elements of the PSA.

In Switzerland, the Swiss Federal Nuclear Safety Inspectorate (HSK) are developing Guidelines on PSA Scope and Quality and on PSA Applications. The Guideline on PSA Scope and Quality gives relatively prescriptive requirements for each of the elements of Level 1 and 2 PSAs for internal and external events. The aim is to further harmonise the quality and scope of the PSA being produced for Swiss nuclear power plants.

In Korea, Guidelines on PSA Quality are being developed by the Korean Institute of Nuclear Safety (KINS).

In Germany, a PSA Guideline has been produced along with technical documents on PSA methods and data, and these were updated in 2005. This requires that a Level 2 PSA is carried out for full power operation and a Level 1 PSA for low power and shutdown states where the scope of the PSA includes internal and external initiating events, in particular internal fire and seismic events.

In the Netherlands, a Procedures Guide was produced for Level 1 and 2 PSA. This captured the experience that had been gained in the production of the PSAs for Borssele and Dodewaard. However, when it became clear that there would be no expansion of the nuclear energy option, the official formalisation of the Guide was put on hold.

In the other Member Countries, no specific PSA standards or guidance has been developed. The position in these countries is that the methods used for the PSAS that have been carried out have been defined within these projects. The way that this has been done has taken account of international practices as defined in documents published by IAEA, NEA and NRC. In these countries, the production of the PSAs has evolved with time and the aim has been to ensure consistency across the set of PSAs being produced in that country.

For example, in France, the PSAS for the 900 MWe and the 1300 MWe plants were carried out by two independent teams at IRSN and EdF respectively. A detailed mutual external review was carried out and this has led to important improvements in the quality of the PSA. In addition, to support the development of PSA, the Swedish Regulatory Authority (SKI) has produced research report on different areas of PSA.

4.2 Country replies

4.2.1 USA

The increased use of PSAs in the regulatory decision making process of the NRC requires consistency in the quality, scope, methodology, and data used in such analyses. These requirements apply to PSAs developed by industry to support specific risk-informed licensing actions as well as PSAs developed by NRC staff to analyze specific technical issues or to support Commission decisions. To this end and to streamline staff review of license applications, professional societies, the industry, and the staff are supporting the development of consensus standards and guidance on the use of PSA in regulatory decision making.

Under this activity, the American Society of Mechanical Engineers (ASME), the Nuclear Energy Institute (NEI), and the American Nuclear Society (ANS) each have the following responsibilities:

ASME: PSA standard for a Level 1 analysis [i.e., estimation of core damage frequency (CDF)] and a limited Level 2 analysis [i.e., estimation of large early release frequency (LERF)] covering internal events (transients, loss-of-coolant accidents, and internal flood) at full power. (The current standard contains two addenda, Addendum A and Addendum B. These addenda provide changes to the standard to respond to comments received and issues identified during a trial application.)

NEI: PSA peer review guidance on internal events at full power (Level 1 and limited Level 2)

Self-assessment guidance for determining the significance of differences between the peer review criteria and the ASME PRA standard (completed through Revision 1)

ANS: PSA standard for a Level 1 and limited level 2 analysis of external hazards (completed, but revision 1 in development)

PSA standard for a Level 1 and limited level 2 analysis of low-power and shutdown (LP/SD) conditions (in development)

PSA standard for a Level 1 and limited level 2 analysis of internal fires (in development)

PSA Standard for a Level 2 analysis (in development)

PSA Standard for a Level 3 analysis (in development)

In parallel, the National Fire Protection Association (NFPA) has developed NFPA 805, a Performance-based Standard for Fire Protection for Light Water Reactor Electric Generating Plants. This standard discusses the use of risk information in the development of a risk-informed, performance-based fire protection program. The standard does not establish requirements for a fire PSA - such requirements are being developed by ANS, as indicated above.

The NRC staff is working with the ASME and other organizations to incorporate risk insights into codes and standards applicable to various activities at nuclear power plants. For example, the ASME is updating the *Code for Operation and Maintenance of Nuclear Power Plants* and applicable code cases to allow the use of risk insights in the in-service testing of pumps and valves. ASME is also developing code cases under Section XI of the *Boiler & Pressure Vessel Code* to apply risk insights in the in-service inspection of structures, systems, and components. The NRC staff has developed regulatory guides to document the acceptance of some of the risk-informed code cases as well as a regulatory guide to list the code cases that the staff has found to be unacceptable. These regulatory guides were finalized and published in June 2003.

It is expected that licensees will use the PSA standards and industry guidance to help demonstrate and document the adequacy of their PSAs for a variety of risk-informed regulatory applications. Therefore, the staff position on the adequacy of the standards and industry guidance to support regulatory applications is documented in a regulatory guide and associated staff guidance in a standard review plan. Such documentation will indicate in which areas staff review can be minimized and where additional review may be expected. To accomplish this objective, the NRC staff has developed RG 1.200 to provide an approach for assessing the adequacy of PSA results used in support of regulatory applications and an accompanying standard review plan (SRP) Chapter 19.1. RG 1.200 and the associated SRP chapter are intended to support all risk-informed activities. The staff's position on each PSA standard and industry guidance document is provided in the appendices. Currently only the ASME Level 1 standard and the NEI peer review process are addressed.

In a Staff Requirements Memorandum (SRM) dated December 18, 2003, the Commission approved implementation of a phased approach to achieving an appropriate quality for PSAs for NRC's risk-informed regulatory decision making. The SRM directed the staff to engage stakeholders and develop an action plan that defines a practical strategy for the implementation of the phased approach to PSA quality so that industry would move in the direction of better, more complete PSAs, and efficiencies would be introduced into the staff's review of risk-informed applications.

The SRM specifies four phases for the NRC staff's efforts. The phase is determined by the availability of the PRA guidance documents (e.g., quality standards, industry guides, regulatory guides) needed to generate the results/decision required for an application. For most applications, the effort is now in Phase 1. Phase 2 will be achieved in stages as application quality needs are identified and guidance documents become available for specific application types. For Phase 2, the scope of the PSA required is a function of the decision to be made (e.g., special treatment requirements, allowed outage time extensions). To complete Phase 3 the staff will produce (by December 31, 2008) an overall guidance document regarding PSA technical adequacy for risk-informed applications. Phase 4 calls for the industry to have full-scope, full-quantification, full-uncertainty analysis PRAs that will be reviewed and approved by the NRC. The Commission did not set a date for implementation of Phase 4.

In response to the SRM, in July of 2004, the staff issued SECY-04-0118, "Plan for the Implementation of the Commission's Phased Approach to PRA Quality" and the Commission approved the staff's plan in an SRM dated October 6, 2004. The phased approach defines the process for achieving PSA quality for current or anticipated applications , and allows risk-informed decisions to be made using currently available methods until all the necessary guidance documents (e.g., standards and regulatory guides) defining the PSA quality are developed and implemented.

It is expected that meeting the phased approach objective will result in the following:

- Industry movement towards improved and more complete PSAs.
- Increased efficiencies in the staff's review of risk-informed applications.
- Clarification of expectations for rulemakings.
- Continued near-term progress in enhancing safety through the use of available risk-informed methods while striving for increased effectiveness and efficiency in the longer term.

4.2.2 United Kingdom

There are no UK specific PSA standard or guidelines. The current raft of UK PSAs have been developed based on that international best practise which each licencee considers to be fit for purpose for their particular reactor design. In general the UK PSAs have been developed in compliance with the IAEA Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants. Separately the AGRs and Sizewell B PSAs have been the subject of recent successful evaluations by the IAEA International PSA Review Service (IPSART) missions.

In evaluating the PSA the NII utilise the Safety Assessment Principles (SAPs) together with the more detailed Technical Assessment Guides (TAGs), to guide their decision-making. The TAGs have been written to help interpret the SAPs and in some cases have addressed gaps in them; currently the TAGs are the subject of an ongoing process of revision. The SAPs and the TAGs form an integrated suite of guidance to NII's nuclear inspectors.

The TAGs most relevant to the assessment of PSAs are:

T/AST/004	Fundamental principles
T/AST/005	Demonstration of ALARP
T/AST/006	Deterministic safety analysis and the use of engineering principles in safety assessment
T/AST/008	Safety categorisation and equipment qualification
T/AST/010	Operator action and the "30 minute rule"
T/AST/011	The single failure criterion

T/AST/013	External hazards
T/AST/034	Transient analysis for DBAs in nuclear reactors
T/AST/036	Diversity, redundancy, segregation and layout of mechanical plan
T/AST/042	Containment: Validation of computer codes and calculation methods
T/AST/044	Fault analysis
T/AST/050	Periodic safety reviews (PSRs)
T/AST/051	Guidance on the purpose, scope and content of nuclear safety cases

Copies of the TAGs (in PDF format) are publicly available on the HSE website: www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/index.htm

4.2.3 Taiwan

Since PSA is not formally required by TAEC, neither national standards, nor national regulatory guidelines have been developed in the area of PSA. In 2002, the Licensee submitted the PSA peer review results[13] of three operating NPPs to TAEC. It was then approved that those PSAs can be adopted in the area of risk-informed applications. The peer review process was based on the review guidelines issued by NEI[14]. In order to extend the application area, INER is now revising those PSA models according to the suggestions from the peer review. The subsequent peer review process will begin in late 2006. This time, those PSAs will be reviewed per both ASME[15] standards and NEI review guidelines.

4.2.4 Switzerland

Using PSA as an element of regulatory decision-making process is based on the premise that the results of various plant-specific PSAs are comparable. However, there is a large number of international guidance and standards. In order to further harmonize the quality and the scope of the Swiss PSAs, it was decided to develop a corresponding HSK guideline, which will be prescriptive as far as possible.

In addition, a HSK guideline, setting forth also the general role of PSA within the HSK decision making process, is being developed for several specific PSA applications.

Guideline on PSA Scope and Quality: Work on the guideline on PSA scope and quality has been started. The guideline encompasses requirements for both level 1 (internal and external events) and level 2 PSA based on the insights gained from more than 15 years of experience in regulatory review including the development of a regulatory PSA-model. The goal of the guideline is to promote the harmonization of various plant-specific PSAs in Switzerland, as the PSA results need to be based on models that enable comparisons as part of the decision-making process. Therefore, the guideline will include aspects (e.g. modelling assumptions or documentation requirements) that are relatively prescriptive in character.

The required level of PSA quality will, in general, enable the following PSA applications:

- Assessment of the overall plant safety (safety level and risk profile)
- Assessment of plant modifications and procedural changes
- Evaluation and rating of operational events
- Assessment of the risk classification of active components

As a part of the development of this guideline, the basic risk measures including core damage frequency, fuel damage frequency, large early release frequency and large release frequency are being defined in an unambiguous manner as far as possible. Furthermore, the required basic results of a PSA will be defined in detail.

Guideline on PSA Applications: Work on the PSA applications guideline has also been started. The guideline will define the general role of PSA within the integrated oversight process with the help of a number of principles and the requirements for some specific PSA applications.

The principles are consistent with the overall legislation. As such, the implementation of the principles is not a revolutionary change in the regulatory oversight process; it is mainly a formalization of the PSA role in safety regulations based on the accumulated experience.

Furthermore, it is planned to describe some PSA applications including changes to technical specifications, risk categorization of components, and assessment of operational experience. The corresponding risk measures and (if sufficient experience is available) risk criteria will be defined in order to be used in specific PSA applications.

4.2.5 Sweden

In this section a description of the standards, guidance documents etc. that has been used in producing and reviewing PSA:s in Sweden are presented.

National regulations: National regulation that rules the quality of the PSA:s, found in the regulation SKIFS 2004:01. This regulation went into force 1 of January 2004.

National standards: There are no formal domestic standard published regarding how PSA:s have to be performed and what they should content. What rules the PSA activities in Sweden today are the demands stated in the regulation SKIFS 2004:1, (see national regulations). The licensees do however interpret and follow, international PSA standards and recommendations in their overall process oriented PSA work. Last but least it are the national industry solutions and practices and interpretations of the domestic regulations on PSAs, that yields.

National regulatory guides*:* By time, SKI and the industry have released results from performed research activities as best way of solving certain matters of interest. These results are published as guidance reports by SKI.

- In 2002 SKI published a report dealing with treatment of external events analysis, The SKI Report 2002:27, Guidance to External events Analysis.
- In 2003, SKI produced a report dealing with best estimate of fire frequencies for Swedish NPPs, the SKI Rapport 2003:25, Branddata projektet.
- In 2003 SKI produced the Reviewing handbook of PSAs. The SKI Rapport 2003:48, Tillsynshandbok PSA.

All SKI research reports are stored on the homepage of SKI at internet address www.ski.se

Widely used national industry guidelines, etc.

The Reviewing handbook of PSAs, SKI Rapport 2003:48, Tillsynshandbok PSA: SKI has listed more or less all the most important references that have been used in the domestic PSAs till now.

In the following section a short presentation of the aims and content in the SKI Report 2003:48 is given, SKI requirements regarding PSA and PSA activities are more descriptive than prescriptive, in PSA review handbook.

The aim with the PSA review handbook is to describe *what* is to be done rather than *how* it is to be done. This approach is preserved in the PSA review handbook developed by SKI, the Swedish Nuclear Power Inspectorate.

Regulatory handbook for PSA review is intended to be a support in SKI supervision of licensee PSA activities. PSA activities shall be interpreted in its widest sense, and includes organisation and working procedures at the licensee, layout and content of the PSA and areas of application of the PSA. It describes SKI procedures for review of PSAs and inspection of PSA activities.

Requirements in the handbook define a PSA review procedure, describe SKI requirements with respect to PSA, ND provide evaluation criteria OF maximum 50 pages.

Three basic types of review activities are covered

P Full PSA Review
A Review of PSA Application
I PSA Inspection (on site procedures, quality and organisation)

Evaluation criteria classified P - A – I: for each type of review, the handbook describes how the review is planned and performed as well as how it is to be documented.

4.2.6 Spain

Spanish national standards have not been developed, but some regulatory guides.

There is a programmatic objective to shape the experience that has been acquired during the performance and application of the PSA in rules and/or guides. The guides for PSA performance have been shaped themselves, in fact, from PSA project to PSA project for each PSA task. This can be considered as a real standardization process and, therefore, the latest PSA task procedures could be easily elevated, if decided, to the category of "standard".

The regulatory guides developed in Spain are those related to the PSA applications similar as the USNRC RG 1.174, (GS 1.14) and a regulatory guide aimed to keep the maintenance and updating of the Spanish PSA (GS 1.15). Others specific guides from the USNRC related to the PSA applications have been indicated as appropriated.

Others documents as NUREGs, IAEA guidelines, etc have been also considered as reference.

4.2.7 Slovenia

In Slovenia there are no national standards or guidance on the scope and quality of the PSA. The scope of the PSA has been based on the IAEA and US NRC guidelines.

Within the framework of the first Periodic Safety Review (PSR) for Krško, the quality of the PSA analyses for internal events at power was reviewed against the NEI/WOG/ASME guidance and standard scope.

There are neither national standards nor guidance on PSA applications. The US NRC guidelines are used in a consultative way.

4.2.8 Slovak Republic

Internationally accepted PSA standards and guidance are used for preparing and review of the PSA studies (NUREGs, IAEA guidelines, Standard for PRA for NPP application). In addition, the PSA guideline of the Regulatory Authority defines probabilistic targets to be fulfilled to reach adequate level of safety. It contains guidance for performance of probabilistic safety analysis (PSA), and applications of PSA for operational safety and regulatory safety decision-making. It summarizes requirements and conditions, which are laid down for the preparation and review of PSA. Duties of the utility are described on the scope, contents, review, quality assurance and upgrading of PSA. The guideline refers to all NPPs operated or constructed in Slovakia. It covers design, construction, operation, or extension of NPP operation.

4.2.9 Netherlands

At the onset of the Dutch PSA programmes in 1988/1989, there existed no national PSA guidelines. Even worse, there was hardly any experience regarding the development of a complete PSA for a Nuclear Power Plant. Most of the knowledge came from reading NUREG reports, and not from hands-on experience. This was equally true for the licensees and the regulatory body. Therefore, foreign contractors were selected by both licensees to develop the two PSAs. In the first discussions (1988) between one licensee (Borssele NPP) and regulatory body only general requirements, the scope and objectives were discussed. An important topic in this discussion was regarding the necessity of technology transfer from the contractor to the plant staff. It is fair to say that the ongoing regulatory guidance benefited largely from this technology transfer as well as from the peer reviews from. The only technical regulatory requirements and/or guidance was given concerning the scope, level of detail, whether or not best estimate techniques can be used in the modelling, etc. Regarding the more detailed guidance the agreement was that the U.S. NRC PRA Procedures Guide (NUREG/CR-2300) and the PSA-Procedures Guide (NUREG/CR-2815) were adequate at that time.

Parallel with the conduct of the PSAs a Dutch PSA procedures guide (level-1 and level-2) was developed by the regulatory body. It is evident that this development highly benefited from the ongoing PSAs. As a final step these documents were reviewed by the Reactor Safety Committee (a governmental advisory board). After finalisation it was too late to be used as further guidance for the PSAs of Borssele and Dodewaard. After it became clear that there would be no expansion of the nuclear energy option in The Netherlands in the near future, official formalisation of these guides as official nuclear safety guide was put on hold.

Because in 1989 hardly any experience existed in the Netherlands (including the regulatory body) regarding state-of-the-art PSA techniques, the IAEA was asked by the regulatory body to review the PSA at various stages of its completion and to train the regulatory body in the art of reviewing nuclear PSAs.

As a kind of sanity check the first IPERS review involved only the above-mentioned bid specification, minutes of the meetings between licensee and regulatory body, and interviews with the responsible staff members of the plant and the regulatory body. The results of this review could be translated by the regulatory body into additional guidance. E.g., the requirement to extend the PSAs with an assessment of the non-power states and to assess the so-called Errors-of-commission was a result of this review.

IAEA training, technology transfer from contractors to the licensees and partly the regulatory body, and participation in IPERS reviews enabled staff members of the regulatory body to review themselves some specific aspects of the PSAs in later stages of the studies. Especially, those parts that required a more in-depth knowledge of the detailed design of the NPP's, e.g., translation of the plant in the modelling of the fire PSA, were reviewed by the regulatory body. Another regulatory involvement dealt with discussions with plant staff regarding the translation of the PSA results in modification proposals. An additional beneficial aspect of this regulatory review was the learning process for those staff members, which were previously not involved with the PSA. Despite these learning and reviewing activities some misperceptions, biases, etc. still emerged.

Nevertheless, it is fair to state that most of the guidance emerged by learning and doing.

Past experience regarding regulatory PSA activities in the Netherlands, including giving guidance, setting preconditions, and reviewing PSAs, have lead to the following conclusions:

- Understanding the causes that drive the outcomes is far more beneficial than blindly producing these outcomes by following a recipe.
- Selection of the contractor, which and how many of their leading experts participate in the PSA team, and selection of the reviewers is equally important as having a PSA-guide.
- Regulatory guidance should primarily aim at a proper agreement between plant staff and regulatory body regarding the scope and objectives of the PSA. Making the plant staff enthusiastic for the benefits of using a LPSA should be the main regulatory role. Hence, stimulation instead of guidance.

An important step in the second 10-yearly periodic safety review of the Borssele Plant was a comparison with the current state of the art. Reference was made with a large variety of international PSA-guides such as: the ASME-PSA Guide, SKI Report 98-30 on piping failure data, NEI-00-02 (PRA Peer Review Process Guidance), NUREG/CR-6268 (Common-Cause), NUREG 1624 and NUREG/CR-6350 (both regarding ATHEANA method for assessing Errors of Commission). This comparison resulted in several proposals for updating the PSA model. E.g., the method for post-initiator human actions is changed from HCR/ORE in the Cause Based Decision Tree (CBDT) method. A new fire analysis with NUREG/CR-6850 as a basis. Expansion of the mission times from 24 hrs to 72 hrs.

4.2.10 Mexico

Neither national standards, nor national regulatory guides have been so far developed in the area of PSA.

There are no specific guides (from international organisations or other countries), recommended to perform PSA-analyses of nuclear power plants, however PSA methodologies such as NUREG/CR-2815,1150, NSAC 159 as well as the IAEA guidelines have been followed during the development of PSA studies. Also some PSA studies have been used as a reference - for example, NUREG/CR-4550 and 6143.

4.2.11 Korea

A lot of regulatory guidelines, including PSA review guidelines, have been made by KINS.

<u>*Guideline on PSA quality*</u>*:* Since the SAP was issued, which prescribes essential elements such as PSA implementation and its periodic reassessment, reliability database, and risk monitoring program to the utility, we have a chance to easily get all kinds of risk information for improving current regulatory framework. In addition, with the overall availability of PSA results for all operating plants, it is expected that many risk-informed applications (RIAs) will be submitted to the regulatory body.

Usually, regulatory decision making in the case of RIAs requires the information enough for ensuring the technical adequacy. This information should be provided with the best available PSA elements including sound work scope covering the objective of RIAs. Therefore, there are lots of regulatory concerns associated with the quality assurance of licensee’s submittals for RIA. It is also noted that making general requirements and touching specific check points are essential for the regulatory decision making process. The regulatory guideline for assuring PSA quality is being announced for comment [1]. It has a primary goal to review all kinds of information related with PSA quality and to identify and correct the limitation or weak points retained in the RIA submittals. It is also intended the risk information in RIAs to be technically checked against consensus PSA standards (e.g., ASME standard for internal events [2]), and to satisfy the minimum requirements (e.g., Category 1, 2, or 3) for each item as appropriate for the intended applications.

Regulatory Guideline on Maintenance Effectiveness: As we desire to keep adequate operational performance of plant SSCs, we have to assure their reliable operability for protecting public's health and property against any radiological hazards. In addition, one of important regulatory technology for achieving public's credibility may be to preserve operational safety related with the maintenance of a lot of active SSCs. As a fundamental of domestic utilization of performance-based regulation, we need a performance monitoring program to check the impact of risk-informed changes on SSCs. Furthermore, the necessity on the verification of the secondary performance for reducing unplanned plant shutdown, is also raised.

The utility is developing maintenance effectiveness monitoring program, and she/he intends it to be pilot-operated after 2006. According to this situation, a regulatory guideline for providing regulatory requirements on this program has been prepared.

4.2.12 Japan

Guidelines for the risk-informed regulation in Japan

According to the Near-Term Implementation Plan made in May 2005 (See 7.7), NISA established High-Level Guidelines and PSA Quality guidelines for RIR in collaboration with JNES, in April 2006.

*High-Level Guidelines for Utilization of 'Risk Information' in Safety Regulations for NPPs - Trial Use***:** These guidelines specify basic principles to be followed in RIR. The guidelines can also be referred to endorse consensus standards for RIR applications, which have been established or are going to be settled by academic societies or industries. In addition, it is recommended to utilities to make reference to these guidelines in their own risk-informed activities.

Although these guidelines, for the meanwhile, aims at using "risk information" obtained from the result of PSA as well as its process to the safety regulation of NPPs, they can also be referred in the safety regulation of non-NPP facilities in the future stage.

High-Level Guidelines are specified from the following points; consistency with the principles used in the current safety regulation; risk metrics, acceptance criteria, and consideration of their uncertainties; observation of NPPs' performance; and processes with which risk-informed decision-making should be complied.

PSA Quality Guidelines for NPP Applications - Trial Use: These guidelines specify required attributes for the quality of PSA used in RIR applications.

Following three basic elements in respect of the quality of PSA for RIR application are defined and required considerations for them are accompanied; scope of PSA; adequacy of PSA models and data; and adequacy of the analysis and evaluation of the results. As for the scope of PSA, it should be considered to what extent of PSA is accomplished; Level 1, Level 2, or Level 3; power operating state or shutdown condition; internal events or external events. As for the adequacy of PSA models, they should reflect the plant design and operation as much as they could. And data used should be consistent with the plant features and operating experiences followed by clear references. As for the adequacy of the analysis and evaluation of the results, it should be clearly defined major contributors to the risk. And uncertainty analyses as well as sensitivity studies should be conducted in order to grasp degree of uncertainties of the PSA results.

Detailed technical requirements for Level 1 PSA, Level 2 PSA, Level 3 PSA, and seismic PSA are prescribed according to the elements of each PSA in these guidelines.

PSA standards and guidance in Japan

Utilizing “Risk Information” obtained from the result of PSA in the safety regulation for NPPs, NISA will endorse the following consensus standards made by academic societies or industries.

NSRA PSA Procedure Guides for level 1 and level 2 PSAs for AM: It is recommended that PSA on individual NPPs should be performed in accordance with the guidebooks issued by Nuclear Safety Research Association (NSRA) in 1992 for level 1 PSA and in 1993 for level 2 PSA, which have been prepared by the voluntary committee consisting of representative PSA-specialists from governmental organizations and industry groups, and the fundamental concept and methodologies of the standards are the same as NUREG/CR-2300.

AESJ PSA Standard: The Power Reactor Technical Committee (PRTC) is one of three technical committees set up in the Standard Committee of AESJ, organized in September 1999 in order to issue the standards for nuclear technology from the viewpoint of effectively securing the safety and reliability of nuclear facilities based on the state of the art technology. The Standard Committee makes and revises the standards, guides and guidance on design, construction, operation and decommissioning of nuclear facilities. The members of committees are elected widely among industrial and academic circles to secure the neutrality, impartiality, accountability and transparency. The proceedings of the committees are made public.

Standard for level 1 PSA for internal events during shutdown operation: The first subcommittee on PSA in PRTC initiated activities to prepare a Procedures Guide of PSA for internal events of NPPs during Shutdown Conditions in June 2000, of which draft was supported in August 2001 by PRTC. After the public examination of two months, the Procedures were issued as ‘A Procedures Guide for Probabilistic Safety Assessments of NPPs during Shutdown Conditions: 2002’, AESJ-SC-P001: 2002, in April 2002. This has been utilized in the shutdown PSA in PSR.

Standard for level 1 PSA for internal events during rated power operation: The work on the level 1 PSA standard for internal events during rated power operation was started in March 2003. This standard describes the requirements on methodologies to be used. The examples of methodologies to satisfy the requirements are suggested in appendices.

The requirements were determined based on a review of existing standard including those of the ASME and NSRA with consideration of current practices in Japan.

There are some important differences from the ASME Standard. For example, in the ASME standard, three categories are made for capability of PSA but, in the AESJ standard, such categorization is not made. It is regarded as an issue to be discussed after more experiences of risk informed applications are obtained in Japan. The first version of this standard was completed in 2006.

As the PSA Quality Guidelines, issued by NISA in April 2006, raised generic requirements for the PSA standards by academic societies, the standard for level 1 PSA will be revised to satisfy their requirements. The PSA Quality Guidelines required PSA standards to provide concrete descriptions of methodologies and explicit requirements on the use of quality assurance procedures, expert judgments and publication of documentations. These requirements of the guidelines are common to the level 2, level 3 and seismic PSA standards described below.

Standard for level 2 PSA for internal events during rated power operation: The work on level 2 PSA for internal events during rated power operation was started in April 2004. This standard describes requirements and methodologies to satisfy the requirements for conducting level 2PSA to obtain the scenarios, frequencies and source terms of containment failure. In its appendices, this standard includes guidance information and examples of the state-of-the art methodologies of level 2 PSA. This standard will be completed in 2006.

PSA Standard of PSA for seismic events during rated power operation: As Japan is a country with frequent earthquakes, the development of a standard for seismic PSA has been given a high priority among those for external events.

The work on seismic PSA was started in July 2006. This standard includes requirements and methodologies to satisfy the requirements to perform PSA for seismic events during rated power operation. It also covers the identification of containment failure scenarios caused by earthquakes so that level 2 seismic PSA can be conducted by the combined use of this PSA standard and the level 2 PSA standard for internal events. The appendices of this standard provides detailed guidance and examples of state-of-the art methodologies for conducting seismic hazard analysis, fragility analysis and accident sequence analysis. The standard will be completed in 2006.

PSA for Standard for Level 3 PSA: Considering the need for level 3 PSA in the utilization of the safety goals, the work on the standard for level 3 PSA of NPPs in November 2004. This standard includes requirements and methodologies to satisfy the requirements to perform level 3 PSA for NPPs. The standard will be completed in 2006.

Standard for Parameter Estimation for PSA: The work on parameter estimation for PSA was started in November 2006. This standard describes requirements and methodologies to estimate Parameter (initiating events frequency, component failure rate, common cause failure, e.g.) and its uncertainty by technique of both Bayes estimate and frequentist estimate. This standard is made as expansion of a level 1 PSA standard, but human reliability is excluded. A draft report will be completed in 2008.

Risk Information Application Guideline: The work on the risk information application guideline was started in Oct. 2006. This application guideline will describe basic processes, which include allowable risk criteria, for utilities to apply risk information to safety management and ensuring safety in nuclear power plant. This guideline keeps in mind the basic principle of "Fundamental Guidelines for Utilization of "Risk Information" in Safety Regulation for NPPs - Trial Use –" issued by NISA. A draft standard will be completed in 2008.

JSME RI-ISI code: Working Group on Risk Based In-Service Inspection (RI-ISI), which belongs to Subgroup on Fitness-for-Service, Subcommittee on Nuclear Power and Main Committee on Power Generation Facility Codes on the Japanese Society of Mechanical Engineers (JSME), has started work to propose the draft code, consistent with the code of Risk-Informed In-Service Inspection in U.S., to Subgroup on Fitness-for-Service. This draft code is to issue the code case of In-Service Inspection on Fitness-for-Service. The body text will be issued in 2006 and the complete code including its supplement will be issued in 2008 or 2009.

4.2.13 Italy

Nothing to report.

4.2.14 Hungary

Neither national standards, nor national regulatory guides have been developed in the area of PSA.

The requirements on the use of PSA for demonstration of the safety level of the operating nuclear units and of the operational/design changes are involved on a general level within the Nuclear Safety Code described in Section 2. Volume No. 3 of the Code contains the regulatory requirements for the design of NPPs, its Sub-section 3.5.4. summarises prescription to be considered for Probabilistic Safety Analysis [1].

No specific international PSA standards and guides have been selected to be strictly followed for the PSA analyses of the Hungarian nuclear units. As several PSA studies having different general framework an methodologies have been performed for the Paks NPP (see Section 5), the actual procedure has been set up and the methodologies to be applied for the main tasks of the given study have been defined during the course of the studies (see Section 6). For this purpose numerous reference documents have been used. Initially the basic IAEA procedure guides and TECDOCs [e.g. 2-3], more recently several NEA documents [e.g. 4-6] and NUREG reports [e.g. 7-8] have been considered.

4.2.15 Germany

The PSA Guideline [1] and its corresponding technical documents on PSA methods [2] and data [3] have been published first in 1997 and updated in 2005 and meanwhile require a Level 2 PSA for full power plant operational states and a Level 1 PSA for low power and shutdown states, including internal and external initiating events, in particular a fire PSA and a seismic PSA. This scope of the PSA reflects the experience in Germany. Up to now, no low power and shutdown states Level 2 PSA has been performed for NPPs in Germany. It was therefore not considered to be justified to make this part of the PSA obligatory for the utilities. The objective of updating the PSA Guide was not only to extend the scope of the PSA, but also to improve the comparability among PSA results for various plants, without being too prescriptive.

4.2.16 France

The first French PSAs were developed according to the general state-of-the-art, without specific standards or guidance.

However the fact that the studies were performed by two independent teams, with a very detailed mutual external review, contributed to an important improvement of PSA quality.

Although the basic PSA Safety Rule presents the acceptable methods for PSA developments and applications, in fact the Safety Rule presents “a posteriori” the methods and applications already used and validated, and is then limited to level 1 PSA and internal initiating events.

For all PSA applications, a detailed technical dialogue between EDF and IRSN is always carried out, including the discussion of methods in case of new developments.

4.2.17 Finland

The requirements on the use of PSA for the risk informed regulation derives from the Degree level trough the Government Decision level to the Regulatory level.

According to the Nuclear Energy Degree the applicant for an operating license has to submit a PSA to STUK. According to the Government Decision (395/1991) nuclear power plant safety and design of its safety systems shall be substantiated by PSA. Detailed requirements on the use of PSA for risk informed regulation and safety management have been set forth in the Regulatory Guide YVL2.8.

The Finnish licensees have not used US PSA standards while performing the current PSAs.

Both Finnish licensees have developed their own PSA guidance independently from each others, based partially on international experience and PSA guidance on the late 1980ies, and partially on their own, and partially on Finnish national research activities. STUK has accepted the methods used in connection with the PSA analysis.

4.2.18 Czech Republic

Safety demonstration of Czech NPPs currently relies on deterministic principles where the Probabilistic Safety Assessment is considered to be a supporting decision tool, always used as a complementary to deterministic approach.

Neither legally binding national standards, nor prescriptive national regulatory guides have been developed in the area of PSA yet. There are no legally binding specific guides, which have been indicated as being strict guides to be followed for the PSAs of the nuclear power plants and PSA applications.

For the PSA main tasks (accident sequence delineation, system modelling, human reliability analysis, CCF modelling, HRA, accident sequence quantification, etc.) methodologies have been adopted within the individual plant PSA projects. Several reference documents (NUREGs, IAEA guidelines, other PSAs, etc.) have been considered for this purpose.

At Temelin and Dukovany NPPs several PSA related guidelines have been developed for Nuclear divisions:

- PP 158 "Probabilistic Safety Assessment – PSA maintenance and applications guideline"
- Me 441, rev.0 "Plant specific data gathering system for PSA"
- Me 457, rev. 0 "Guideline for use of real-time risk assessment tool - Safety Monitor"
- Me - , rev.3 "Guideline for risk informed assessment of Tech Specs (AOT)",

The Czech Regulatory Body (SUJB) facilitated increased use of PSA techniques for risk informed applications by introduction of probabilistic approach into regulatory body decision making process by documents "SUJB PSA Policy" and "Action Plan of SUJB PSA Policy Implementation" in 2003. Subsequently, the regulatory body guidelines were developed within 2004 to 2006 in the frame of "PSA Applications Project". The guidelines are as follows:

- Methodological Guidelines For Using PSA In Risk-Informed Decisions On Plant-Specific Changes In Technical Specifications, Rev. 1.
- Guidelines for evaluation of risk-informed license amendment requests to be used for regulatory decision making, Rev. 0.
- Risk-Informed Categorization of SSCs - Methodological approach, Rev. 0

4.2.19 Canada

Regulatory policy, standards and guides in Canada

<u>Safety Goals for Nuclear Power Plants (NPPs) (P-324)</u>: Most of the information on this policy has already been included in Section 3. The policy is intended to promote Safety Goals to ensure that NPPs are safely-built and operated so as to protect health, safety, security and the environment and to respect Canada's international commitments on the peaceful use of nuclear energy.

The policy describes the Safety Goals to be taken into account by the CNSC when making a regulatory decision concerning the licensing of NPPs.

Use of both Deterministic and Probabilistic Criteria for Regulatory Decision Making (P-151) The draft issued in 1999 is presently on hold.

<u>Reliability Program for Nuclear Power Plants (S-98)</u>: The standard has been revised and re-issued in July 2005 [2] and it requires the licensees:

- to identify and rank the systems, structures and components (SSCs) according to their risk significance,

- to specify the targets for assessing the reliability of the risk-significant SSCs (through surveillance activities),
- to record, report and document the program activities and its results.

The standard's requirements are consistent with the growing trend in the Canadian nuclear industry towards the use of risk-informed processes and applications.

All licences are being amended to include S-98 as a new condition of operation. The reliability programs from each licensee have been submitted to CNSC for review. The Standard will be accompanied by a regulatory guide, G-98 (see below).

<u>PSA/PRA for Nuclear Power Plants (NPPs) (S-294)</u>: The regulatory standard, published in April 2005 [2], will be incorporated into the licence to construct or operate a NPP or other legally enforceable instrument. The standard sets out the requirements for the plant specific Level 2 PSA that licensee shall perform. The PSA models have to reflect the plant as built and operated, as closely as reasonably achievable, within the limitations of PSA technology and consistent with the risk impact. The PSA models will include both internal and external events[4], and at power and shutdown states. The quality assurance process and the technical quality of the PSA must be acceptable to the CNSC. The models shall be updated every three years or sooner if major changes occur in the facility.

<u>Regulatory Program for Nuclear Power Plants (G-98)</u>: This document accompanies the regulatory standard S-98. The draft guide developed in 2002 needs updating to ensure consistency with new developments in the area of regulatory documents. However, most of the work has been done, and at this point, a working group is expected to be set up to produce the final document.

There will be consultations with the licensees. Since 2003, the industry, under the umbrella of the industry's Candu Owners Group (COG), commenced to develop recommended good-practice guidelines for implementing the S-98. The interim industry guidelines document has been drafted and is expected to be finalized in 2007.

<u>Balanced Use of Deterministic and Probabilistic Criteria in the Decision-Making (G-152)</u>: The guide, drafted back in 1999, is one of the most important documents still to be issued. The purpose of the regulatory guide is to provide guidance to the CNSC staff when considering probabilistic arguments to complement the traditional ones for decision making. The document guides the user how to use the PSA to prioritize inspections, to assess licensees submissions, and how to review the appropriateness of the PSA for the given application, along with the use of reference safety metrics (e.g., CCDF).

The draft has been used as one of the important references in developing the guidance document on risk-informing CNSC planning, licensing, and compliance activities for power reactors.

<u>PRA attributes (G-42) necessary for every foreseen application</u>: The draft guide has been issued almost a decade ago, and at present is still pending completion. The main intent of the document is to provide guidance regarding the attributes of the PSA for specific applications. The use of G-42 will guide the CNSC in assessing the technical quality of the PSA.

<u>Implementation of the Policy on Cost-Benefit (P-242)</u>: A Cost-Benefit Analysis (CBA) Group has been formed to prepare a guide on the use of cost-benefit analysis.

The group prepared and presented for CNSC upper management's approval, a position paper that addresses the use of CBA to support or to influence regulatory decision-making which falls under

[4] The external events may be excluded from the scope of the PSA upon the condition the CNSC agrees on the alternative analysis method used by the licensee to conduct the assessment.

CNSC jurisdiction. In 2004, the paper has been endorsed by the CNSC vice-president. Since then, no significant progress has been done towards the completion of the guideline.

A COG Working Group developed a document on behalf of the industry that is intended to be used as a basis for guidance by the industry. This document has been produced using existing standards and government policy, in consultation with CNSC. Point Lepreau Nuclear Generating Station has used the CBA during the development of its refurbishment project. The CNSC will consider this document as it develops its own guidance.

At the beginning of 2004, COG issued the document "Benefit-Cost Analysis Implementation Guidelines" (available on: http://canteach.candu.org/catalog.html#COG).

Industry policies, standards and guides in Canada

Ontario Power Generation (OPG) has developed Corporate Governance regarding the development and use of PRA (PSA). The OPG Nuclear Safety Policy expressly requires the development of PSA for each nuclear plant and its use to support decision making.

The PSA Standard provides for preparation, maintenance and application of PRA at Ontario Power Generation. The purpose of the PRA is to establish whether the design and operation of the plant poses an acceptable level of risk to the workers, the public, and the environment, and to identify the major sources of risk. The purpose of risk assessment maintenance is to ensure that the PRA represents the current state of the plant, and therefore reflects any changes to the design, operation and maintenance of the plant. The purpose of risk assessment application is to support continuing use of PRA in decision-making relating to the conduct of engineering, maintenance, and operations at Nuclear facilities after the initial PRA is completed.

The PRA Guide is intended to be a reference document for PRA practitioners to build and apply OPG PRAs in a consistent manner at each station.

The OPG PRA Guide generally follows international practice adapted for use at multi-unit Candu plants. The guide covers the major elements of a Level 3 PRA, consisting of:

- Initiating Event Identification and Quantification
- Event Tree Analysis
- Fuel Damage Category Analysis
- System Fault Tree Analysis
- Common Cause Failure Analysis
- Component Reliability Data Collection
- Human Reliability Analysis
- Event Sequence Quantification
- Accident Analysis
- Containment Analysis
- Public Health Risk Assessment
- Economic Risk Assessment (optional)
- Uncertainty Analysis

Each of the elements of the PRA is addressed in the PRA Guide. Each subsection discusses the purpose of the PRA element, the inputs to the activity, and the outputs or deliverables of the element, as well as outlining the steps necessary for completion.

Results of PRA have been used for quantified cost/benefit analysis, in accordance with CNSC policy P-242. The Canadian industry has developed a standard methodology for the use of cost-benefit analysis in decision making, though the Candu Owners' Group (COG).

OPG is in the process of developing numerical criteria to support operational decision making, issued as "Guideline for Management of Incremental Risk from Abnormal Plant Configurations". The objective of this guideline is to provide consistent risk management principles to cover all the scenarios (planned or unplanned) which requires risk-informed decision making for continued operation. The guideline was produced based on best industry practices and is currently issued for a period of trial use.

Bruce Power at the time of separation in 2001 had a similar hierarchy of policies, standards and procedures as OPG but has since then gradually evolved.

The BP policies and procedures in PRA are being integrated with Bruce Power's Management System Manual that governs the corporate business process structure and associated governing documents. The main governing document for PRA is a divisional document (DIV-OD-00028) on Probabilistic Risk Assessment. It derives authority from a Process Level 3 document (BP-PROC-00363) which pertains to Nuclear Safety Assessment that in turn supports a Process Level 2 document (BP-PROG-10.01) on Plant Design Bases Management.

The main PRA document describes the intended conduct and application of PRA for Bruce Power nuclear facilities and the expectation that PRA is consistent with good practice in the industry. It calls on a set of related Process Level 5 procedures, which are in various states of preparation, for implementation of PRA-related programs and applications. Key procedures in this set include the following:

- Preparation and Maintenance of PRAs
- Assessment Guidelines Using PRA
- Risk Assessment of Operational Events
- Evaluation of Risk Outside the Scope of the PRA
- Risk Assessment of Proposed Change to Engineering, Operations, surveillance and Maintenance
- Outage and Online Risk Management
- Risk Significance System Decision Methodology

4.2.20 Belgium

Neither national standards, nor national regulatory guides have been developed in the area of PSA.

There are no specific guides (either national guides or guides from international organisations or other countries), which have been indicated as being strict guides to be followed for the PSA-analyses of the nuclear power plants. For the main tasks of the PSAs (accident sequence delineation, human reliability analysis, CCF modelling, accident sequence quantification, etc.) methodologies have been defined within the PSA projects. Several reference documents (NUREGs, IAEA guidelines, other PSAs, etc.) have been considered for this purpose.

5 STATUS AND SCOPE OF PSA PROGRAMS

5.1 Summary

All operating nuclear power plants in the reporting countries have been studied using PSA methods. A Level 1 internal events PSA has been performed on all plants. In many cases, this has been extended to a Level 1+ or Level 2 PSA. In several cases, the Level 2 PSA consists mainly in the determination of the Large Early Release Frequency (LERF), rather than a complete Level 2 analysis of plant damage states. More and more, the Level 1 PSAs have been (or are being) extended to consider low power and shutdown events. Examples include Belgium, Canada, Japan, Korea and Switzerland. In other instances, analyses of only a few plants in a given country have been performed to identify the need, if any, for further analysis.

External events, such as earthquakes, high winds, floods, and internal fires and other external or area events, as necessary, depending on the site are being factored into the basic PSA analyses in several countries or have already been considered. In some instances, the methods used for seismic analysis consist of a combination of probabilistic and deterministic analyses, such as the Seismic Margins analytical technique. These have been found to be adequate to identify outliers in the overall risk profile. Fire risk analytical methods have been the subject of considerable recent research. The analyses that have been completed reflect the state of the art at the time they were performed. In most cases, these analyses will be updated as part of the periodic update of the PSAs.

Only a few level 3 PSAs have been performed. They have typically been used to develop insights into the societal risk of a class of plants. One country (Canada) does require a Level 3 analysis on all plants. Several countries will require Level 3 analyses for new plants of advanced design.

In most countries, the PSA is updated as part of the Periodic Safety Review which is part of the regulatory requirements. The interval for this update varies from three to ten years. In countries where a formal Periodic Safety Review is not performed, updates are made as necessary when the PSA is used to support a regulatory action.

There is an increasing use of PSA in risk monitor mode in several countries. This allows more direct use of PSA methods and results by the operational staff and by regulatory body. Several countries require that a living PSA be maintained (e.g., Finland, Korea, and Switzerland).

5.2 Country replies

5.2.1 USA

Since the publication of the landmark Reactor Safety Study (WASH-1400) in 1975, plant-specific PSAs have been completed for all operating U.S. nuclear power plants. These studies have been performed by licensees and by the NRC. Notable licensee studies performed in the early 1980s include the Big Rock Point, Oyster Creek, Zion, Indian Point, Limerick, and Oconee PSAs. Notable NRC studies performed in the late 1980s include the NUREG-1150 analyses of the Surry, Peach Bottom, Sequoyah, Grand Gulf, and Zion plants, and the NUREG/CR-4832 and NUREG/CR-5305 analyses of the LaSalle plant.

In 1988, the NRC issued Generic Letter (GL) 88-20, which requested all licensees with operating nuclear power plants to perform an Individual Plant Examination (IPE) for severe accident vulnerabilities. The scope of the IPE program included internal initiating events (including internal flooding events, but not internal fire events) occurring at full power. In 1991, the NRC issued Supplement 4 to GL 88-20, which requested that all licensees perform an Individual Plant Examination of External Events (IPEEE). The scope of the IPEEE program included external events (including seismic, high wind, external flooding, accidental aircraft crash, transportation, and offsite industrial events) and internal fire events. The primary goal of the IPE and IPEEE programs was for licensees to identify plant-specific vulnerabilities to severe accidents. The specific definition as to what constituted a vulnerability was left to the discretion of the licensees.

In response to these generic letters, the NRC received submittals covering all operating U.S. plants. The results of the IPE program are summarized in NUREG-1560. Key results of the IPEEE program are summarized in NUREG-1742.

Since the completion of the IPE and IPEEE programs, licensees have continued to update their PSAs to reflect plant changes (many of which involved improvements identified by the IPEs and IPEEEs) and current operational experience. Gaertner et al discuss some of the results and insights from post-IPE/IPEEE plant-specific PSAs, as well as example plant changes spurred or enabled by these PSAs.

The NRC has developed Standardized Plant Analysis Risk (SPAR) models for each plant and is in the process of benchmarking these models against licensee PSAs.

The key characteristics of these studies vary, as discussed below.

PSA objectives

The preceding PSAs discussed above were performed for a variety of reasons. For example, the WASH-1400 and NUREG-1150 studies were performed to develop an improved understanding of severe accident risk. The Big Rock Point and Oyster Creek studies were performed to prioritize and justify safety changes. The Zion, Indian Point and Limerick studies addressed the risk to large nearby populations; the first two studies also addressed the risk reduction potential of particular accident mitigation strategies (e.g., filtered vented containments). The Oconee PRA was performed to demonstrate PRA methods, train PSA practitioners for utilities, and provide a model for future utility studies. NUREG/CR-4832 was performed to, in addition to characterizing the risk for the LaSalle plant, develop, apply, and evaluate improved PSA methods and procedures. NUREG/CR-6143 and NUREG/CR-6144 were performed to assess the risk significance of events occurring during shutdown operations at the Grand Gulf and Surry plants, respectively. The IPEs and IPEEEs were performed not only to identify plant-specific severe accident vulnerabilities but also to develop an improved understanding of severe accident behavior and to identify potential cost-effective plant improvements.

With the increasing use of risk information in regulatory decision making, current PSA work is aimed at supporting a wide range of risk-informed regulatory applications, as discussed in Section 7.US.

PSA level

All U.S. plants have Level 1 and Level 2 assessments. Most of the current Level 2 assessments are limited in scope, being focused on the assessment of large early release frequency (LERF). Level 3 PSAs have been performed only for a few plants. NRC's SPAR models are Level 1 PSAs; work to develop LERF models is ongoing.

Initiating events addressed

Most PSAs for U.S. plants address the full range of initiating events usually considered for internal events analyses (including different classes of loss of coolant events, transients, and support system failures).

Regarding seismic events and internal fires, some of the plant PSAs address these initiating events and others do not. (As discussed in Section 6.US, some plants used simplified approaches, e.g. seismic margins studies aimed at identifying vulnerabilities to satisfy the requirements of the IPEEE program, while not providing quantitative estimates of risk.) Only a limited number of plants have performed PSAs for other external events (e.g., high winds, external flooding, accidental aircraft crashes).

Modes of operation addressed

Most of the current PSAs are limited to consideration of events occurring during full power operation. Only a few PSAs address events occurring during low-power or shutdown operation.

PSA updates

When used to support risk-informed regulatory applications, PSAs are required to reflect current plant conditions relevant to the application. However, NRC does not require periodic updates. A few plants employ risk monitors to manage risk.

5.2.2 United Kingdom

PSA for the Sizewell B PWR

The PSA that has been produced for Sizewell B is a full scope Level 3 PSA. It addresses all modes of operation of the plant (full power, low power and shutdown modes), and all internal initiating events and internal and external hazards.

The PSA that was produced as part of the safety case leading up to fuel load in September 1994 has been revised so that it can be used as a Living PSA during station operation. The Level 1 and 2 parts of the analysis has been changed from a large fault tree approach to one that is based on linked event trees and fault trees using the Risk Spectrum software. The Level 3 part of the analysis has been factored in using invariant transformation matrices. This PSA gives a better estimate of the risk by removing some of the conservatisms which were in the licensing PSA and will be used by the licensee to advise on configuration control during plant outages, to assist in monitoring the validity of the Technical Specifications and to produce risk profiles with the aim of maintaining the risk as low as reasonably practicable.

Current model developments include: updating generic data with Sizewell B specific data, further increasing the scope of the electrical modelling to support station activities, more detailed analysis of mid-loop operation, revising the RCP Seal LOCA modelling.

The PSA has been used to provide operational support in a number or areas including the following:

- increasing the enrichment of the fuel used in the reactor,
- increasing the time defined in the Technical Specifications for refuelling from 18 months to 2 years,
- considering the best options available for managing the risk during refuelling outages. This addressed the risk which would arise when the reactor coolant system inventory was reduced to mid-loop level,
- optimization of the in-service testing intervals for Motor Operated Valves, and
- safety case support.

In 2004 the Sizewell B PSA was subjected to a licencee lead International Probabilistic Safety Assessment Review Team (IPSART) review which, upon request from British Energy, mainly focused on the suitability of the PSA to support risk-informed decision-making.

PSA for the AGRs

PSAs have been produced for all the AGRs as part of the Periodic Safety Reviews (PSR) which are carried out every 10 years. The aim of these analyses being to address the dose criteria established by the licensees in line with the SAP 42 criteria (see section 3.2 above). The first Periodic Safety

Reviews (PSR1) for the AGRs was started in 1994 with the last, Heysham 2 and Torness, being completed in 1999.

The PSR1 PSAs considered only internal initiating events occurring during full power operation (the licensee having argued that the level of risk during shutdown conditions would be very low). These PSAs addressed internal initiating events fully but have only a limited treatment of internal and external hazards.

The PSA has been used to provide operational support in a number or areas including:

- increasing the time given between refuelling outages from 2 to 3 years, and
- extending the duration of shifts at Hinkley Point B from 8 to 12 hours, and
- safety case support.

In addition, the Heysham 2 and Torness PSR1 PSAs were enhanced to produce a four-quadrant model which explicitly represents initiating events occurring in each of the four quadrants. The four-quadrant model is being maintained as the Living PSAs for these stations, and is used as the basis for the updated Risk Monitors that are being implemented.

Currently the PSAs for the Hinkley Pt B and Hunterston B AGRs are being updated to PSR2 (completion 2006).

Progress is now underway on the updating of the Dungeness B, Hartlepool and Heysham 1 PSR2 PSA, for completion in 2007. Whilst work will start on the PSR2 update of the Torness and Heysham 2 AGR PSAs for completion in 2008.

Note: Between the PSR1 and PSR2 updates the PSAs are updated to reflect major changes thereby ensuring that an understanding of the station risk can always be inferred.

In 2002 and 2003 respectively, the Hinkley and Hunterston PSAs were subjected to NII-led international reviews that adopted an approach based, to some extent, on the IAEA IPSART (International PSA Review Team) Service. Follow-up reviews are being carried out in 2006/07. NII has plans to perform similar reviews for all the other AGR PSAs.

PSA for the Magnox reactors

A Long Term Safety Review (LTSR) was carried out for each of the Magnox reactors to determine whether it was safe to allow operation to continue beyond 30 years. The LTSRs reviewed the plant against both engineering/deterministic and probabilistic principles. As a result of this, a number of changes were identified to the design and operation of the plant which were required to meet modern standards and to reduce the risk. In addition, significant deficiencies were identified in the scope and contents of the PSAs and it was agreed that they should be improved.

The PSAs for all the Magnox reactors were completed and updated as part of the PSR process. These PSAs addressed internal initiating events occurring during full-power operation only. There was only a limited treatment of internal hazards and, for natural external hazards such as seismic events, a deterministic approach had been used supported by some probabilistic analysis.

In the analysis, it has been assumed that failure to trip, shutdown or provide post trip cooling would lead to a large release - that is, an off-site dose of greater than 1000 mSv. Sequences which resulted in smaller releases (generally less than 100 mSv) were also assessed in terms of frequency and consequence and the results brought into the consideration of whether the risk from the station was ALARP. The smaller releases arise from sequences following a successful reactor trip and shutdown where there was nevertheless the statistical possibility of limited fuel failures. In addition, the analysis has addressed faults involving water ingress into the reactor with safety relief valve lift, and fuel route faults.

The Magnox PSAs have been used for a number of activities as follows:

- to inform decision making with respect to requirements for heating and ventilation dampers used to protect equipment from the effects of a loss of primary coolant accident (hot gas release),
- to assist in setting the design requirements for modifications to boiler headers whose failure would result in a loss of primary coolant accident (hot gas release),
- to inform on the benefits of modifications in terms of reductions in expected accident cost, and
- to check that operating rules related to plant unavailability deliver satisfactory control of risk.

Currently only two Magnox reactors remain operational; Oldbury due to close in 2008 for which no further updates of the PSAs will be required; and Wylfa where a revision of the LTSR PSA is currently nearing completion (2006). In addition the Wylfa PSA will be enhanced to include a more detailed consideration of fire hazards; this work is due to report in late 2007.

In 2004 the Wylfa PSAwas subjected to an NII-led international review that adopted an approach based, to some extent, on the IAEA IPSART Service.

5.2.3 Taiwan

PSAs of three operating NPPs were conducted following their commercial operation. The scope of at-power PSAs includes level 1 internal events (LOCA, ISLOCA, transients, scrams with specific support system failures and ATWS) and external events (seismic, typhoon, fire and flood). In 1995, the at-power PSAs were updated to living PSAs. The PSAs of both Kuosheng and Maanshan included full scope level 2 analysis in their original PSA but not being revised when updated to living PSA. The living PSA for at-power containment integrity is limited on LERF evaluation. For living shutdown PSA, only level 1 internal events were included.

Lungmen PSA was already included in PSAR which was prepared by the reactor vender. The living PSA of Lungmen conducted by INER will be completed before startup test. The scope is the same with the operating NPPs.

5.2.4 Switzerland

Historical Development:

The development of a PSA for a Swiss nuclear power plant was started in 1983. This initiative was aimed at the development of a level 1 PSA for the Beznau nuclear power plant. Subsequently, in 1987, HSK required the utilities to perform full power level 1 and level 2 PSAs for all Swiss nuclear power plants. Four years later, HSK additionally required the licensees to develop plant-specific low power and shutdown PSAs including external events.

In the meantime, PSAs for all Swiss nuclear power plants have been completed by licensees and independently assessed by HSK. The plant-specific PSAs include internal and external events such as fires, flooding, earthquakes, aircraft impacts and high winds. Level 1 PSAs have been developed for full power as well as for shutdown mode. Several intermediate updates of the PSAs have been performed. For every periodic safety review a fully updated PSA needs to be submitted to HSK by the licensees.

In February 2005, a new Nuclear Energy Law and an accompanying ordinance were enacted in Switzerland. The ordinance anchors the PSA and also its application into the law. The ordinance requires the quantification of the release risk for all relevant operational modes. This implies the introduction of a level 2 PSA for low power and shutdown modes. It is intended, until the end of 2006, that the licensees present ideas on how to perform such an analysis. The specific requirements will then be defined in a guideline (see Section 4).

Level of PSA:

All Swiss licensee PSAs are full scope level 1 and level 2 studies. A level 3 PSA is not required in Switzerland.

Range of Initiating Events Included:

The plant-specific PSAs include all relevant internal and external events such as fires, flooding earthquakes, aircraft impacts and high winds.

Modes of Operation Addressed in the PSA:

All relevant operational modes are assessed as part of the Swiss PSAs. This requirement is also anchored in the appendix of the ordinance.

Living PSA:

Living PSA process is a requirement that has been mandated by HSK, in order to ensure that the PSAs are commensurate with important plant hardware and operational changes. A list of all plant modifications that are not implemented in the plant-specific PSA model and that may have some impact on the PSA results is continuously being maintained. At least every five years, the PSA model is updated to reflect plant modifications and accumulation of additional reliability data. As part of the Periodic Safety Review (i.e., usually conducted every ten years), PSAs are revised as needed to consider advances in methods, and to reflect the current operational experience. Every licensee has prepared procedures that outline the utility process and policies applicable to maintaining their plant-specific “living PSA”. The implementation of “living PSA” at all plants was completed in 2005.

5.2.5 Sweden

Description of the status and scope of the PSA:s that have been carried out in Sweden as follows, (status in the beginning of 2006):

Within the reactor safety area SKI:s supervision is to ensure that Swedish nuclear facilities implement and maintain adequate protection based on the concept of multiple physical barriers to prevent the occurrence of severe incidents and accidents originating from technology, organisation or human competence as well as to prevent or mitigate radioactive releases to the environment in the event of an accident. Thus, safety must be based on the internationally accepted defence-in-depth principle, which has been adopted in the international convention on nuclear safety, in order to protect man and the environment from the harmful effects of nuclear activities.

Status of the Swedish PSA programme, is as follows (as of 28th February 2006): See Appendix A.

5.2.6 Spain

The Probabilistic safety Analysis (PSA) has being used in Spain as an important tool for helping the risk informed regulation, risk informed inspections and the new implemented reactor oversight process.

The common scope established by the PSA Integrated Programme second edition for the Spanish NPP PSA is that of Level 1 and 2 analyses, including all reactor operating modes and all external events. The original scopes of the plant specific PSA has been progressively increased and most of the seven original PSA have reached that level, including the Low Power and Shutdown PSA (SPSA).

Current status can be summarized as follows:

- Garoña. (BWR, GE Mark I). CSN review completed for Level 1, Level 2 and internal (fires, floods), SPSA and external hazards. Whole PSA revised and updated by the utility in 2005.
- Almaraz. (PWR, W 3 loops). CSN review completed for Level 1, Level 2 and internal and external hazards. PSA have been revised and updated in a continuous maintenance process. SPSA was finished in 2005
- Asco. (PWR, W 3 loops). CSN review completed for Level 1, Level 2, SPSA and fires and internal floods. Whole PSA revised and updated between 2001 and 2003. Level 2 for external events is finished.
- Cofrentes. (BWR, GE Mark III). CSN review completed for Level 1, Level 2 and internal and external hazards. PSA has been revised and updated in a continuous maintenance process. SPSA was finished in 2004.
- Jose Cabrera. (PWR, W 1 loop). CSN review completed for Level 1, Level 2 and fires and internal floods. Whole PSA have been revised and updated in 2005. SPSA have been finished and it is been reviewed by the CSN. PSA used extensively in the Periodic Safety Review process. The plant was permanently removed in April, 2006 from commercial operation after 38 years of operation.
- Vandellos. (PWR, W 3 loops). CSN review completed for Level 1, Level 2, SPSA and internal and external hazards. Level 1 PSA revised and updated in 2002. SPSA started in 2005.
- Trillo. (PWR, Siemens 3 loops). CSN review completed in 2001 for Level 1, internal floods, Level 2 and external hazards. Level 1, Level 2 and internal flooding have been revised and updated in 2005. Fire risk analyses still to be completed by the utility. SPSA was finished in 2005.

Appendix A gives an overview of the time schedule of the different PSA projects.

According to the plant specific PSA status above summarised, the PSA performance activities are basically on the completion of the review of some SPSA studies submitted by the utilities. Therefore, from the last years the PSA activities in Spain are mainly directed towards PSA applications and related tasks, like the PSA maintenance and updating process.

PSA have to be maintained and updated according to the GS 1.15, incorporating the operating experience and the impact on the risk of the plant modifications every fuel cycle, also a completed PSA updated has to be done with the PSR every ten years.

CSN and the licensees agree to maintain and update the PSA through the issue by the CSN of the Regulatory Guide GS 1.15. This guidance establishes the basis and scope of the maintenance and updating depending of the impact on the risk of the plant and procedures modifications. Otherwise the applications submitted to the CSN required that the PSA has to be updated specially on the aspects related to the application in course. The scope of the updating has to be commensurate with the impact on the risk of the plant application.

5.2.7 Slovenia

Historical development

The development of the PSA started in Slovenia in 1991 with the issuance of a SNSA decree, which required from the Krško NPP to develop the PSA for all plant states of operation. The KRŠKO NPP PSA model was originally developed along the KRŠKO NPP IPE / IPEEE project (1994 – 1995). Since then the PSA model has undergone various revisions to reflect plant configuration changes. The model has also undergone various peer-reviews by IAEA IPERS and IAEA IPSART missions. The last review was preformed within the scope of the PSR.

Level of PSA and addressed modes of operation

The Krško NPP has developed a detailed Level 1 and Level 2 PSA model for full power operation (including internal and external events) and a simplified PSA model for low power and shutdown states, which also include internal and some external events. A Level 3 PSA was neither developed nor required by the SNSA.

Range of initiating events included

The plant-specific PSA include all relevant internal initiating events. Also events such as internal fire, internal flooding, seismic and other external events (aircraft accidents, external flooding, severe winds, external fire, industrial facility accident, pipeline accident, release of chemicals in on-site storage, transportation accidents and turbine generated missiles) are included.

Living PSA

Living PSA was required by the SNSA in order to ensure that the PSA reflects a real plant configuration. The PSA model is updated regularly by the plant after each larger modification or at least once per fuel cycle.

Use of PSA at the Krško NPP

PSA is used at the Krško NPP for determining the necessary modifications that reduce the total CDF or LERF. Changes that mostly helped in reducing the total CDF of the plant were the changes involving the fire protection system or equipment fire barriers. Fire protection action plan implemented in the year 1999 helped reduce risk by more than 85 %. Also the recent reduction by more than 50% in the seismic CDF has significantly reduced the total CDF of the plant. The seismic hazard re-evaluation was conducted in 2004.

The Krško NPP also uses PSA for evaluating and scheduling the on-line maintenance of equipment, technical specification optimization, plant modernization and for plant event analysis.

Use of PSA at the SNSA

The SNSA uses PSA studies to assess plant modifications, as a source of information and for performance of analyses, including event analyses. Next, the SNSA also uses PSA studies for informing the wider expert community on the Krško NPP safety.

5.2.8 Slovak Republic

The status of PSA for the Slovak NPPs is as follows:

- The J. Bohunice V1 NPP: Level 1 and level 2 full power and shutdown PSA is performed for the post reconstruction status of the plant. According to an agreement reached with the EU several years ago, the Bohunice V1 plant is to shut down prematurely. An agreement requires that Unit 1 will be shutdown in December 2006 and Unit 2 in December 2008. In order to assess the site risk a PSA study was performed for Unit 2 of the Bohunice V1 plant after termination of the Unit 1 operation. Risk assessment is performed for full power operation of the reactor and for the refueling outage. Risk assessment is also performed for the Unit 1 in the time period of 2007-2008 and for final shutdown of both units after 2008.
- The J. Bohunice V2 NPP: Level 1 and level 2 full power and shutdown PSA is performed for the plant. Within the living PSA program of the plant the PSA studies are being updated.
- The Mochovce NPP: Level 1 full power and shutdown PSA is performed for the plant. Within the living PSA program of the plant the PSA study is being updated. At the present time the level 2 PSA study of the plant is being undertaken.

5.2.9 Netherlands

Borssele

In the PSA of the Borssele NPP were analysed for all operating states for all internal, external and area events.

For the level 2-analysis 16 source terms were the result of the binning process.

Within the PSA framework a special assessment was carried out regarding the so-called human Errors of Commission. Although no proper numerical evaluation was possible, the assessment could identify several weak spots.

Dodewaard

In the PSA of the Dodewaard NPP all 3 levels were analysed for all operating states for all internal, external and area events. A very detailed seismic PSA was made due to some weaknesses of the plant regarding its structures

For the level 2-analysis 12 source terms were the result of the binning process.

In 1997 Dodewaard was closed down permanently and prepared for decommissioning. All PSA activities were stopped.

High Flux Reactor (HFR)

The PSA of the HFR is a level-3 PSA covering only the full power state and covers both internal events and area events (fire and flooding)

5.2.10 Mexico

The PSA program in Mexico formally started in the early 80's during the construction phase of the Laguna Verde nuclear power plant, with the conformation of PSA groups within the different institutions of the nuclear sector: the utility (Comisión Federal de Electricidad), the regulatory agency (Comisión Nacional de Seguridad Nuclear y Salvaguardias) and the national research institutes (Instituto de Investigaciones Eléctricas and Instituto Nacional de Investigaciones Nucleares).

In 1985 a multi-institutional PSA group was formed in order to apply the PSA techniques to the evaluation of the core damage frequency for Laguna Verde Nuclear Power Plant unit 1. The group was integrated with staff members from the above mentioned organizations, under the technical project management of the Instituto de Investigaciones Eléctricas (Electric Research Institute). This project was developed on a voluntary basis, since there was no regulatory requirement at that time to perform a PSA.

Once this project was completed, the PSA groups within the different institutions continued their probabilistic safety assessment related activities at various levels of effort. The regulatory agency initiated their first PSA application to the safety evaluation of Laguna Verde NPP, the analysis of the station blackout scenario. The station blackout event tree was developed along with the development of front line and support systems fault trees. During the development of this analysis, and as a result of the lacking of a regulatory probabilistic model of LVNPP that would establish the initial and boundary conditions for a posterior containment response analysis, as well as the need to have and adequate tool for regulatory decision making and for benchmarking the results of the licensee plant specific evaluation, the objectives and scope of the initial station blackout analysis were reoriented to yield a full Internal Event Analysis for Laguna Verde NPP unit 1. This PSA level 1 developed for the regulatory staff excludes the external events and consider the full power operation of LVNPP unit 1 as initial condition. The initiating events considered involved 3 types of LOCA's inside the primary containment, one interfacing LOCA and seven transient categories. Systemic event trees were developed for each initiating event depicting the possible plant response to the initiating event and solving the core vulnerable sequences. Over 30 fault trees for front line and support systems were developed. Generic data, compiled from different sources, were used to quantify the accident sequences as well as the total core damage frequency. Uncertainty and importance analyses were performed for the total core damage frequency. After the conclusion of the PSA level 1, the CNSNS began the development of a PSA level 2 for the 25 plant operational states obtained in the Internal Event Analysis.

In parallel, the regulatory authority, following the USNRC generic letter 88-20, requested the utility to perform an Individual Plant Examination (IPE) of Laguna Verde NPP. The IPE involved a thorough examination of the plant design and operation to identify dominant severe accident sequences and their contributors. Then the utility (CFE) proceeded to assess areas of potential improvements and to implement them when warrant by a cost-benefit analysis. The scope of the IPE is equivalent to a Level 1 and Level 2 analysis for events initiated during full power operation by internal initiating events and internal flooding events. The CFE performed the front-end analysis of the IPE by updating the PSA level 1 that had been developed by the above multi-institutional project. The Instituto de Investigaciones Eléctricas was commissioned by the utility to perform the back-end analysis of the IPE using the NSAC 159 methodology. The IPE was submitted to the regulatory authority and subject to a detailed review process.

The primary objective of the IPE review process was addressed to determine whether the CFE met the intent of the Generic Letter 88-20, i.e., that the CFE (1) develop an overall appreciation of severe accident behavior through their involvement in the IPE process; (2) understand the most likely severe accident sequences that could occur at Laguna Verde NPP; (3) gain a quantitative understanding of the overall probability of core damage and radioactive material release; and (4) reduced the overall probability of core damage and radioactive release by modifying procedures and hardware to prevent or mitigate severe accidents.

The current PSA model for Laguna Verde developed by the utility and approved by the regulatory authority, is a detailed one that involves the utilization of safety and non-safety systems that assess the impact of the containment status on the continued core cooling (i.e. the model evaluates the harsh environment as result of primary containment venting or failure and evaluates the failure probability of the core cooling systems components to survive such conditions). The PSA model uses plant specific data for failure rates and for initiating event frequencies.

The utility develop a Risk Monitor (RM) in order to comply with the paragraph 4 of the Maintenance Rule, which states that before performing maintenance activities the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The Risk Monitor was developed using the Equipment-Out-Of-Service (EOOS) computer package from EPRI/SAIC. The regulatory authority has been involved in the review of the implementation of the PSA models into the EOOS software. The RM is updated accordant with the updating of the PSA used to support such tool, commonly the updating takes place on each refueling.

Currently the CNSNS is involved in the development of PSA level 1, internal events, for low power and shutdown conditions.

5.2.11 Korea

It has been recommended to the utility to do plant-specific level 2 PSA, including external events (mainly fires, floods, and seismic) analyses, identifying the mitigating plant features against severe accidents. As a result, in the case of new plants, level 2 PSAs have been done, depending on their construction schedule. On the other hand, APR1400 was decided to do full scope (Level 3) PSA for using PSA insights in a standardized design and operation.

KHNP performs PSA and develops risk monitoring system as planed on the implementation plan to satisfy SAP. In accordance with the implementation plan, PSAs on the Level-1 and Level-2 internal/external events for all operating NPPs were completed in 2005, and risk monitoring system will be installed in all domestic NPPs until the end of 2007. For NPPs under the construction, KHNP is performing the Level-1 and Level-2 internal/external event PSA during the full power operation and the Level-1 internal event PSA during the shutdown operation as a part of construction permission and operating licensing.

PSAs of operating NPPs

The PSAs for operating NPPs cover basically Level-2 PSA on the internal event, internal fire, internal flood and seismic during the full power operation. Kori unit 1, the oldest plant in Korea, is Westinghouse 2-loop NPP, and its first PSA was completed in 2002. The analysis for the seismic event is analyzed by SMA (Seismic Margin Assessment). Kori unit 2 which is a Westinghouse 2-loop NPP performed its PSA in 2003, and is being revised along with the risk monitoring system development.

Kori units 3&4 and Yonggwang units 1&2 are the Westinghouse 3-loop NPPs, and their first PSAs were completed in 1992, and revised along with the development of risk monitoring system in 2003. The first PSAs cover the evaluations of the internal events, internal fires, internal floods, earthquake and typhoons. Since the design related with an earthquake was reinforced after the first PSAs, typhoon event is excluded from the revisions. The PSA peer review was performed for the revised PSA for Kori units 3&4 in 2005.

Yonggwang units 3&4, Ulchin units 3&4, Yonggwang units 5&6 and Ulchin units 5&6, which are KSNP 1000MWe rating NPPs, performed PSAs in design stage to find out the vulnerabilities of the plants and to improve their safety. Especially, Yonggwang units 5&6 and Ulchin units 5&6 performed the internal event Level-1 PSA during the shutdown operation. In addition, the revision of their PSAs will be completed by 2006 reflecting operating experiences. The revision of Yonggwang units 3&4 PSA and Ulchin units 3&4 PSA revised the analysis, including success criteria analysis based on recent PSA results, so improved the consistency in the results.

As for CANDU 600MWe NPPs, Wolsong units 2,3 and 4 performed their first PSAs during the construction phase, and Wolsong unit 1 which had started the commercial operation in 1983 performed the PSA in 2003. These PHWR NPPs currently revise their PSAs, and make an effort to improve the consistency for success criteria, etc. The seismic event analysis for Wolsong unit 1 is performed using SMA. Ulchin units 1&2 which are Framatome 900MWe NPPs performed the first PSA in 2005.

PSAs of NPPs under the construction and design stage

PSA for the plant under the construction is used to identify the effects of the design changes and to maintain the plant safety. The scope of PSA is same those of operating PSAs. The scope also covers the Level-1 PSA on the internal events during the shutdown operation.

Shin-Kori units 1&2 and Shin-Wolsong unit 1&2, advanced KSNP OPR 1000 units, are being constructed by 2010 and 2012. These NPPs' designs are upgraded through various system changes based on the designs of original KSNP plants. As for these plants, Level-1 internal event PSA during the full power operation was performed to check the safety compared to the core damage frequency (CDF) of the previous KSNP in the design developing process.

Shin-Kori units 3&4 are the plants based on APR1400 which has been developed in Korea. In the process of the APR1400 development, Level-3 PSA during the full power operation and Level-1 PSA during the shutdown operation were already performed for the internal and external events. Through these PSA results, it is verified the plants have lower risk metrics than the previous 1,000 MWe rating plants.

PSAs for regulatory uses

In any regulatory matter affecting the risk, a requisite for achieving reasonable decision making is to be supported by qualified technical information. Also, due to the increased public requests for giving a safety guarantee, the regulator should provide the visible means of safety. The use of PSA by the regulator can give the answer on this problem. Therefore, in order to study the applicability of risk information for regulatory safety enhancement, it is a demanding task to prepare a well-established regulatory PSA model and tool.

KINS has been developing a general guidance for using risk information in regulatory decision-making, and the fundamental policy for implementing risk-informed regulation. KINS is also preparing the regulatory position on relevant issues, including PSA quality. In 2002, KINS and KAERI together made a research cooperation to form a working group to develop the regulatory PSA model - so-called MPAS model. The MPAS stands for multipurpose probabilistic analysis of safety. For instance, a goal of the MPAS model is to give essential risk insights in the preparation and implementation of various regulatory programs. Major role of this model is to provide some independent risk information to the regulator during regulatory decision-making, not depending on the licensee's information. The MPAS model is pilot-developed for KSNP (Korean Standard Nuclear Power Plant) and finished for Level 1 PSA model in 2005 [3], which aims at having the equivalent quality of ASME PSA capability category II. The MPAS model for evaluating LERF (large early release frequency) is being developed.

5.2.12 Japan

Basic Concept for Risk Informed Regulation

In November 2003, NSC published the basic policy statement to introduce the RIR concept in nuclear regulation in Japan, aiming at (i) enhancement of the rationality, consistency and transparency of the safety regulation and proper allocation of resources for activities of the safety regulation and (ii) improvement of regulation, which is currently based on the conventional engineering judgment and deterministic safety assessment, by utilizing PSA results, while maintaining the defense-in-depth concept.

In 2003, NISA started discussion to embody RIR reflecting the NSC policy statement. Then in December 2004, NISA established a subcommittee on the utilization of risk information in the safety regulation under the Advisory Committee on Nuclear and Industrial Safety (ACNIS) in order to study the concrete approaches for the utilization of risk information. The basic concept was discussed under the subcommittee, in the following view points;

- status and issues of current safety regulation, and the role of risk information in the nuclear safety regulation,
- characterization of the risk information, and the merit of its utilization,
- basic approach toward the risk informed regulation, etc

Supported by the subcommittee, NISA, in collaboration with JNES, established the Basic Concept for RIR in May 2005 after receiving the public comments of one month.

This Basic Concept includes the feature and role of the "risk information", the approach of NISA to utilize the "risk information", etc. Its summary is as follows.

(1) One of major objectives, that NISA addresses, is to enhance the rationality of the nuclear safety regulation and to realize the effective and efficient regulation. It is expected to be a valuable approach for improving the rationality, effectiveness and efficiency of the regulation to apply PSA methods and associated information (i.e., "risk information").

(2) PSA has a capability to quantify the risk from the nuclear facility, by comprehensively assembling and evaluating various sorts of safety related information, and to provide the "risk information", such as a total risk level, a contribution level of each SSC to the total risk, and their uncertainty. The limitations of PSA should be taken into account. Namely, PSA results contain inherently uncertainty due to the incompleteness of models, the limitation of the state-of-knowledge, etc. Therefore, the utilization of the "risk information" continues to maintain the defense-in-depth philosophy and the adequate safety margin, both of which are essential elements in the current safety regulation.

(3) The "risk information" should be initially applied to regulatory issues, where PSA quality is appropriately achieved, and the application is deemed to be most intensive, urgent and practical. Therefore, NISA will firstly utilize the "risk information" gained from PSA, which evaluates the risk associated with the severe accident of nuclear power plants. Especially, NISA, with a priority, intends to principally promote the application of the "risk information" to the development of the regulatory system, criteria, guidelines, etc. On the other hand, NISA will judge to promote or not, on the case by case basis, the application of the "risk information" to confirm that an individual plant complies with the regulation. NISA will also review and identify the possible regulatory areas to which the "risk information" may be applied, and identify issues to be studied, for regulatory activities of other nuclear facilities than nuclear power plants.

(4) NISA will continue discussions on the risk informed items of mid and long term phase, and to develop the common recognition among pertinent organizations. NISA will develop and follow up the implementation plan that covers the concrete actions to steadily promote the application of the "risk information" to the safety regulation, together with the regulatory guidelines necessary to promote the application of the "risk information" to the safety regulation. NISA will also achieve the accountability through activities to understand interests of the public sincerely, and to provide the information, including the policy and concepts with due considerations to assuring the adequate transparency.

The NISA's approach to utilize the risk information is consistent with that in the NSC's "Interim Report".

NSC's Taskforce on Introduction of Risk Informed Regulation

NSC set up the taskforce on introduction of risk informed regulation (RIR) in April, 2004. Since then the taskforce has reviewed the status of risk considerations at related organizations and discussed the issues for developing RIR in Japan. The taskforce prepared the interim report on the review results and discussions in December, 2005.

The report described that the risk consideration in concerned organizations in Japan has made progress in line mostly with the NSC's basic policy for introduction of RIR expressed in 2003. However, the followings were identified as important issues for further promotion of RIR introduction: policy for utilization of risk information considering Japanese features, usage of safety goals and performance objectives in RIR, decision-making process using risk information, pilot program, PSA quality, improvement of safety examination guidelines considering risk information, utilization of risk information in nuclear fuel cycle facilities and risk communication.

The taskforce plans to prepare the final report within about three years from the issue of basic policy in November 2003 and will continue to promote the further introduction of RIR in the future.

Revision of Examination Guide for Seismic Design of Nuclear Power Reactor Facilities

NSC approved the examination guide for seismic design of nuclear power reactor facilities on September 19, 2006, which was revised through the five-year intense discussions in the subcommittee composed of the experts and specialists in the field of earthquake. The main motivation of the revision was the reflection of the significant technical advancements occurring after the former guideline was issued in 1981. The advancements include the technologies for the geological investigation for the active faults, the numerical prediction of the strong earthquake motion, and the earthquake-proof design such as seismic isolation, which were enhanced especially after the Hyogo-ken Nambu Earthquake in 1995.

In the revised guideline, the subcommittee recommended to analyze the exceedence probability of the design-basis-ground-motion (DBGM) to provide complementary information to discuss the adequacy of the conservatism in determining DBGM. The subcommittee also concluded that the qualitative use of the exceedence probability in the licensing process is helpful to provide opportunities to find and solve problems in calculation of the probability, to promote the study related to the seismic PSA, and to contribute to the future risk-informed regulation.

The new guideline will be applied to the regulation for the reactor construction in the future. However for the existing plants, NSC recommended NISA to take actions so that the utilities make an appropriate review on the seismic safety of the nuclear facilities based on the new guideline.

NISA directed the utilities to make a review on the seismic safety of the nuclear facilities based on the new guideline and to report to NISA the results of their reviews. The review will be performed in the two steps: First, deterministic seismic safety back-check of the existing nuclear facilities; second, evaluation of the residual risk of the facilities by seismic PSA after the completion of the deterministic seismic safety back-check.

5.2.13 Italy

Not applicable.

5.2.14 Hungary

Historical development

A project called Advanced General and New Evaluation of Safety (AGNES) was performed in Hungary between 1992 and 1994 under the sponsorship and supervision of both the Hungarian Atomic Energy Authority (HAEA) and the Paks NPP. The project was aimed at a comprehensive reassessment of the safety level of the Paks plant by the use of internationally accepted and state-of-the-art safety principles, requirements, analysis methods and tools. It also included level 1 PSA that was the first comprehensive PSA study for the plant. The PSA part of the AGNES Project included internal initiating events during full power operation of the reactor. Unit 3 (out of the 4 VVER-440/213 units operating at Paks) was selected as a reference unit for the analysis. The conclusions of the first PSA – completed in 1994 – corresponded well to that of other safety analyses performed under the auspices of the AGNES Project. The safety level of the plant was found to be similar to the safety of other PWR's of the same vintage inernationally.

Recommendations were made in the AGNES Project to extend the safety-upgrading programme of the plant and prioritise the necessary safety measures based on the results gained. In particular, quantitative results and qualitative findings from the PSA study were used for prioritising safety enhancement efforts as well as for identifying areas of safety concern that needed further investigation following the AGNES Project. An important recommendation was to make extensions to the PSA study in a number of areas. This recommendation has been taken into consideration since the AGNES Project ended. Also, emerging requirements from the regulatory authority have added momentum to continue and extend the PSA programme for Paks. Accordingly, in the recent years substantial improvements and extensions have been made to the original PSA to ensure a credible, up-to-date safety assessment and to support safety enhancement at the plant by PSA applications.

The PSA scope and level of detail for Paks has been gradually extended. The major steps of this developmental process have been as follows:

- First the level 1 PSA of anticipated internal initiators at full power operation was performed for each unit within the framework of periodic safety reviews for the plant. This ensured not only plant but unit specific PSA models and results. The availability of unit specific PSA studies appeared particularly important during the intense period of safety upgrading at Paks, i.e. between 1994 and 2002 when PSA was applied to support design of safety measures and also to evaluate effectiveness of improvement form the point of view of risk reduction.
- The second major extension to the Paks PSA was level 1 PSA for an annual refuelling outage (so-called low power and shutdown PSA) including all phases of cooling down, refuelling and start-up. Unit 2 is the reference unit for the shutdown PSA, and the results were found applicable to the other units at Paks too. Use was made of the shutdown PSA to meet regulatory requirements for the scope of PSA and to reduce core damage risk in shutdown operations by means of partly administrative, partly technical measures.
- The scope of level 1 PSA was further broadened by analysing internal fires and internal flooding during full power operation. Similarly to internal events, analysis of these internal hazards was done on a unit specific basis. Although the four units are seemingly almost identical, differences can be observed if the fire and flood PSA results are compared for the different units. This is attributable to differences in location of safety related components, cables in particular.
- A level 1 seismic PSA was done parallel to completing the seismic upgrade of the plant. Unit 3 was selected for seismic PSA. Recommendations for improvements made on the basis of seismic PSA are given to serious consideration by the utility. Core damage risk from seismic events is expected to decrease mostly as a result of further structural reinforcement in the turbine hall.

- In addition to the reactor core, fuel assemblies in the spent fuel pool (SFP) were also looked at as a potential source of large radioactivity releases. Internal events, internal fire and internal flooding were analysed in the PSA for the SFP. Again, PSA identified measures to reduce the risk of fuel damage in the SFP.
- A level 2 PSA was performed for all types of initiating events and plant operational states that were included in the level 1 analysis at the time of launching the level 2 PSA project. Currently the level 2 PSA covers internal events, internal fires and flooding during full power operation, internal events in low power and shutdown modes as well as accidents of the spent fuel pool duo to internal event, internal fires and internal flooding.
- As to ongoing analyses for Paks, it should be noted that level 1 PSA for internal fires and internal flooding during shutdown operation is near completion. Also, level 1 shutdown PSA for seismic events has been started. Extension of the level 2 PSA to seismic events in full power operation is underway too.

Level of PSA

As described in the previous chapter, both level 1 and level 2 PSA studies are available for the Paks NPP. This is in agreement with regulatory requirements laid down in the Nuclear Safety Codes. Although the level 1 and the level 2 analyses differ in scope, the objective is to finalise the studies at both levels so that all important plant operational states, all initiating events are covered and all potential sources of large accidental releases are considered.

Range of initiating events included: The initiating events included in the Paks PSA cover internal technological events, internal hazards, and earthquakes:

- Loss of coolant accidents, transients and special common cause initiators were analysed from among internal technological events. The total number of internal events exceeds 50 in the full power PSA and these events were grouped into 14 categories. The same types of internal events were considered in the low power and shutdown PSA resulting in a much greater value for the total number of events analysed because the low power and shutdown PSA covers 24 plant operational states. Also, attention was paid to special internal initiators and initiating events in the shutdown PSA such as pressurised thermal shock, heavy load drop, termination of natural circulation and inadvertent boron dilution in the primary circuit.
- Internal fires and internal flooding were the subject of the PSA for internal hazards. All plant locations, systems and components were looked at to identify the potential sources of fire or flooding during full power operation of the reactor and during all operational states of the spent fuel storage pool.
- The seismic PSA for unit 3 of the Paks plant includes earthquakes ranging 0,07g from to 1,00g in terms of horizontal peak ground acceleration (PGA) of the free soil as determined from seismic hazard analysis for the site. These earthquakes have been considered for full power operation to date.

Modes of operation addressed: The level 1 PSA that is available for the Paks NPP covers full (nominal) power operation of the reactor as the most common and longest plant operational state. In addition, the plant operational states of the annual refuelling outage have been analysed too, covering all phases of shutdown, refuelling and start-up. The PSA of the spent fuel pool addresses all of its planned plant operational states including storage and configuration features when the reactor is at power, when it is under partial refuelling (annually) as well as when it is under complete refuelling (every fourth year).

Living PSA: All the available logic models, databases, results and documentation for the Paks level 1 PSA are regularly updated using a living PSA procedure. Safety related plant modifications and changes in the reliability characteristics of plant equipment and/or plant personnel are modelled and quantified. The updating is performed in co-operation between plant personnel and PSA analysts of VEIKI. Operation of this living PSA helps to follow changes in the safety level of the plant, and it also ensures that risk based decisions can be supported by up-to-date risk models and data. Living PSA enables a range of PSA applications and it also ensures usefulness and credibility of results gained from the applications. Both the utility and the regulatory body possess the very same living PSA models. The latest PSA update was made in 2005 following the regular refuelling outages for the four units of NPP Paks.

In general, the update is made annually so that the updated models and results represent the plant state after the start-up following the refuelling period each calendar year. Plant modifications are generally made during refuelling outages and the focus of the living PSA has been on these modifications in the past ten years. The use of the living PSA approach has been particularly helpful during the safety upgrading programme for Paks. The input data base of the PSA is updated less frequently because the reliability of plant systems and components do not change so dynamically that an annual update would be necessary and justifiable. After some eight years without any significant changes in input data a complete update of the component reliability data base is on agenda for the next PSA update due by the and of 2006. Data update will focus on the operating experience accumulated at the Paks NPP in the recent years.

There is no living PSA programme in place for the level 2 PSA of NPP Paks. However, a complete revision and update of the initial analysis is planned in a 2-3 year timeframe.

Appendix A presents a concise description of PSA history for the Paks plant.

5.2.15 Germany

In the Atomic Energy Act of 2002 the dates when the results of the safety review have to be submitted to the regulator are fixed (see following table). Because of the limited remaining lifetime of German NPPs the Atomic Energy Act uses the term "Safety Review (SR)" instead of "Periodic Safety Review (PSR)", since for most plants the review has to be performed only once in the remaining lifetime.

<u>Table:</u> *NPP and date of submission of safety review to the authority*

Plant		Type/ Electrical power (net)/ Year of commissioning	Date of (P)SR
Biblis A	KWB A	PWR / 1167 / 1974	Dec. 2001
Brunsbüttel	KKB	BWR / 771 / 1976	June 2001
Neckarwestheim 1	GKN 1	PWR / 785 / 1976	Dec. 2007
Biblis B	KWB B	PWR / 1240 / 1976	Dec. 2000
Isar 1	KKI 1	BWR / 850 / 1977	Dec. 2004
Unterweser	KKU	PWR/ 1285 / 1978	Dec. 2001
Philippsburg 1	KKP 1	BWR / 890 / 1979	Aug. 2005
Grafenrheinfeld	KKG	PWR / 1275 / 1981	Oct. 2008
Krümmel	KKK	BWR / 1260 / 1983	June 2008
Gundremmingen B	KRB B	BWR / 1284 / 1984	Dec. 2007

Gundremmingen C	KRB C	BWR / 1284 / 1984	Dec. 2007
Grohnde	KWG	PWR / 1360 / 1984	Dec. 2000
Philippsburg 2	KKP 2	PWR / 1385 / 1984	Oct. 2008
Brokdorf	KBR	PWR / 1370 / 1986	Oct. 2006
Isar 2	KKI 2	PWR / 1365 / 1988	Dec. 2009
Emsland	KKE	PWR / 1290 / 1988	Dec. 2009
Neckarwestheim 2	GKN 2	PWR / 1269 / 1989	Dec. 2009

5.2.16 France

History

In 1977, the Safety Authority set probabilistic safety objectives relating to the probability that a plant could be the source of unacceptable consequences (see section 3). However these objectives were only considered as orientation values and the demonstration of compliance with these objectives was not required.

Later on, and although it was not a regulatory requirement, partial probabilistic studies were carried out since 1980 by EDF (Electricité de France – the French utility) and IPSN (Institute for Nuclar Protection and Safety - technical support of the Safety Authority), and two global PWR PSAs were completed in 1990.

The first of these studies (PSA 900) concerns a standard reactor of the 900 MWe series, and was carried out by IPSN. The second study (PSA 1300) was carried out by EDF for a unit representative of the 1300 MWe series.

The PSAs have been developed independently by IPSN and EDF. However, the important problems related to methods and data were discussed together, and extensive mutual external reviews by EDF and IPSN were very helpful in order to assess the exhaustiveness of the PSAs as well as the validity of the assumptions made. Since PSA was not a regulatory requirement, the relations between EDF and IPSN were more a cooperation and a technical dialogue than a classical safety analysis process.

The results of these studies led to several important plant modifications and backfits.

Presently French PSA activities are carried out in mainly three organisations: IRSN (Institut de Radioprotection et de Sûreté Nucléaire - Technical support of the Safety Authority), EDF (Électricité de France) and CEA (Commissariat à l'Énergie Atomique). These activities concern the development of PSA models and methods, as well as PSA applications for various safety analysis problems. Moreover, for the French-German project of a future plant (the European Pressurised water Reactor-EPR), a PSA was performed by the designers since the beginning of the design, and analysed by the Safety Authorities.

PSA has been recognised as an important tool for safety analysis in France, and it appeared necessary for EDF and for the Safety Authority to define a more precise framework for PSA developments and applications. So a Basic Safety Rule has been issued in 2002.

PSA development in IRSN

Level 1 PSA for 900 MWe NPP: The level 1 PSA for 900 MW plant series (CPY series) was updated in year 2004 and completed for the site of BUGEY (CP0 series). The results of the level 1 PSA are used for the review of the level 1 PSA performed by EDF in the framework of the Periodic Safety Review of the 900 MW plant series.

*Level 1 PSA for 1300 MWe NPP:*The level 1 PSA for the 1300 MWe standardised PWRs is finished and a publication of the main report has been performed. Updating of Level 1 PSA for 1300 MW NPP must begin in 2006. This study should be available for the third Periodic Safety Review of these plants (2009).

Fire PSA for 900 MWe NPP: A version of the fire PSA for 900 MWe was performed in 2004 taken into account the event oriented operating procedures. In 2004, results obtained in the framework of the Fire PSA activities are used for the review of 900 MWe fire protection improvements.

Level 2 PSA for 900 MWe and 1300 MWe NPP: The level 2 Probabilistic Safety Assessment for the French 900 MWe PWR is on-going. A version of the study was performed in 2003 for power states of reactor. This version is being updated on the following points:

- plant modifications (recombiners, new severe accident guides …),
- severe accident studies with last version of severe accident codes,
- improvement of uncertainties evaluation for physical phenomena,
- evaluation of core reflooding possibility during the degradation process,
- introduction of shut-down states of reactor,
- interface between level 1/ level 2 PSA,
- assessment of radiological consequences for each release category (with standard meteorological data).

In 2004, results have been used for the review of EDF level 2 PSA for the 900 MWe series. For the 1300 MWe series a level 2 PSA is planned for 2009 (third 1300 MWe periodic safety review)

PSA development in EDF

Level 1 & 2 PSA for 900 MW NPP: The level 1 PSA for 900 MW plant series (CPY series) was updated in year 2003 and completed in 2004 for the sites of BUGEY and FESSENHEIM (CP0 series). Accordingly, the final results of Level 2 PSA have been produced in 2004 on the basis the new updated version of the level 1 PSA for CPY and CP0 series. Those PSA has been discussed till the beginning of 2005 with the technical Support in the framework of the preparation of the next Periodic Safety Review of the 900 MW plant series. Standing Group meetings dedicated to Level 1 & 2 PSA hold in February 2005.

Level 1 PSA for 1300 MW NPP: The updating of Level 1 PSA for 1300 MW NPP has begun in 2005. It takes into account the plant modifications decided during the second periodic safety Review of the EDF 1300 MW plant series.

Level 1 PSA for 1450 MW NPP: Updating of Level 1 PSA for 1450 MW NPP was achieved in 2005. It takes into account Safety Authority expectations, future uses of PSA for AOT calculations and a preliminary assessment of containment failure (Level 1+ PSA). It will be used for safety assessments during the preparation on the first periodic safety Review of the EDF 1450 MW plant series.

PSA for EPR project: The development of a Level 1 PSA and a simplified Level 1+ PSA (containment failure assessment) for the Preliminary Safety Assessment Report (expected in April 2006) of the French EPR has continued in 2005. It is based on the PSA developed during the EPR basic design and takes into account Safety Authority expectations. The development of the Level 1 PSA for the Intermediate Safety Assessment Report (expected in 2010) has begun in 2005.

5.2.17 Finland

In Finland, the regulatory authority (STUK) and licensees have introduced probabilistic safety analysis (PSA) as a widely used method in the nuclear safety regulation and safety management. The possibilities of probabilistic methods in nuclear safety management were recognized by the Finnish authorities and licensees in the early 1970`s while the Loviisa and Olkiluoto NPPs were under construction. In 1984, STUK formally required the Finnish licensees to perform PSA studies. The first PSA studies were submitted to STUK in 1989.

STUK´s requirement included that the licensee personnel performs the PSA studies as an in-house project. External consultants were to be utilized only in support of methodological tasks. The goal was a living PSA model, which is easy to use and keep constantly up-to-date. The underlying idea of this approach was to make the plant personnel well commited to the efficient use of PSAs. These decisions laid the foundation for the present use of PSA in risk informed regulation by the authority (STUK) and in risk informed safety management by the licensees. Risk-informed regulation means an approach where both the PSA results and the deterministic criteria combined with engineering judgment are considered and they complement each other in regulatory decision-making. The general aim of the risk informed methods is to use the available resources in the most efficient way to maintain and increase the nuclear safety.

STUK and the licensees made also a special agreement for introducing the Living PSA as a common information platform. According to the agreement, the identical, reviewed PSA model is used for resolution of safety issues both by the licensee and by STUK. The use of the same PSA model gives a common basis for discussions between the authority and the licensees on risk-related issues. A prerequisite for the use of a common model is a thorough review of the PSA models by the authority.

The risk-informing of regulatory and risk management activities is a step by step process. STUK has promoted the use of PSA in regulation and safety management of NPPs since 1987 when the regulatory guide YVL 2.8 was issued. The first version of the guide set forth several requirements to the licensees on how to use PSA in the safety management of the NPPs. The 1996 version of YVL 2.8 extended the use of PSA to further applications and the 2003 version extended it still further. The regulatory guide YVL 2.8 includes general guidelines for ensuring the quality of PSA.

Today the Living PSA is formally integrated in the regulatory process of NPPs already in the early design phase and it is to run through the construction and operation phases all through the plant service time. STUK will review the PSAs and makes an assessment of the acceptability of the design phase PSA/ construction phase PSA prior to giving a statement about the construction licence/operating licence application. This approach is used in the licensing process of OL 3 EPR plant unit.

Living PSA models have been developed for both the Olkiluoto and Loviisa NPPs. The PSA studies include level 1 and level 2 models. Level 1 comprises the calculation of severe core damage frequency (probability per year) and level 2 the determination of the size and frequency of the release of radioactive substances to the environment. At the moment, level 1 studies for full power operation cover internal events, area events (fires, floods), and external events such as harsh weather conditions, and seismic events. The shutdown and low power states of level 1 PSA cover internal events, floods, fires (being studied for Loviisa NPP), harsh weather conditions, oil and seismic. The Lo Level 2 studies include internal events, flooding and weather in full power state and are being extended to cover fires as well as low power and shutdown states. The OL Level 2 study includes the same initiators as level 1 PSA.

Level 1 and 2 Design Phase PSA was developed for the application of construction licence of OL 3 EPR. The development work continues for construction phase level 1 and 2 PSA which is to be submitted to STUK in conjunction with the application of Operating Licence.

PSA has got an important role in the evaluation of needs for plants modifications of operating plant units. The licensees have provided STUK with the assessment of safety significance of each proposed modification. The risk assessment has to be submitted to STUK independent of the safety class of the systems to be changed. For example, in the course of past several years the estimate of the core damage frequency of the Loviisa plant has decreased with a factor of ten thanks to the plant modifications.

In the area of operational events, PSA is a standard tool to assess the safety significance of component failures and incidents. Today risk follow-up studies are a common practice at STUK. Since 1995 STUK has performed systematic risk follow-up studies on the annual basis for each Finnish nuclear power plant unit.

Certain inconsistency of AOTs in comparison with the respective risk impact has been identified between various safety systems. Risk assessment has also questioned the traditional conclusion that in all faulted states the shutdown of the plant would be the safest course of action. If systems used for decay heat removal are seriously degraded (CCF), it may be safer to continue operation than to shut down the plant immediately, although shutdown may be required by the current Technical Specifications. Hence the licensees has to re-evaluate the relevance of allowed outage times (AOT) of most important front line safety systems and to figure out those failure states of the plant when it is safer to continue operation than to shut down the plant immediately.

If a licensee applies for an exemption from Tech Specs the licensee has to submit a risk analysis to STUK and indicate that the risk from the exemption is tiny. STUK reviews the licensees´ analysis and makes its own risk assessment for comparison as necessary.

STUK allows on-line preventive maintenance during power operation provided that the deterministic safety criteria are fulfilled (e.g. single failure criterion) and the risk contribution is small. According to the first Olkiluoto PSA study in 1989, the risk contribution of on-line preventive maintenance was about 5 % of the total core damage frequency. When the maintenance schedule was optimised with PSA, the risk contribution of on-line preventive maintenance could be reduced to less than 1 % of the total core damage frequency.

Pilot projects on in-service inspections of piping both in a pressurized water reactor plant (Loviisa) and a boiling water reactor plant (Olkiluoto) have been completed by STUK in cooperation with the licensees. STUK's risk-informed procedure combines both the plant specific PSA information and the traditional insights in support of the system specific detailed in-service inspection program planning. Finnish licensees have set up projects for risk-informing their in-service inspection programmes. RI-ISI approach is used also in the context of the on-going EPR project.

STUK is in progress of training inspectors to understand and use the PSA insights while planning the regulatory inspection programs and conducting the inspections at site. A special PSA Info system has been developed in order to use the insights of PSA for training the inspectors, to upgrade their risk perception and to demonstrate the importance of most significant accident sequences.

5.2.18 Czech Republic

A basic PSA study as a first step of typical PSA programme, was for NPP Dukovany unit 1 completed in 1995 /initial version in 1993/. The study was performed for internal initiators and full power operation. Since that milestone a "Living" PSA programme has come into force at the site. Three main project tasks have been established within ongoing Living PSA Programme in Dukovany NPP: Risk management (executive task), Data Collection and Information Exchange (data support task) and Maintenance and continuous improvement of PSA models (maintenance task). [2]

Specific Living PSA QA guidelines have been developed to assure consistency of all current activities and to establish a control system for information transfer, which is necessary for Dukovany PSA models use, maintenance and improvement. For all regular activities specific schedules have been defined. The basic living PSA models and all related PSA applications tools are updated regularly every year.

The original PSA of Temelin NPP Unit 1 was performed during 1993 -1996 and covered Level 1 PSA for both at power and non-power modes of operation, external hazards, seismic hazard and the Level 2 analysis. Acts of sabotage, acts of war, and off-site consequence of fission product on public health were not evaluated. From the project beginning also the requirement to transfer PSA technology to the NPP Temelin members of the project team so that the resulting models could be used by plant personnel in the future, both for the "real-time" (Safety Monitor) and "normal" (WinNUPRA) evaluation of a wide range of design and operational issues. [3]

The current Dukovany Living PSA models, which include analysis of internal initiators, internal fires and floods, reflect all power plant modifications up to December 2005 and are valid for all operating states. There are three unit specific models, one for unit No. 1, one for unit No. 3 and common one for units No. 2 or 4. RiskSpectrum PSA /RS PSA/ Professional code is used for PSA model development and calculation. Models for both reactor units in the twin co-unit are maintained in the common RiskSpectrum database. Such approach allows explicit modeling of shared systems including their neighbor unit support systems.

The Level 1 PSA model for NPP Dukovany in RS PSA is extended with Level 1/Level 2 interface model to obtain simplified Level 2 model. The Level 1/Level 2 interface contains consequentional event trees linked to the same or similar Level 1 event tree sequences. It addresses systems that maintain Containment Integrity critical safety functions as well as systems not addressed in Level 1 event trees but important for Level 2 accident progression event trees (APET's). The interface results in 31 Plant Damage States (PDS's). Conditional LERF given PDS frequency is then obtained from detailed Level 2 model developed with EVNTRE code and included into interface event trees.

The PSA model for each NPP Dukovany unit is capable to quantify not only total average yearly risk (CDF, FDF, LERF), but also risk resulting form each POS or risk resulting from each IU over all relevant POS's.

For the Dukovany plant Unit 1 at power operation, Level 2 PSA analysis was performed excluding external events like earthquake or airplane crash, but including internal floods and fires. Level 1 results were binned into PDS and the accident progression and containment response were described by a probabilistic analysis based on the large event tree APET method. The main supporting tool for accident sequences analysis was MELCOR, its results were supplemented by expert judgement especially in the region of energetic events or plant design features not included in MELCOR (DDT, DCH, containment and cavity strength, cavity door). Source term calculation and binning was included in the event tree using retention factors obtained from MELCOR analyses. Only the very crude method of sensitivity analyses was used for mapping uncertainties.

Appendix A gives an overview of the time schedule and scope of the Dukovany PSA project.

Temelin NPP basic PSA study was completed in 1996 for all operating modes and internal and external events and updated in 2002. A Level 2 analysis was a part of study.

In order to reflect actual design status following safety improvements prior commissioning and better understanding of the short operational experience of the plant to the PSA, all Temelin original models, i.e. Level 1 internal initiating events for both at power and shutdown states, were updated in 2002 time frame to ensure that information and assumption in the PSA reflects the ultimate design and construction of the plant.

The update activities continued in 2003 by the fire hazard analysis, flooding hazard analysis and Level 2 PSA update, as well as by the update of the on-line risk evaluation tool - Safety Monitor™ models.

For the Temelin PSA, the Level 2 analysis was performed binning accident sequences into Plant Damage States (PDS) and a probabilistic analysis of the containment response for all core damage sequences with the MELCOR and other codes analyzing phenomena in the containment. In this way, the phenomena (hydrogen burning, basemat melt-through, DDT conditions, DCH, etc.) threatening the containment integrity could be identified for each of these typical accident scenarios. Limited source term analyses have been performed. Only at power operational states were covered by Level 2 analysis.

An update of the Temelin PSA is done annually as a consequence of adopted PSA concept as well as regulatory body requirement to provide regular PSA models update, maintaining them consistent with the plant actual status for risk informed applications.

Appendix A gives an overview of the time schedule and scope of the Temelin PSA project.

5.2.19 Canada

In Canada, the licensees have developed PSAs over the last two decades. Since 1987, when the Darlington Probabilistic Safety Evaluation (DPSE) has been issued, four more PSAs have been completed for operating plants, namely Pickering A Risk Assessment (PARA-1995), Pickering B PRA (PBRA-2006), Bruce B Risk Assessment (BBRA-1999), and Bruce A PRA (BAPRA-2003). The summary regarding the scope and use of the CANDU plants PSA is presented in Appendix A, Figure 1.

The completed PSAs for multi-unit plants received by CNSC are Level 3 PSAs, at full power and shutdown operating states (BAPRA's shutdown risk model has not yet been provided to the regulator), including internal events and flooding. The DPSE, PARA, PBRA and BBRA were developed as result of the industry initiatives.

On the other hand, development of the BAPRA was one of the CNSC conditions to be satisfied prior to the restart of two laid-up units (Units 3 and 4). The same study is being used and applied in support of the licensee safety case for the refurbishment of the other two units (Units 1 and 2) of the Bruce A plant. BAPRA forms part of and supports the Periodic Safety Review associated with the Bruce refurbishment project.

All PRA s belonging to OPG, i.e., PARA, PBRA, DPSE, as well as those for Bruce Power were developed for multi-unit plants with many shared systems and the PRA model must address the interfaces and interactions between units. This results in very large fault tree models. In the level 1 part, at-power and shutdown states are analysed. A wide scope of internal events is covered, represented by typically 150 initiating events, including LOCA's, secondary line breaks, transients and loss of support system functions (electric power, service water, instrument air, etc..). Some internal hazards (fire) and all external hazards (except loss of offsite power) are currently not covered but must be addressed in the future when regulatory standard S-294 is applied. Candu PRAs also consider Level 1 end-states involving limited core damage, primarily to assess economic risk implications.

Level 2 analysis has been performed initially using scoping calculations and more recently using the MAAP3B and MAAP4-CANDU code. The results are used to bin sequences into up to ten release categories for comparison with safety goals and use in the level 3 analysis. Only at-power states are covered.

OPG plants are located near highly populated areas so information on the potential societal impacts of accidents is of interest. Level 3 analysis has been performed using the MACCS2 code to estimate public health and economic consequences of accidents.

An update of the PSAs every 3 years has been set as the requirement in the OPG PRA Standard.

The PSA study for Point Lepreau Generating Station is under development with the on-line CNSC review of the model. This is a Level 2 PSA, for both full and shutdown states, including internal and external events (flood, fire, seismic). The insights are being used for refurbishment purposes.

Regarding new designs, AECL produced a Level 1 PSA, for full power and shutdown states, and internal events, including limited flood analysis. The model was a design-assist tool for the ACR-700.

The CNSC reviews all the PSAs. In general, the reviews of the PSA technical quality have been performed off-line, following a two-stage process that assumed a preliminary and then a detailed review. The 1st stage, the preliminary review was focused on the qualitative assessment of the PSA adequacy in terms of completeness, quality assurance, scope of the work, methods applied, and results. In addition, the preliminary review identified the key areas and key accident sequences that constituted the input for the 2nd stage of the review (the detailed review). This last stage was the quantitative assessment of the PSAs, with insights regarding the model weaknesses, and plant vulnerabilities. The BAPRA has recently completed this CNSC review.

5.2.20 Belgium

A specific PSA model has been developed for each plant (Doel 1/2, Doel 3, Doel 4, Tihange 1, Tihange 2, Tihange 3).

In the level 1 part, power and non-power states are analysed, covering about 99% of the operating profile of the NPPs. A wide scope of internal initiating events is covered, including LOCA's, secondary line breaks, transients and loss of particular functions (electric sources, heat sink, ..). The update of the level 1 models foresee, among others, the update of some methodologies (HRA, CCF, etc.), the extension of the covered POS to 100%, the update of plant specific features.

Internal hazards (fire and flooding) and external hazards are not covered. Nevertheless, fire and flooding PSAs are foreseen in the following years. These studies should start in 2010 and be completed in 2015 for all belgian units.

In the previous PSR, level 2 analyses performed for the Belgian NPPs were limited to the analysis of the containment response, with the aim to investigate dominant containment failure modes. No source term analyses have been performed. Only power states were covered.

For the Doel 3 and Tihange 2 PSAs, the level 2 analysis was limited to a binning into Plant Damage States (PDS) and a deterministic analysis of the containment behaviour for some dominant core damage sequences with the STCP code. In this way, the phenomena (hydrogen burning, basemat melt-through, etc.) threatening the containment integrity could be identified for each of these typical accident scenarios, however without obtaining information on the probabilities of the failure modes.

For the Doel 1 and 2 and Tihange 1 PSAs, a probabilistic level 2 analysis using Containment Event Trees (CETs) was performed, using MELCOR for the analysis of the severe accident progression.

The scope of the update of level 2 analyses is discussed in the framework of the actual PSA. The update will be based on a hybrid accident progression event tree (APET), which will be quantified for different representative units. The shutdown states will be covered as well as the determination of the source term.

Appendix A gives an overview of the time schedule of the different PSA projects.

6 PSA METHODOLOGY AND DATA

6.1 Summary

The overall methodology described by all the countries uses the small event tree/ large fault tree approach for the Level 1 PSA and an event tree approach for the Level 2 PSA. The methodology generally follows the approaches described by NRC (for example in NUREGs CR-2300 and 1150) or the procedures for carrying out Level 1, 2 and 3 PSAs defined by IAEA in the Safety Series documents and associated TECDOCs. In addition, it is recognised that the approach used for the PSA and the level of detail of the model need to be consistent with the proposed PSA applications.

In the Level 2 PSA, there is a wide variation in the number of Plant Damage States defined, the number of attributes used to define the PDSs, the number and type of nodes in the Containment (Accident Progression) Event Trees and the number of Source Term/ Release Categories defined. However, it is now agreed that all the consequences of a severe accident can be modelled by either a small event tree or a large event tree approach.

A number of countries have highlighted the need to identify a comprehensive set of initiating events as the starting point for the PSA. The way that they have done this is to apply a number of different approaches that typically includes the use of generic lists of initiating events, the existing PSAs for the same type of reactor, top down approaches such as the use of a Master Logic Diagram, bottom up approaches such as Failure Modes and Effects Analysis (FMEA) and the use of operating experience data.

In a number of countries, there has been a move towards an integrated approach to the Level 1 – Level 2 analysis that avoids the need to group cut-sets into PDSs which are then used in the Level 2 PSA. The integrated approach is aimed at avoiding this “discontinuity” in the analysis.

The accident sequencing modelling to support the event tree analysis is carried out using integral codes such as MAAP and MELCORE, and a range of separate effects codes. In addition, new codes have been developed in some countries.

The functional and physical dependencies are included explicitly in the PSA model. In addition, there are a number of methods of taking account of the residual dependencies not taken into account explicitly. These include the Multiple Greek Letter (MGL) approach the alpha-factor approach, the beta-factor approach with a number or variants. Other often used approaches are impact vector (and alike) and for high redundancies common load model. In Germany, a new method, the “coupling model” has been developed. It is a binomial failure rate approach that has been modified to take better account of the high levels of redundancy incorporated in the safety systems. The Unified Partial Beta Factor Method (UPM) is a completely different approach concentrating on defences against CCFs.

The Human Reliability Analysis (HRA) carried out as part of the PSA typically addresses: human errors leading to the unavailability of a standby safety system; human errors that can lead to an initiating event; and human errors of omission in responding to an initiating event that has occurred.

There are a number of methods used for the identification and quantification of human errors. These include the traditional methods such as the Technique for Human Error Rate Prediction (THERP) which is still widely used. In addition, other methods such as MERMOS and the Human Error Assessment and Reduction Technique (HEART)/ Nuclear Action Reliability Assessment (NARA) have been developed and are used in particular countries.

All the PSA have included human errors of omission. Some of them have also included errors of commission or, in some cases, a partial analysis has been carried out. This is seen as a difficulty or limitation of many of the PSAs that have been produced.

The overall trend is to use plant specific data whenever possible and systems for plant data collection have been set up in many countries. However, some of the PSA in existence still use generic data, or generic data that has been supplemented by plant specific data for the risk significant initiating events or component failures.

A two stage Bayesian approach is generally used to revise the data. This generally uses generic or old data for the prior distribution which is updated using the new or plant specific data.

A number of PSA codes are in use for the quantification of the PSA including RiskSpectrum, WinNUPRA and CAFTA. New codes have been developed in Finland (FINNPSA) and in KOREA (FTREX). As well as being able to solve very large fault trees, the latter software is also able to resolve circular logic in the tree.

There are two issues raised by many respondents/PSA studies: 1) the need for the PSA to model shared systems (has been done in some PSAs but not in others) and 2) the lack of models for taking software reliability and organisational factors/ safety culture into account.

Some countries have made the recommendation that the PSA should be carried out by station staff or they should be heavily involved in carrying out the PSA. This ensures that the station staff is familiar with the PSA so that it can be used routinely for a wide range of applications during station operation.

6.2 Country replies

6.2.1 USA

Current licensee and NRC PSA models for operating nuclear power plants in the U.S. use the classical PSA framework first established by WASH-1400. This involves an event tree/fault tree analysis for Level 1 PSA, a containment (or accident progression) event tree analysis for Level 2 PSA, and, for those plants having a Level 3 analysis, a simulation-based accident consequence analysis for Level 3 PSA.

All U.S. operating plants have Level 1 and Level 2 PSA models for internal events (including internal flooding events) occurring during full power operation. As discussed in section 5.2.1, many of these models were created in response to GL 88-20. The NRC has also developed Level 1 PSA models for all plants under the Standardized Plant Analysis Risk (SPAR) program and is in the process of benchmarking these models against licensee PSAs. All operating plants also have external event and internal fire vulnerability assessment models developed in response to Supplement 4 to GL 88-20. Some of these latter models were developed using methods specifically aimed at identifying potential vulnerabilities (e.g., the Seismic Margins Assessment – SMA – and the Fire Induced Vulnerability Evaluation – FIVE – method), while others were developed using risk assessment methods. A small number of plants have models for events occurring during low power and shutdown (LP/SD) conditions.

The specific scope, methods, and level of detail of these models vary. The variation is greater for external events, internal fires, and accident progression (containment performance) analyses than for Level 1 internal events PSA. As discussed in section 4.2.1, a number of consensus standards have been developed or are being developed to help ensure consistency in the quality, scope, methodology, and data used in PSA analyses intended to support risk-informed decision making. As discussed in section 9.2.1, a number of activities are also underway to improve current methods, tools, and data.

The approaches used for a number of PSA topics of interest can be summarized as follows.

<u>Common Cause Failure</u>: PSA models incorporate explicit causal models for many sources of dependence (e.g., equipment functional requirements, equipment support requirements, cascading failure effects, common equipment environment) between failure events. As described in

NUREG/CR-5485, Common Cause Failure (CCF) analysis generally involves a parametric assessment of residual dependencies, i.e., dependent failures whose root causes are not explicitly modeled in the PSA In current U.S. PSAs, these CCF analyses employ either the beta factor, multiple Greek letter (MGL), or alpha factor methods for representing and quantifying CCF events. For example, NRC's SPAR models use the alpha factor method, where the alpha factors are quantified using data from the NRC's common cause failure database.

Human Reliability Analysis: Human Reliability Analysis (HRA) involves the identification, modeling and quantification of potentially significant human failure events (HFEs). In general, the HFEs of interest may result in an initiating event or may impact the mitigation of an initiating event. The HFEs affecting mitigation may occur before or after the initiating event.

The state of HRA as applied in current U.S. PSAs is generally as discussed in NUREG-1560. The analyses range from highly-simplified approaches judged acceptable for vulnerability assessments (but not necessarily for other risk-informed applications) to detailed scenario-specific analyses reflecting the best-available information on the causes and likelihood of human error. For the more detailed HRAs, considerable effort is spent on identifying HFEs. As described in NUREG-1792, such detailed analyses can require a multi-disciplinary effort involving extensive interactions between the HRA analysts and other domain experts (e.g., PSA analysts responsible for developing the event tree models, human factors specialists, thermal-hydraulics analysts, and personnel knowledgeable of plant operations and training). These interactions should result in an HRA model that accurately reflects the plant's current design and operating practices. In addition, they should provide important feedback to the PSA model, supporting the development of event sequence models that better reflect the role of plant operators during an accident.

Several methods are available to model and quantify HFEs. In the IPEs, the most widely used methods identified by NUREG-1560 are: the failure likelihood index methodology (a modified version of the success likelihood index methodology – SLIM), the cause-based decision tree (CBDT) method, the human cognitive reliability (HCR) method and the operator-reliability experiments (ORE)-based modification of HCR, the operator reliability characterization and assessment method, the technique for human error prediction (THERP) method and the related accident sequence evaluation program (ASEP) HRA method, and the Individual Plant Examination Partnership (IPEP) method, also a modified version of THERP. These methods employ different approaches to the identification and treatment of factors affecting human performance.

Recent U.S. methods and tool developments include the assembly of a number of these approaches within the Electric Power Research Institute (EPRI) HRA calculator, the development of the SPAR-H method (an offshoot of the THERP and ASEP methods) used in NRC's SPAR models, and the development and limited application of the ATHEANA method. To support the application of these methods, the NRC has developed a summary of HRA good practices, documented in NUREG-1792, and is in the process of documenting work involving the testing of a selected group of methods against these good practices. Also, as described in Section 9.2.1, efforts are underway to collect and analyze empirical data (both operational and experimental) needed to improve confidence in the modeling and quantification of HFEs.

Other Basic Event Data: Most U.S. PSAs use generic and plant-specific data to estimate initiating event frequencies, equipment failure probabilities, and equipment unavailabilities due to testing and maintenance. Some PSAs (including NRC's SPAR models) only use generic data. NRC is currently developing a revised set of generic distributions for SPAR model parameters based on recent U.S. operational data collected from a variety of sources, including the Institute for Nuclear Power Operations' (INPO) Equipment Performance Information Exchange (EPIX) system, the NRC's Initiating Events Database, and the NRC's Reactor Oversight Program. The estimation process uses methods described in NUREG/CR-6823, including adjusted Empirical Bayes' methods for addressing plant-to-plant variability, and constrained non-informative distributions to represent diffuse knowledge.

Characterization of Results: Most current PSAs use a combination of methods to characterize important contributors to risk, including the identification of important event tree sequences, important cutsets, and important basic events. In the case of sequences and cutsets, importance can be indicated in terms of absolute risk, relative risk, and risk ranking. In the case of basic events, importance can be indicated using a variety of standard importance measures, including the Fussell-Vesely (FV) measure, the Risk Achievement Worth (RAW) measure, and the Birnbaum measure. The FV and RAW importance measures are currently being used to identify classes of components requiring special treatment, as defined under 10 CFR 50.69, "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors." The Birnbaum measure is being used in the recently developed Mitigative Systems Performance Index (MSPI), which is one of the plant performance indicators being used in NRC's Reactor Oversight Program.

6.2.2 United Kingdom

There are no UK specific PSA standard or guidelines and hence there are no prescribed PSA methodologies. The current raft of UK PSAs have been developed based on that international best practise which each licencee considers to be fit for purpose for their particular reactor design.

Overall PSA methodology: In general the UK PSAs have been developed in compliance with the IAEA Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants, Levels 1, 2 and 3. In addition IAEA guidance on Framework for QA Programme (TECDOC 1101), Living PSA (TECDOC 1106), Regulatory Review of PSA Level 1 (TECDOC 1135), PSA for Low Power & Shutdown Modes (TECDOC 1144) and Applications of PSA (TECDOC 1200) are adhered to. Whilst the scope of each PSA varies, all Level 1 PSAs employ small event trees/ large fault trees and consider all internal faults and relevant external hazards; for example, the Sizewell B Level 1 PSA considers quantitatively 170 Initiating Internal Faults and 6 Hazards (Seismic, Extreme Wind, Flooding, Fire, Aircraft Crash and Turbine Disintegration.)

For Level 2 PSA the methods used are more variable although all employ thermal hydraulic analyses and source term analyses to varying extents. Again using the Sizewell B Level 2 PSA as an example, the phenomenological event trees consider steam explosions, hydrogen burns, direct containment heating, debris coolability, molten core coolant interaction, natural circulation induced reactor coolant system failures, etc. With the thermal hydraulic and source term analyses being performed using MAAP 3B.

Common cause failure: In UK PSAs common cause failure (CCF) probabilities are calculated using a method based on the beta factor approach, known as the Unified Partial Beta Factor Method (UPM). The UPM is based on structured expert judgment for a broad and complete range of important influence and conditioning factors regarding CCF events. In addition to the UPM approach, common cause failure is limited in the reliability that can be claimed for a safety system that incorporates redundancy only. This limit is generally in the range 10^{-3} to 10^{-5} failures per demand and a value of 10^{-4} failures per demand is chosen for design purposes for active safety systems, such as pumping systems.

Human reliability: In UK PSAs, the principal tool used to quantify the reliabilities of human interactions has been the Human Error Assessment and Reduction Technique (HEART). Established in the late 1980's, although it has had some minor modifications, it has remained principally the same technique, based on the same original data. An internal industry review of the application of HEART usage in nuclear PSAs revealed some shortcomings of the technique; in particular that HEART does not always 'fit' very well with the NPP tasks being assessed. Since 1992, a human error probability (HEP) database called CORE-DATA (Computerised Operator Reliability and Error Database) has been under development in the UK, and it was considered that a new tool should be developed along the same lines as HEART, but based on the more recent and relevant data, and more tailored to the needs of UK nuclear power plant PSAs and HRAs. This has led to the development of a nuclear power plant specific HRA approach called NARA (Nuclear Action Reliability Assessment). The

NARA development project is now nearing completion. Within the last year (2005) it has been the subject of a NII sponsored peer review which raised various issues for further consideration. These issues have now been addressed. British Energy are awaiting formal acceptance by the NII of NARA as an appropriate human error quantification technique. Meanwhile some outstanding tasks are being finalised, and workshops are being set up to disseminate the NARA methodology to potential users.

Availability assumptions: For the Magnox and AGR PSAs the models considered that all plant is available i.e. no allowance is made for plant potentially out on maintenance. Similarly, no allowance has been made for the repair of plant which fails to start or run; repair of failed items as part of mitigation or recovery actions are also not considered. The latter AGR PSR PSA models were later amended to allow for average maintenance considerations. The Torness and Heysham 2 PSA models have been updated to allow plant items to be taken out for maintenance by means of 'house' events; these models are now used for risk monitoring. The Sizewell B PWR PSA model have always allowed for average maintenance.

Multiple cores: In the UK, the Magnox and AGR stations each have two identical reactor cores, each with their own independent essential systems and balance of plant. The PSA model considers only one unit, in general no account is taken of support available from the adjacent functional reactor (such as electrical supplies, feedwater supplies, etc), and in this regard the PSA can be considered as conservative. The risk from the station is assumed to be twice that of a single core

6.2.3 Taiwan

For level 1 PSA, the small event tree/large fault tree methodology is used. Current state-of-the-art methodology and PRA procedures guide from NUREG/CR-2300 was adopted when categorizing initiating events, developing event trees and fault trees, and quantifying accident sequences. The LERF evaluation was based on the methodology suggested in NUREG/CR-6595. Level 1 model and LERF evaluation model are developed and quantified with the WinNUPRA code.

The CCF modelling is based on the Multiple Greek Letter model and adopts generic CCF-parameter data in NUREG/CR-5497.

For human reliabilities, pre-initiating-event as well as post-initiating-event human errors are modeled. Maintenance and test induced human errors are included in pre-initiating-event human reliability analysis. HCR model is used to quantify the human error probabilities of cognitive part. The available time and execution time is defined from both the interview with operating crew and the thermal-hydraulic calculations. THERP methodology is used to quantify the human error probabilities of execution part. The parameters required are also defined from the interview with operating crew. Dependency between human actions is defined by reviewing the emergency operating procedure and the organization of operating crew.

Generic data estimated in NUREG/CR-5750 and EGG-SSRE-8875 with plant specific data collected from 1994 to 2002 are used to estimate the initiating event frequencies and component failure probabilities. Generic data is updated by plant specific data using Bayesian update.

6.2.4 Switzerland

Overall Methodology: In Switzerland, the linked event tree as well as the linked fault tree methodology has been used for level 1 PSA. Both methods have been accepted.

The definition of plant damage states covers the various attributes important to the progression of severe accidents and containment response that are typically addressed through an event tree computational process. The number of nodal questions is by itself not an important determinant of the level 2 process or PSA quality, as long as the key severe accident progression and containment challenges are adequately considered. The same is the case for the release categories. Level 3 PSAs are not required by HSK, however, the regulatory PSA studies undertaken by HSK are considered as level 2+ since the risk of activity of release is calculated for the most risk-dominant radio-nuclides (i.e., about 60 nuclides).

Common Cause Failure: The accepted CCF parameter models are the Alpha Factor and the Multiple Greek Letter models. The determination of CCF parameters is, in general, based on plant-specific evidence and generic data. If for special components no such data is available, data may be based on expert judgement. International experience shall be applied in order to check the completeness of the considered component types susceptible to CCFs.

Human reliability analysis: Pre-initiator Human Errors (HEs) (category A actions), HEs causing initiating events (category B actions) as well as post-initiator HEs (category C actions) is expected to be considered in the PSA. Modelling of errors of commission is not currently required, due to limitations in the state-of-the-art. However, any significant errors of this type that are identified should be documented and countermeasures should be discussed.

Operator actions of Category C are primarily credited if the corresponding procedural guidance is available and operator training has included the actions as part of crew's training. A review of the operator training and plant operating procedures relevant to the specific operator response is performed. Acceptable quantification methods are SLIM (success likelihood index methodology) variants accepted by HSK, Technique for Human Error Rate Prediction (THERP), and the Accident Sequence Evaluation Program (ASEP). The assessment of HEPs is required to consider both the decision/diagnosis aspect and the execution aspect of the human actions modelled in the PSA

Dependency within a task (e.g., calibration and subsequent testing) and among tasks (e.g., for different trains of a system) is required to be examined and documented.

6.2.5 Sweden

The licensees do create or use existing method descriptions for the PSA level-1 and level-2 analysis to be performed. At lack of method descriptions for certain analysis, the matters are discussed e.g., in the Nordic PSA Group, in the Nordic BWR Owners Groups and new methods are commonly developed to save money and time.

A common approach in Sweden is to create small event trees and large fault trees. PSA code used at the licensees as well as the SKI, for the quantification PSA models is Risk Spectrum.

All plants have more or less completed studies for all operating modes (from full power to reactor shutdown for level 1 studies, and on good way also to be performed for level 2 studies). These studies are also complemented with the area analysis (fire, flooding) and the external events studies.

MAAP and MELCOR codes are used in the PSA framework, to support the accident sequence analyses.

Overall methodology: The main aspects of the overall methodology applied in Sweden are as follows:

Level 1 PSA: methods for creation and development of event trees, fault trees are according to national standard.

- o Often referred international PSA standards are followed, e.g., IAEA guides, EU PSA guide, also American guides are referred to. In e.g., the US and UK presentations in above, lot of these guides are already mentioned.

Level 2 PSA: methods for creation and development of plant damage states and how they have been defined, the containment event trees, etc. exist.

- It is very common in the Swedish level-2 studies, that a reference is found to the methodology given in the NUREG-1150.

Domestic level-1 and level-2 studies are nowadays integrated with each other. This means that the Boolean link exists and correct cut-sets from level-1 are also considered in the level-2 studies.

Level 3 PSA: in Sweden no level-3 studies are required. Anyhow, some plants have done pilot applications.

Common cause failure: Method descriptions do exist at all licensees on how CCFs have to treated, covered in the PSA models. CCF:s are treated in the Sweish PSA:s between components in redundant systems. A common CCF-model used in Sweden is the alfa-factor method in low redundant systems. CCF-modell used in high redundant system is the HiDep common load model.

Sweden do participate in the international OECD/ICDE project, to be able to get accessto as wide and QA dependency and CCF data as possible.

Human reliability: Method descriptions exists at all plants, on how to work with the modelling and quantification of human errors in the PSAs. HE analysis in Sweden cover the main control room personnel activities. HE due to e.g., maintenance errors are most often a part of the frequency given for individual basic events on components. The Human Reliability Analysis (HRA) carried in the PSA do often addresses: HE:s that can lead to faulty system configuaration, to the unavailability of a standby safety system, to an initiating event, to errors of omission. The common method widely used is the Technique for Human Error Rate Prediction (THERP), also the accident sequence evaluation program (ASEP). Discussions are now held on how to incorporate and follow the HE analysis needs and good practices, given in the NUREG-1792.

PSA component data: The overall approach is to use plant specific data whenever available. Plant specific data are also complemented with other international data as generic data, when the own operating experience data is too scarce. The safety related component data handbook, the T-Book - Reliability Data of Components in Nordic Nuclear Power Plants. The T-book is regularly updated about every new 50-60 reactor year, most often due to the need of new data for PSA updates and to keep the update expenditures on defendable levels.
The most resent edition is - T-Book 6th version. The T-Book can be ordered from: The TUD office, SwedPower AB, Energy Technology, PO Box 527, SE-16216 Stockholm, Sweden: Phone: +46 8 7397320

PSA initiating event data: Initiating events data are nowadays updated by the plants them selves at the time of each PSA update, this process includes also an analysis and grouping of all the occurred transients and other initiating events, to be modelled in the PSA.

PSA results evaluations: In most of the PSA:s the behaviour of important contributors to risk, the dominating event tree sequences, dominating cut-sets, as well as dominating basic events and basic event groups and parameter values are presented in the results presentation. Importance measures are commonly estimated by using the Fussell-Vesely (FV) measure, the Risk Achievement Worth (RAW) measure.

A PSA study that a licensee sends to the SKI has to be independently reviewed and a documented statement of results of this process have also to follow with this delivery.

Status of the Swedish PSA:s are also considered as a part of the SAR of the plant. In the SAR the PSA results have to be summed up and explained and references must be given the latest and valid PSA documentation.

6.2.6 Spain

Most of the utilities performed the PSA in-house according to state of the art methodologies. The PSA studies have been very detailed and as consequence considerable amount of resources were consumed.

Initiating events

Usually generic data are used, however the operating experience is analyzed and incorporated in the updated PSA by means of using specific transient data when available or specific simplified fault tree for support system failures.

Sequence and System modelling

All PSA used the typical small event tree – large fault tree technique.

Dependencies

Dependencies have been taken into account designing matrices of dependencies and developing fault trees in a very detailed level.

Common cause failures

Quantification is performed using parametric methods. For CCF basics events of two redundancies an acceptable method is to use the factor beta. For more than two redundancies the alpha factor or multiple Greek letter (MGL) method is used.

Collection and analysis of reliability data

The IP included the requirement to design a Data Base to be used in the Spanish PSA. This Data Base was part of the program DACNE and should include specific information related to the components (BDC) and operating experience (BDIO). Also the requirement includes the maintenance and updating of this Data Base.

Objectives of the BDC is the classification of the components by design and operation, definition of codification for plants, systems and components, failure modes, etc. The information included are general data, description, report on the events.

The objectives of the BDIO are to determine the operating experience root cause, and to group the events and transients.

Special impact on updating of the PSA has the incorporations of the operating experience affecting to the initiating events and the components modelled in the PSA. The operating experience is analysed and the initiating events and the failures of components and their associated unavailability identified. Also the unavailability due to test and correctives are analyzed. Maintenance and test policy are considered in order to estimate their associated unavailability. For initiating events and component failures when the plant experience is statistic significant direct estimation is performed and when limited experience exists Bayesian treatment is carried out with the generic data. Criteria for analysis of the component failures are standard for all the plants and are defined in the Spanish Component Data Base (BDC).

Thermal-hydraulic calculations

Thermal-hydraulic calculations have been used for the estimation of success criteria and available times. These were performed for representative sequences in an event tree and these values have been used for the remaining of the sequences. In special cases more thermal-hydraulic calculations were needed for estimating available times. MAAP and RELAP were the codes used. For the level 2 the CSN independent review used MELCOR. Most of the calculations performed by the utilities were running for 24 hours, however in the level 2 the independent review performed by CSN made MELCOR calculations for at least 48 hours.

Analysis of human errors

For human reliability, as well pre- as post- initiating event human errors are modelled, by using a methodology that is largely based on SHARP and using mainly THERP, HCR and TRC quantification techniques. Test and maintenance activities are covered in the pre-initiating event human reliability analysis. Human errors in dealing with Emergency Operating Procedures are considered for post-initiating event human errors. Recovery actions are also taken into account. Errors of commission are included to some extent.

Model quantifications

The computer codes used by the licensees for the quantifications of the PSA are CAFTA and Risk Spectrum. The CSN receives the models of the updated PSA and use for their own quantification the Risk Spectrum code. Models received from CAFTA are converted to the Risk Spectrum platform. CSN benchmark and reviews the updated models and performs own calculations for evaluating the external applications submitted by the utilities and for own proposals, for instance for supporting the CSN PSA information System and for verification of the PSA performed by the utilities, and also for the categorizations of the inspections findings.

Level 2 PSA

For the level 2 utilities groups core damage accident sequences in Plant Damage States using around 10 or 12 attributes. Containment Event tree (CET) approach has been used developing decomposition trees for considering accident progression of severe accident events. CET End States are grouped in Release Categories for later estimation of the Source Term according to magnitude and time of the releases.

CSN has performed independent review of the Level 2 using was called Level 2+, i.e.: the APET methodology has been used similar as those performed in the NUREG-1150. Containment failure modes and release categories has been compared with those calculated by the utilities. Others results from the review are the activities of the releases categories, and additionally the impact of different Severe Accident Management (SAM) strategies has been evaluated.

Low Power and Shutdown

Low Power and Shutdown analysis have been performed for all Spanish plants. The CSN is still evaluating part of these analyses.

Operational modes during shutdown were subdivided in Plant Operational States taking into account operational conditions and technical requirements. In general in the LPSD studies around 13 Plant Operational States were considered.

6.2.7 Slovenia

Overall methodology

The methodology for the Krško NPP PSA level 1 is consistent with the US NRC NUREG/CR-2300. An event tree (ET) is developed for each initiating event and is used to identify accident sequences leading to core melt. These accident sequences are grouped for each initiating event category and linked together by fault tree (FT) linking. Fault trees are developed to evaluate the failure probability of frontline and support systems. System fault trees are developed to the component or basic fault level and include common cause faults, human error, and test and maintenance unavailabilities.

The Krško NPP PSA level 2 objectives are specified in US NRC Generic letter 88-20. The results of level 1 system analysis, in the form of grouped accident sequences leading to core damage, are taken into level 2 analyses. Level 2 evaluates the consequences of the severe accidents in terms of the plant’s and particularly the containment’s response.

Initiating event selection

A complete list of unique initiating events was identified and appropriate initiating event frequency for each event was determined. The Logic Diagram for internal initiators was developed to systematically categorize all "internal" initiating events on the basis of similar transient progression or consequences. Next, the initiating event categories were grouped into three categories, LOCAs, transients and special initiating events. LOCAs include all accidents that result in a reduction of primary coolant system water inventory. The category was divided into three subcategories: leak to the secondary system (SGTR), leak that bypasses the containment (interfacing system LOCA), and leaks within the containment (which was further subdivided based on the size of the break). In order to determine the specific events modelled for the transients and special initiating events, the Krško's systems were reviewed to determine if the failure of the system could result in a reactor trip, the Krško's operational data were reviewed and compared to similar plants, and the initiators provided in NUREG/CR-3862 were reviewed for applicability. The transient initiators were than grouped into categories based on plant response, signal actuation, systems required for mitigation, and subsequent plant related effects.

Common Cause Failure (CCF)

In the Krško NPP IPE PSA the failures of equipment due to common causes were represented in the fault trees explicitly by means of basic events. Two types of modelling of CCFs were distinguished:

- The modelling of CCF of two components in IPE PSA was done in a way to define separate basic events for each group of two components susceptible to CCF. For quantification of CCF of two components beta-method was used and a representative basic event was quantified accordingly.
- The CCF of more than two components were all included into a single basic event, which represented a system-level failure and was included into the top logic of a fault tree of system of concern. The Multiple Greek Letter (MGL) method was used for quantifying the frequency or the probability of occurrence of CCF.

In order to facilitate the Krško NPP Living PSA, re-modelling of the existing CCF representation in the Krško NPP baseline PSA was performed by employing (RiskSpectrum) built-in CCF modelling capabilities. The focus of the work done was on re-modelling CCFs involving two components. For each two-component CCFs the components to which CCF basic event relates were determined. Respective individual failure basic events were determined. Individual failure basic events identified were sorted into RS CCF groups. Re-modelling was performed. Existing CCF basic events were removed from a FT structure, together with associated parameters and notes describing them. New RS parameters representing beta-factors were defined and appropriate notes were added in a RS model. New CCF groups were defined instead using beta factors from the Krško NPP IPE CCF Notebook.

Human Reliability Analysis (HRA)

The HRA was based on the THERP (Technique for Human Error Rate Prediction) methodology described in the NUREG/CR 1278 and Westinghouse RMOI HRA Guidelines. The HRA consists of delineating the procedural steps which are absolutely necessary for successfully completing the task for a given event, modelling the task in failure configuration, and deducing the probability that the operating crew will fail to complete the task.

Data analysis and Master Data Bank

Plant data are collected, organized, and reduced in order to generate the types of quantification data (initiating event frequencies, system unavailabilities, component unavailabilities, test and maintenance unavailabilities).

The primary sources of data are the records kept by the Krško NPP. An organized effort is preformed in developing a plant specific data base that accurately represents the reliability of equipment and systems. Main sources from which the plant specific raw data comes are plant procedures, work requests, operator's log book, results of surveillance testing, reports on operating events and trip data base lists. In case where the plant records are not available or their quality is questionable, generic data sources are used.

Low power and Shutdown PSA

The Krško Probabilistic Shutdown Safety Assessment (PSSA) initiating events are defined by faults that impact the primary safety functions. However, only faults challenging continued RHR system operation are included in the PSSA model. The safety functions are supported by front-line fluid systems backed up by vital safety support systems such as Essential Service Water (ESW), Component Cooling Water (CCW) and AC power. Failure of these functions could lead to one or more of the following undesirable end states: core damage, reactor coolant system (RCS) boiling, spent fuel pool boiling, cold overpressurization of the reactor pressure vessel (RPV), unplanned reactivity insertions (prompt criticality), exposure of a fuel bundle in transit, and unfiltered radionuclide release from the fuel.

Given that the principal safety function during shutdown involves the operation of the residual heat removal system to provide core cooling, maintain reactor fuel integrity, and participate in chemistry control, the primary concern of the PSSA initiating events is RHR system operation and recovery of its failure. The loss of the RHR system function can occur for the following general reasons:

- Mechanical failure of RHR system components (the running pump),
- Loss of RCS level causing loss of the RHR system suction or draindown through the RHR system itself (i.e., Rapid Draindown or Small Leak Event),
- Loss of offsite power, and
- Loss of support system function (e.g., the supporting AC bus to the RHR pump or CCW supply to the RHR heat exchanger and pump).

Grouping of initiators is the second step in the initiation event selection. Considering the reasons listed above, the possible initiating events during shutdown are generally defined by the following groups:

- Loss of residual heat removal (RHR) events,
- Loss of coolant accidents (Rapid Draindowns & Small Leaks),
- Loss of offsite power (LOOP) events

The event tree structures in the PSSA are developed based on the Krško shutdown operational procedures. At least one event tree (represented by a Group Variable) exists for each initiating event modelled in the Krško PSSA. Although each initiating event is treated separately, the mitigative responses are similar among many of the initiators, which in turn, create similar event tree structures.

6.2.8 Slovak Republic

Overall methodology: Level 1 and level 2 full power PSA and low power and shutdown PSA are performed or being performed for the Slovak NPPs. The overall methodology is based on IAEA procedures for conducting PSA (Level 1 and Level 2 PSA: Safety Series No. 50-P-4 Safety Series No. 50-P-8). In addition, the NUREG procedures are used (NUREG/CR-4550, NUREG/CR-2300, etc.).

Initiating events: The primary source for the generic initiating events was IAEA-TECDOC 749. This report presents a list of the initiators for full power operation of VVER 440 type units which was agreed upon by all VVER operators. In addition, this list was compared with the standard list of the initiators for PWRs. Combination of a various methods was used in the identification of the initiating events for the shutdown PSA. The main elements of this approach were: references to previous western PSAs, analysis of the operating experience of the plant, and engineering evaluation of the plant.

Accident sequence modelling: The plant responses to the initiating events were described using the event trees. Small event trees and large fault trees were constructed in The RISK SPECTRUM PSA code. The trees represent accident sequences, consisting of an initiating event and a combination of various system successes and failures that lead to a given consequence. Because the plant has been studied thoroughly, functional event trees were not developed. The states of the systems are defined in the event trees using the fault tree top events, which provided the interface between the event trees and the system fault trees. The purpose of the event trees from a risk modelling perspective was to identify all accident sequences for the initiating events. The initiating events, which have the same accident sequences, e.g. the same demands upon the safety systems, were grouped and the final event trees were constructed for the groups. The event tree development involved definition of the system success criteria. In general, the success criteria were based on the plant past PSA studies and the available transient analysis. Where such analyses are not available, the unit FSAR was used and as such was conservative with respect to the general PSA modelling requirements.

System analyses: Fault trees were used to model the front-line and support system failures. In this activity, system descriptions were developed which contained all relevant information. The information in the system descriptions was verified by the plant personnel. Failures in the support systems were modelled in PSA through the linking of the appropriate portions of the support system fault trees in the front-line system fault trees. Fault trees were developed to the detailed level. In addition to the component failure actuation signals, the electric power supply and the component cooling failures were modelled. For a better orientation in the model also highly reliable components, such as the tanks, were included in the fault trees. Development of system models also provided information about the potential initiating events resulting from the failure within the systems. If the system could be shown to be relatively unimportant, simplified fault trees were constructed. If the system was considered important detailed modelling effort was undertaken. The dependent failures were included in the fault trees through the integration of the front-line and support system models (functional hardware dependencies) and inclusion of common cause events.

Data analyses: There are three basic categories of data used in the PSA: plant specific data, data of the manufacturers supplying new equipment within the reconstruction of the plant and generic data. Plant specific data refers to the component failure rates, test intervals, maintenance duration time and initiating event frequencies based on the operating history of the plant modelled by PSA. For the new components implemented during the reconstruction data provided by the manufacturers has been used. Generic data is used in all cases where plant specific data and data from manufacturers were not available.

Common cause failures: The common cause failure probabilities were estimated using the Alfa factor models.

Human reliability analysis: Three types of human errors are typically included in the model. They are pre-accident human errors, connected with the maintenance and test during the normal operation of the reactor, post-accident operator failures and man induced initiating events, typical for shutdown operating modes. The THERP and TRC methodologies were used to calculate the human error probabilities. Detailed analyses are performed for all man-induced initiating events, pre-accident and post-accident human errors. In case of post-accident human errors the dependencies are implemented into the PSA model.

External events: Internal fire analysis, internal floods and external hazards are implemented into the model. The objective of the analyses was to assess the potential contribution of these external events to the overall core damage frequency. The fire risk analyses was performed on the basis of the IAEA guidelines: IAEA-Safety report series No 10 - Treatment of internal fires in PSA for NPPs. The flood analyses examined internally initiated floods consistent with the methods specified in NUREG/CR-2300, Vol.2. Impact of the air craft crash, extremely low temperatures and neighbouring industry on the total CDF was calculated within the external hazard analysis.

Quantification and interpretation of the results: Within this task the PSA model is analysed, the dominant accident sequences and their minimal cut sets are identified and the core damage frequency is calculated. Also the importance and sensitivity analyses are performed for the initiating events, component failures and human interactions from the risk point of view. Uncertainties are also handled. The main motivation for performing uncertainty analyses is to obtain reasonable upper and lower bound estimates for the CDF.

Level 2 PSA: Full power and shutdown level 2 PSA is developed for the Bohunice V1 and V2 NPP. At the present time the level 2 PSA is being developed for the Mochovce NPP. The objectives are the following: 1) to identify the ways in which radioactive releases from the plant can occur following the core damage, 2) to calculate the magnitudes and frequency of the release, 3) to provide insights into the plant behaviour during a severe accident, 4) to provide a framework for understanding containment failure modes, the impact of the phenomena that could occur during and following core damage and have the potential to challenge the integrity of the containment, 5) to support the severe accident management and development of guidelines. The level 2 PSA model of the J. Bohunice V1 NPP was developed in the RISK SPECTRUM Professional code. This model calculates the frequency of the individual release categories generating minimal cut sets which involve the initiating event of the accident, component failures of the safety systems and human errors. The magnitudes of release categories are calculated using the deterministic codes for the accident modelling: the MAAP4/VVER code was used for reactor operation and shutdown mode with closed reactor vessel and the MELCOR code for shutdown mode with open reactor vessel.

Supporting TH analyses and source term analyses: MAAP, RELAP and MELCOR codes are used to support the level 1 and level 2 PSA modelling.

6.2.9 Netherlands

Borssele: For the level 1 PSA, the methodology is current state-of-the art methodology. The small event tree – large fault tree methodology (using fault tree linking) is used. The models are managed with the NUPRA code.

For the initiating event identification master logic diagrams were developed, a systematic safety parameter review was conducted, the system loads from all support systems were reviewed, operation experience and plant specific data was screened and other PSAs were reviewed

For the failure data plant specific data are used. Each year the data set is updated via Baysian updating.

The CCF-modelling is based on the alpha-factor model and uses both generic CCF-parameter data and data from the International Common Cause Failure Data Exchange Project (ICDE) via the German power plant owners organisation VGB. Special attention was given to the common cause factors for the two testing strategies (sequential testing and staggered testing)

For human reliability pre-initiating and initiating errors are modelled within the SHARP framework via THERP. Originally, the post-initiator errors were modelled via HCR/ORE. This was recently revised by the Cause Based Decision Tree (CBDT). A special assessment was made regarding the so-called errors of commission via an ATHEANA like method. Special attention was given to the dependencies in the human factors associated with the two testing strategies (sequential testing and staggered testing).

For the Borssele NPP 111, plant damage states were identified, with each PDS characterized with 8 attributes. Containment event trees were developed for all 111 PDSs. For evaluation of all branching points Decomposition Event Trees (DETs) were developed to determine the likelihood of each branch occurrence.

For the Source Term calculations both MELCOR and MAAP 4 were used.

The level-3 assessment was carried out via the COSYMA code.

Dodewaard: For the level 1 PSA, the overall methodology is still current state-of-the art methodology, although some constituent parts, such as the use of TRC for HRA, are nowadays debatable. The small event tree – large fault tree methodology (using fault tree linking) is used. The models are managed with the CAFTA code.

The CCF modelling was done via the beta-factor method.

The post-initiating human errors were modelled via the Time Reliability Curves (TRC)

The assessment of seismic events was modelled in large detail with floor response spectra for each floor, fragility curves for all components, systems and structures. Besides flooding was steam flooding assessed separately.

Also for Dodewaard a large number of CETs, APETs and DETs were modelled.

Also for Dodewaard the level-3 assessment was carried out via COSYMA.

HFR: For the assessment of the level-1 risks the same method was used as for power reactors; small event trees and large fault trees. The models were managed with the CAFTA code.

Generic data were used (e.g., T book for instrumentation)

For dependent failures the beta-factor method was used. The factors were taken from NUREG/CR-4780.

For the pre-initiator human actions ASEP and THERP was selected. For the post-initiator actions were modelled with TRC.

As a basis for the fire assessment IAEA Report Series No. 10, Treatment of internal fires in probabilistic safety assessment for nuclear power plants was selected.

For the level-2 part MELCOR was modified to handle Aluminium cladding and U.Al_x fuel (High Enriched Uranium) respectively U_3Si_2 fuel(Low Enriched Uranium).

6.2.10 Mexico

The methodology used for the front–end portion of the IPE, was based on the development of small events trees and large fault trees. The fault trees for the front line and support systems were developed on the level of detail of components like valves and its actuator, pumps with its motor, breakers, internals relays, initiation logic components, etc. The component fault was defined on the failure mode concept identifying the component fault statement (example, open failure valve). All models are handled with the CAFTA code. The CCF-modelling is based on the Multiple Greek Letter model. For human reliability, pre- and post-initiating-event human errors were modelled, taking into account only errors of omission, THERP and ASEP methodologies were used to model such human actions. Failure data obtained from the maintenance rule program have been incorporated. The human actions were modeled using the THERP methodology,

The interface between level 1 and 2 was made by grouping the accident sequences that have been identified to lead the core damage into Plant Damage States (PDS), considering the availability of the systems to mitigate the source term releases. The utility used a matrix approach to establish the status of reactor vessel, containment and emergency systems at the onset of core damage. The grouping of important characteristic results in the definition of 10 PDS. The criterion used to consider minimal cut sets to be grouped in a PDS assures at least 90% of CDF.

The small Containment Event Tree method described in the NSAC-159 was selected by the utility to develop the Level 2 of the IPE. Nine Plant Damage States (PDS) were defined by binning the Level 1 PSA end states and were assessed in an equal number of CETs developed for the accident progression analysis. The CET top head includes: the status of the vessel pressure, the coolant recovery, the vessel failure modes, early and late containment failure, the early and late suppression pool scrubbing, the core concrete interaction and the fission product retention. The main phenomenological aspect such as in and ex-vessel steam explosion, direct containment heating (DCH), high pressure melt ejection (HPME), system availability and human error were modelled by approximately 160 fault tree models. The quantification process was performed by means of the computer code CAFTA and MAAP was used to support the development of the CET´s.

For the regulatory authority PSA level 1, systemic event trees were developed for each initiating event depicting the possible plant response to the initiating event and solving the core vulnerable sequences**.** Fault trees for front line and support systems were developed at the same level of detail than the IPE, and the models are handled with the SHAPIRE code. The NUREG-1150 methodology was used to perform the level 2 PSA. Therefore, an APET of 131 questions was developed to cover the 25 PDS defined based on the CNSNS level 1 PSA end states. More than 1000 accident progression paths were obtained from the APET. The questions included in the APET cover the main phenomenological aspect along with systems availability and operator interactions. The APET covers conditions before core damage (initiating event, vessel pressure, emergency systems conditions etc), containment conditions after and before vessel failure, mitigation systems availability, and phenomenology aspect such as hydrogen production, oxidation of zircalloy, core-concrete interaction, in-vessel and ex-vessel steam explosions. Containment failures modes such as rupture, leak or venting as well as their location were assessed in the APET for the different accident progression time frames. Examples of the APET questions are: Amount of the zirconium oxidized in the vessel pressure?, Is the molten material coolable?, What is the location of the primary containment failure?. The quantification process was performed by means of the computer code EVNTRE developed by Sandia National Laboratories and MELCOR code was used to support the APET development.

A parametric computer code called LVSOR, which is based on the XSOR type of codes, was developed for the source term estimation. LVSOR employs a parametric equation based on mass conservation that takes into account the phenomena and events related with the accident progression. Every parameter represents either a release or a decontamination factor and their figures are estimated based on MELCOR simulations.

A criterion based on the fraction of iodine and caesium released to the environment was used to assign each source term into a release category. The criterion takes into account the initial core inventory and the time at which the release begins. The source terms were classified in nine categories, according to the time of release: early (less than 6 hrs), intermediate (from 6 to 24 hrs) and late (more than 24 hrs), and the amount of radioactive material released: high, medium and low. The high release category was defined when more than 10% of Cs-I or an equivalent amount of radioactive material is released and capable to cause early deaths. The medium release category can cause health effects in a medium or short time with a release of 1 to 10% of Cs-I, while the low category is responsible only of potential of latent health effects with a release of less than 1% of Cs-I.

6.2.11 Korea

Overall methodology: The scope of most PSAs is limited to Level 2 PSA. Level 3 PSA is performed only as a part of research works. Level 1 PSA is based on the small event tree and large fault tree approaches, and it combined during the quantification stage. Since there are several types of reactors in Korea, the number of plant damage states (PDS) and nodes in the containment event tree are differently defined for each type of reactor. The general methodology of Level 2 PSA follows the methodology of NUREG-1150 of USNRC.

Common cause failure: The CCF is modelled based on the Alpha factor or Multiple Greek Letter methods and uses generic CCF parameter data at this moment. After joined the ICDE (International Common Cause Failure Data Exchange) project, we have considered the use of its data in PSAs.

Human reliability: According to the update program of all PSAs in Korea, human errors of those PSAs have been re-evaluated one by one using the ASEP- and THERP-based methodologies. Main focus of the HRA (human reliability analysis) update is to take operating experience into account for assessing human error probability. For human reliability, pre- and post-initiating human failure events are modeled in HRA. Test, maintenance and calibration activities are identified as pre-initiating human errors, and after initiating events recovery activities for failed pumps of safety systems are also covered in the HRA. Data used for the HRA are collected from the associated plants, including simulator, interviews, and walk through. Interdependencies between human failure events are also modeled and assessed using THERP equations for dependency analysis. However, errors of commission are not explicitly considered in the HRA. On the other hand, a standardized method has been developed to avoid high uncertainty of HRA caused by analysts' subjectivity by a joint research of KAERI, KOPEC and KINS. The method is designed to meet the quality requirement for capability category II of ASME PRA standard.

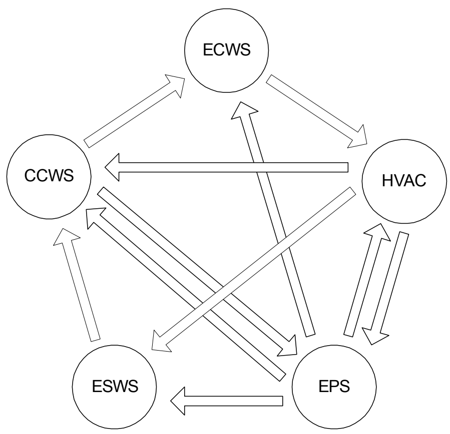
Initiating events: Unplanned plant transient data has been gathered from all commercial NPPs during April 1978 in which the first Kori 1 unit started its operation through the end of 2004. During this duration, about 500 plant events were gathered from all operating NPPs and the cumulative operating experience has been about 164 reactor operating years. After the data were collected each transient was reviewed and categorized to apply it to a PSA or other quantitative activities. In addition, in order to analyze the data, computer-based database program was developed to display information from the data collected. After the data were collected and inserted into the program, each transient was reviewed and analyzed.

Plant specific reliability database: As the number of operating years of Korean NPPs has increased, the necessity of the site-specific component reliability database has spread. KAERI has developed a domestic NPP component reliability database, KIND, that reflects the plant-specific characteristics of KSNP since 1998. The operation and failure/repair data for components for about 24 safety related systems of KSNPs have been collected, and analysed. KIND can provide the unavailability data, and 3 types of failure rates based on the component operating time, demand number, and plant operating time, respectively.

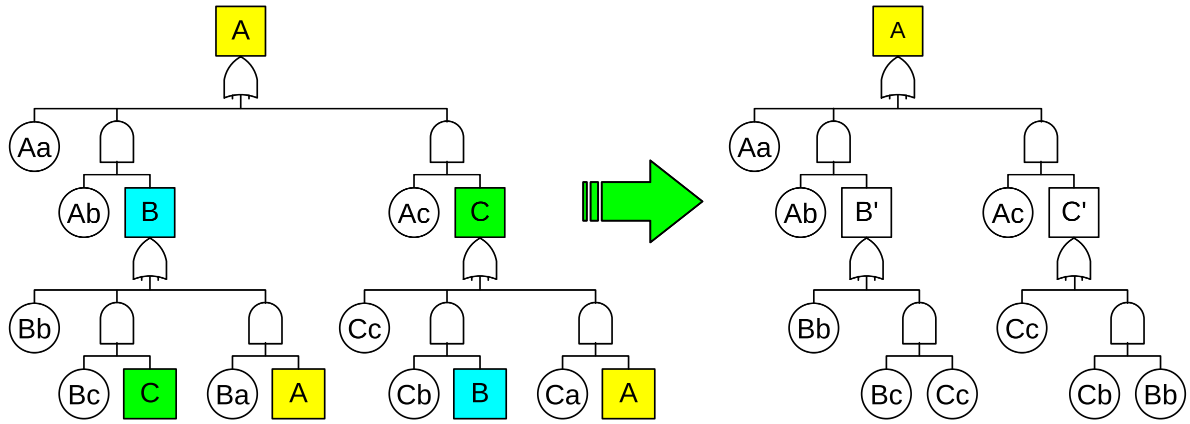
The failure rates of KIND are compared with those of generic database used for YGN 5&6 PSA. In the case of YGN 4, the result of the comparison shows that most of the failure rates of the KIND are lower than those of generic database. And 60% of compared failure rates show no big differences between KIND and the generic database. KIND may be used not only for PSA of new NPPs but also for PSR (Periodic Safety Review) and risk-informed applications being performed in Korea.

The cut set generator FTREX: A cut set generator based on the binary decision diagram (BDD) has been developed in other countries from the mid of 1990. But, it is not easy to solve big PSA models using the BDD algorithm. KAERI developed a coherent BDD algorithm to solve large fault trees, and developed a cut set generator FTREX [4]. The benchmark test performed by DS&S in USA shows that FTREX is 2 to 50 times faster than the cut set generators using the traditional algorithm.

Automatic solution of circular logic in a fault tree: A typical PSA has the circular logic in the fault tree model because circular relations exist among the systems. For example, as shown in Figure, the diesel generator supports the electrical power system and the electrical power system supports the cooling water system, which in turn supports the diesel generator.

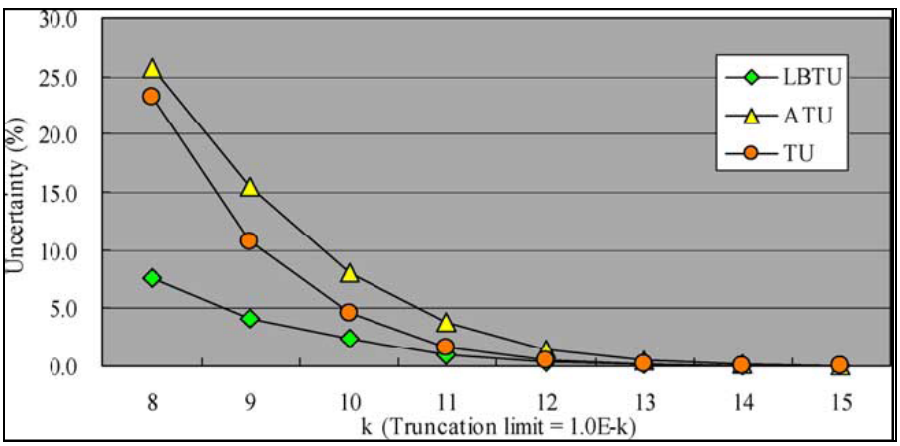


Many PSA analysts modify the fault tree manually to break the circular logic because most cut set generators can not solve a fault tree which has the circular logic. An algorithm to solve circular logics, as shown in figure below, was developed by Yang [5].



FTREX automatically convert a fault tree which has circular logics into a logically equivalent fault tree which has no circular logic.

<u>Truncation error in quantification of a fault tree</u>: The fault tree quantification uncertainty from the truncation error has been of great concern in the PSA. The truncation limit is used to truncate cut sets of the gates when generating minimal cut sets for the fault trees. The value of the truncated cut sets should be estimated to know the range of the exact value of a CDF. Measures to estimate the truncation uncertainty were developed. Using the measures, we can estimate the truncation uncertainty with one calculation of minimal cut sets at the given truncation limit. The algorithm is implemented in the cut set generator FTREX. The following figure shows the example of truncation uncertainty for the CDF where TU, LBTU, and ATU represent the Truncation Uncertainty, Lower Bound of Truncation Uncertainty, and Approximate Truncation Uncertainty, respectively [6].



<u>Other issues</u>: Many Korean NPPs share the Alternative AC (AAC) DG between several units. The effect of such arrangements is surveyed in a research projects. The results show that the conventional PSA overestimates the reliability of AAC DG [7].

6.2.12 Japan

<u>General description</u>: Although there are some variations among methodologies and data used in different organizations in Japan, general descriptions on current practices are publicly available in sources such as the NSRA standard and the draft of AESJ standard. Specific methodologies used in the PSAs by JNES are described in their PSA reports.

Generally, level 1 PSAs for internal events in Japan have been performed according to the NSRA procedure guide, which was made on the basis of NUREG/CR-2300. The AESJ standard would be used in the future.

Initiating events: Identification of IEs are made with combined use of : (a) results of preceding analyses including existing PSAs and EPRI list of transients in EPRI NP-2230, (b) master logic diagram analysis, (c) failure mode and effect analysis, (d) fault tree analysis. In order to minimize the overlooking of potential IEs, used for backup of above approaches are: (e) review of operating experiences in the analysed plant and other plants in Japan, (f) interviews with plant workers in operation, maintenance and safety management, and (g) insights from precursor analyses.

Frequencies of IEs which Japanese BWR and PWR have experienced, such as loss of PCS (Power Conversion System) and transients are estimated through the operating experiences. These can be estimated based on NUClear Information Archives (NUCIA). Frequencies for rare initiating events, such as LOCA, loss of CCWS and Interface System LOCA (ISLOCA), are derived through the system reliability analysis and the statistical approach. Frequency of small LOCA is estimated statistically assuming one small LOCA for Japanese and US operating experiences as 90 % upper limit in log-normal distribution with error factor of 10. Frequency of ISLOCA is estimated through the system reliability analysis considering human error probability for restoration after maintenance.

Component failure rates: Component failure rates used in PSA for AM and PSR review are so far derived from US ones such as LER and IEEE Std.500 except for fail-to-start of DG. On the other hand, component failure data found in periodic inspection and surveillance test in every NPP in Japan are registered in NUCIA, through which generic component failure rates and plant specific failures can be estimated. NUCIA data being endorsed, PSAs using these data will be utilized in the inspection and operating areas in the safety regulation.

Common cause failures: As there are few common cause failure data in Japan, Beta-factor method used in NUREG-1150 is applied for some systems.

Human reliability analysis: Human error probabilities are estimated by the THERP methodology based on the operating manuals at accident and the status of operator training.

6.2.13 Italy

No information provided.

6.2.14 Hungary

Level 1 PSA: In general, the methodologies followed during the level 1 PSAs for Paks were based on internationally accepted guidelines. However, use of improved or novel methods was also necessary to properly address the specificity of the Paks plant as well as the characteristics of accident sequences during off-power conditions or following the occurrence of internal hazards, such as a fire. The major analysis steps can be briefly summarised as follows.

Definition of plant operational states: This initial analysis was important for the purposes of the shutdown PSA. The plant operating modes described in the Operating Procedures and Technical Specifications of Paks were decomposed into 24 distinct plant operational states (POSs) that represent a PSA driven breakdown of a complete shutdown-refuelling-start-up process. Within a POS the availability and configuration of plant systems, the system success criteria related to a given initiating event (plant transient), as well as the means and conditions of operator responses to a transient can be considered constant. This approach enabled the development of POS dependent PSA sub-models.

Identification of initiating events: A preliminary initiating event list was compiled as a result of reviewing generic and VVER specific databases as well as available, internationally recognised PSA studies for pressurised water reactors. This preliminary list was modified by using operating experience of the Paks plant and by expert opinion. A final list of PSA initiating events was produced after grouping initiating events according to their consequences on plant operation. The final list of internal initiating events contains over 50 different events grouped into 14 major categories. Subsets of these events were taken into consideration during the analysis of low power and shutdown modes as required by the configuration of plant systems, physical parameters, characteristics of operation and maintenance. For internal hazards those fire and flooding initiators are included in the PSA models that cause at least one of the internal initiating events or they require manual reactor shutdown. A task oriented relational database was developed and used to select these fire and flooding initiators. Among others this database contains all essential (safety related) plant components, their exact locations within the plant as well as their functional connections through cabling, an inventory and distribution of ignition sources and combustibles for each plant location, etc.

Frequencies of internal initiating events were calculated by combining generic and plant specific data. A two-stage Bayesian approach was applied to integrate operational data of Paks with generic initiating event frequencies. In addition, use was made of fault tree analysis, human reliability considerations, and expert judgement to generate frequencies of some initiators specific for low power and shutdown modes. The so-called FIVE methodology was followed to estimate fire frequencies. Flood frequencies were determined on the basis of data and recommendations given in a specific report on the subject.

<u>Event sequence analysis</u>: The small event tree - large fault tree approach was followed to develop event trees (and the corresponding accident sequences) for modelling the consequences of an initiating event and additional malfunctions/ failures caused by either random failures or as a consequence of the initiating event (e.g. a fire) itself. In most cases two end-states were modelled: success and core damage, the latter being the (single) plant damage state. Core damage was defined on the basis of DBA criteria using fuel clad temperature and coolability of core geometry as determinants of damage. In addition, boiling of primary coolant in the reactor core was treated as another end-state in those plant operational states where it can lead to direct increase in radiation exposure of plant personnel. System success criteria for ensuring safety functions were defined mostly by the use of results from thermal-hydraulic calculations and from event simulations performed specifically for the purposes of the PSA study. In the shutdown PSA special attention was paid during event tree construction to: (1) modelling system unavailability due to outage operations (maintenance), and (2) identification of required human responses as they depend on the emergency situation and on the plant state as well. Complex, generic event trees were built for internal hazards to describe their multiple effects on the availability and on the operation of plant systems needed for accident mitigation.

<u>System analysis</u>: Modular fault trees were constructed as failure logic models of plant systems included in the PSA. Specific fault tree sub-models were developed for mechanical, electrical and instrumentation and control (I&C) failures. Definitions of component boundaries and failure modes were given so that they would be in agreement with available component reliability data and would allow adequate modelling of failure events. For the purposes of the shutdown PSA differences in system success criteria and system operating modes in the different plant operational states and accidental situations were modelled by extensive use of conditional events (boundary conditions) in the system fault trees. Boundary conditions were defined to describe consequential failures of internal hazards too. These consequential component failures of fires and floods were identified by the use of the database (and event evaluation tool) mentioned earlier in relation to initiating event identification.

<u>Analysis of dependent failures</u>: Functional dependence between systems and system components was explicitly modelled in the system fault trees by a decomposition of systems into functionally independent parts and into the associated basic events. Functionally dependent failures due to the adverse effects of internal hazards were evaluated separately for each fire and flood scenario based on the functional connections between mechanical, I&C and electrical failures. Physical dependence was considered as correlation between an initiating event (or a transient process) and its potential

consequences on system operation. Consequences of heavy load drops were analysed in detail. In particular, use was made of the results from specific analyses performed during the safety evaluation of lifting and moving heavy equipment in the reactor hall. Dependence between human interactions was considered in the human reliability analysis by evaluating those influences on performance that may lead to multiple dependent errors. The residual dependent events were treated as common cause failures using a simple parametric model, the β factor approach. Parametric common cause failure analysis and quantification was based on internationally accepted methods and on generic data.

Human reliability analysis: Human reliability analysis was aimed at selection and quantification of those human errors that can take place either prior to a plant disturbance or during evolution of an incident/accident and, thus, may substantially contribute to the development of a severe accident. Selection of important human-system interactions was integrated into the process of initiating event identification, and event tree and fault tree development. The methods and data used for quantification varied according to (1) the type of action (pre-initiator, initiator and post-initiator actions), (2) the potential error mechanisms and error modes, and (3) the main influences on human performance (actual performance shaping factors). Pre-initiator and initiator errors were modelled by an analysis of operational and maintenance activities, examination of plant experience and also by the use of generic data on error rates. Post-initiator human actions were quantified by developing a generalised decision tree approach to integrate the results of simulator observations, field experience and expert judgement into a context driven model of human reliability.

Reliability database development: Component reliability data were derived from both generic and plant specific data sources. The approach followed was based on an integration of generic and plant specific data. In most cases generic data were combined with plant specific information by the use of Bayesian updating for mechanical, electrical and I&C components as well. Where sufficient data were available preference was given to plant specific estimates of failure parameters. Probability of some fire-induced failure modes (short circuit of power and I&C cables) was assessed by (1) performing cable fire experiments, (2) comparing experimental results with literature data, and (3) using expert estimates for cable arrangements not covered by experimental or literature data.

Accident sequence quantification: During quantification the frequency of sequences leading to core damage (or boiling in some low power and shutdown states) was determined, and the most important risk contributors were identified. Overall point estimates of core damage and boiling risk were computed through integrating the results obtained for the individual accident sequences. Based on these overall measures plant vulnerabilities were determined with respect to the likelihood of a severe accident. Finally, importance, sensitivity and uncertainty analyses were performed to gain further insights useful for characterising risk profile and for recommending safety improvements. Mostly the Risk Spectrum PSA programme was used for quantification. Post-processing of Risk Spectrum results was necessary for integration and overall evaluation of quantitative risk measures and the underlying risk contributors.

Level 2 PSA: The related guideline of the International Atomic Energy Agency published as IAEA Safety Series, No. 50-P-8, 1995 was applied to the extent feasible and practicable as a general methodological framework of the level 2 PSA for NPP Paks. Following is a summary description of the most important analysis steps.

Plant damage state analysis: Level 1 PSA was available for the purpose of the study. So, the first step taken was plant damage state analysis and the development of an interface between the level 1 and level 2 PSA models. 182 theoretically possible plant damage states (PDS) and the corresponding attributes were defined for reactor accidents. Two categories of PDS attributes were applied:

- Category 1 PDS attributes include primary pressure at the onset of core damage and availability/ operation of the emergency core cooling systems before and after core damage. Four pressure ranges were found useful to characterise different types of severe accident progression and source term: very low (< 7 bar), low (7-20 bar), medium (20-60 bar) and high (> 60 bar).

- Category 2 PDS attributes describe the containment status at the onset of core damage and availability of containment spray before and after core damage. Distinction was made between an isolated and a non-isolated containment. Containment bypass was treated as a separate group.

Consequence event trees were developed and linked to the event trees of the level 1 PSA model to decompose the initial core damage sequences into PDS sequences. It appeared most advantageous to apply separate consequence event trees were developed for category 1 and for category 2 PDS attributes respectively. The consequence event trees and the associated fault tree models were constructed so that a correct treatment of dependence could be ensured between the level 1 PSA model and the level 1 – level 2 interface.

The important plant damage states were determined by the use of frequency ranking. As a result 15 plant damage states were selected for further detailed analysis including 13 damage states for power operation and 2 damage states with open reactor vessel and open containment for shutdown operations.

Modelling of severe accident progression and releases: A generic Containment Event Tree (CET) was delineated to describe the progression of an accident from a plant damage state into containment damage states. Early (prior to reactor vessel failure), intermediate (during vessel failure) and late (following vessel failure) phases of accident progression are modelled in the generic CET with the associated physical processes that effect the containment damage state and the source term. Initially, a total number of 28 questions were used in the CET which could be subsequently reduced to 15 branch points to model accident progression and the resulting containment damage state. Most importantly, the headings in the CET are concerned with:

- in-vessel melt retention through melt arrest,
- recovery of failed containment spray in early or late phase,
- early or late hydrogen burn, and
- containment failure due to loads from severe accident in different phases of accident progression.

The containment damage states were defined so that they would represent different release categories. The following containment damages states/release categories were used for the purpose of CET modelling:

1. High Pressure Vessel Failure (HPVF)
2. Containment By-pass (B)
3. Early Containment Failure, Rupture (ECF) – Break size of 0.5 m^2 or higher
4. Early Containment Enhanced Leakage (ECL) – Leak size of 0.05 m^2
5. Late Containment Failure, Rupture (LCF)
6. Late Containment Enhanced Leakage (LCL)
7. Early Containment Failure, Rupture with Spray (ECFS)
8. Early Containment Enhanced Leakage with Spray (ECLS)
9. Late Containment Failure, Rupture with Spray (LCFS)
10. Late Containment Enhanced Leakage with Spray (LCLS)
11. Intact containment (I)
12. Intact containment with Spray (IS)
13. Partial Core Damage (PDC) – no excessive core melt
14. Shutdown State, Open Containment Before Refuelling (SDOC_BR)
15. Shutdown State, Open Containment After Refuelling (SDOC_AR).

The generic CET was the basis for developing PDS specific containment event trees for the dominant plant damage states. This approach was useful in ensuring that the complexity of the CET could be much reduced.

Quantification of CET branches: Severe accident analyses were performed using the MAAP4/VVER code to determine the containment damage state and the release into the environment in relation to the various sequences for each PDS specific containment event tree. Moreover, a dedicated method was developed to express the containment pressure loads in the form of probability distributions. Pressure loads from hydrogen combustion were determined for spontaneous ignition and ignition caused by recombiners for design basis accidents due to the lack of hydrogen management for severe accidents. The pressure load curves were convoluted against the fragility of the containment to obtain the probability of containment failure.

The probabilistic pressure capacity (fragility) of the VVER-440/213 containment structure was determined in a separate analysis. This analysis covered the reinforced concrete pressure boundary and the containment penetrations as well. The results were aggregated in the form of fragility curves for the overall containment structure. The paramount failure mode was found to be containment rupture, whereas gradual, limited leak failure modes could be excluded.

In addition to the likelihood of containment failure, the other major source of input to CET quantification was an assessment of recovering safety injection before reactor vessel damage could occur and recovering containment spray to limit releases as long as it was found effective. The conditions and the probability of such recoveries were evaluated by identifying recoverable failures and by comparing recovery times with the available time window for each relevant CET sequence. A decomposition of system failures into basic event level failures (including equipment failures in the support systems) was used to identify recoverable failures. It was found that both the emergency core cooling systems and the spray system could be recovered by the same recovery actions, i.e. the dominant failure modes were failures in the support systems (e.g. failure of emergency power supply). Non-recoverable component level failures were assigned a conditional probability of 1 for unsuccessful recovery, whereas the probability of successful recovery for recoverable failures was determined on the basis of expected time to recovery from expert opinion. The results from MAAP simulation were used to obtain the time windows for recovery. Separate recovery analysis was performed for each dominant plant damage state.

Each PDS specific CET sequence was quantified to obtain a characterisation of a given plant damage state with respect to the consequences on containment status and the associated release. The sequence level results were added up for the various CETs to arrive at an overall measure for the frequency of each containment damage state. A relationship between containment damage states and consequence categories, derived in a separate part of the analysis, was used to produce a probabilistic description of different releases. The containment event trees were elaborated and quantified by using the Risk Spectrum PSA software. This choice ensures that the level 1 and level 2 PSA results are available on the same platform.

Uncertainty analysis: Uncertainties in large radioactivity release frequencies were assessed in a follow-on analysis of the baseline study. Uncertainties were analysed and evaluated both qualitatively and quantitatively. Qualitative analysis was descriptive by its nature. Quantitative uncertainty analysis covered the following:

- Uncertainties were propagated from the level 1 PSA model to the level 2 PSA in the first phase of the analysis. Quantification was based on the use of the minimal cut sets for the different plant damage states. Monte Carlo simulation was applied and dedicated software was developed and used to assess uncertainties in PDS frequencies by means of propagating uncertainties through the PDS level minimal cut sets.

- The Monte Carlo approach was used to quantify uncertainties in accident progression from a plant damage state to the different containment states and the associated release categories. First the important severe accident phenomena were determined. For these phenomena the available model in the MAAP4/VVER severe accident code was reviewed and refined. Then model parameters were selected for the purpose of uncertainty calculations. The number of variables treated uncertain for MAAP4/VVER simulation was 40. Also, other parameters, e.g. the ignition of burnable mixture and containment fragility were taken into account. Finally, 50 variables were chosen for random sampling in total. The samples from the range and distribution of the selected model parameters were generated by Latin hypercube sampling. Severe accident calculations were done for each branch of the CET. A calculation included MAAP4/VVER runs and processing of the results to get probability samples for the branches of a CET. 200 calculations were performed for each branch of a CET.
- The uncertainty distributions for the PDS frequencies and for the CET branches were sampled and then the frequencies of containment failure states were calculated on the basis of this sampling in accordance with the logic of the CET sequences. The total uncertainty for a containment state was determined by combining the PDS level results for the given containment state. The results obtained for the different containment states were further aggregated to yield overall measures of uncertainty in the so-called consequence categories defined for the purpose of the Paks level 2 PSA. A dedicated spreadsheet based tool was developed and used to propagate uncertainties between plant damages states and containment states/release categories.

<u>Use of results to support severe accident management</u>: Earlier severe accident analyses performed prior to the level 2 PSA had already outlined potential severe accident management measures for NPP Paks. The level 2 PSA and associated uncertainty analysis helped to:

- prioritise measures from risk reduction point of view,
- select feasible and effective measures, and
- develop technical requirements against certain measures.

6.2.15 Germany

The methods to be applied for the PSA, including methods to collect and process reliability data, are described in the PSA Guideline [1] and its technical appendices on PSA methods [2] and data [3].

The quality of a PSA for German NPPs strongly depends on a careful quantification of common cause failures (CCF). The degree of redundancy of the safety systems/trains in German NPPs is especially high (4 x 50 % or 3 x 100 % redundancy). As a consequence, the core damage frequency is dominated by contributions from CCFs. GRS has developed and is applying an own CCF-model ("coupling model", based on a modified BFR model, using empirical data as far as possible [4]). International cooperation in this field and, in particular, the ICDE project of the OECD/NEA, is very important to further develop the CCF modeling and quantification.

Currently, the limitations of the PSA quality are mainly caused by difficulties in quantifying human error probabilities for "errors of commission" and taking into account organizational influences on the reliability of plant staff actions. Further problems are caused by the lack of a model for quantifying the reliability of software-based digital I&C systems being increasingly used also for safety functions in NPPs. An intense continuation of the research activities in these fields is necessary. (Information on Seismic PSA is given in another presentation.)

The PSA Guide and its corresponding technical documents require the use of plant specific reliability data as far as possible and practicable. GRS performs a lot of activities in this field in cooperation with several operators, while nuclear industry has its own program to collect plant specific data. The detailed approach of data collection and use is outlined in the PSA Guide's corresponding technical document on PSA methods.

With regard to Level 2 PSA, the Guideline and the supporting documents contain data recommended for several not well known physical phenomena, based on actual research results. Uncertainty and sensitivity analyses are highlighted as indispensable parts of Level 2 PSA, taking into account the remaining lack of knowledge in this field.

6.2.16 France

Overall methodology: For the Level 1 PSA, EDF and IRSN use a similar classical methodology (Event trees, Fault Trees). Due to the frequent technical discussions, the IRSN and EDF level 1 studies are rather similar, with a comparable level of detail, and similar data (based as far as possible on French experience feedback). The remaining differences are not due to PSA methods or data, but to functional assumptions.

For the Level 2 PSA, in order to evaluate the environmental releases in a probabilistic standpoint, the EDF level 2 PSA covers the level 1 PSA accident sequences leading to core uncovering, both in reactor at power states and in shutdown states. This evaluation is divided in three main parts: an interface between level 1 and level 2, an accident progression analysis modelled by an event tree and a releases evaluation. The level 2 evaluation is also ruled by a simplicity principle, as opposed to the Level 1. Indeed, the uncertainties on the knowledge of the energetic phenomena, which are likely to occur during severe accidents, are much greater than the uncertainties that concern the level 1 model. Therefore, the level 2 model focuses on the main energetic phenomena and on the containment responses to the corresponding stresses and avoids details that would be covered by the inherent uncertainties.

The IRSN level 2 methodology differs from EDF on several points. In the IRSN study, a particular effort is developed for obtaining as far as possible “best estimate” results, avoiding too conservative assumptions. This objective implies in particular a very large number of supporting studies carried out with IRSN codes.

Important specific features are the following:

- a detailed level 1/level 2 interface with > 450 PDS in last version,
- a specific CET quantification software - KANT - developed by IRSN which includes Monte-Carlo simulation and results presentation,
- a high number of core degradation calculations using IRSN codes: severe accident codes: ASTEC, ICARE-CATHARE, MC3D (steam explosion), CAST3M (containment behavior, mechanics), CATHARE 2 or SIPA (thermal-hydraulics transients),
- detailed studies for each physical phenomena,
- use of response surface method and grid method for physical modules of CET and uncertainties assessment,
- no limitation in release category number (more than 1000); effort is made to keep information on kinetics of accidents in the release categories,
- a very fast model for release assessment based on experimental results or ASTEC calculation, and
- in progress work to assess radiological consequences for each release category in relation with Emergency Crisis Center tools.

Common cause failure: The Multiple Greek Letter Method is applied. The parameters values are estimated as far as possible from the French operating experience feedback. It has to be noted that CCF data collection follows the specifications of the OECD/CSNI International Common Cause Failure Exchange project (ICDE).

Human reliability: In the first PSAs HRA was assessed with a methodology (common to EDF and IRSN) based on the THERP methodology and further developed by using mainly simulator observations. This methodology covered pre-accident errors and post-accident actions. The accidental operations are based on the Event-Oriented procedures.

Following the implementation of the State-Oriented procedures, the HRA models were revised, according to the new procedures logic and to simulator observations.

Moreover EDF developed a new generation HRA method (MERMOS), which is now used for all the EDF studies. The MERMOS method assumes that the emergency operation missions are carried out by the emergency operations system, which consists of the control room and the man-machine interfaces, which are controlled by the control room crew by means of the emergency operation instructions. The general approach of the MERMOS method consists in identifying all the scenarios for failure of these emergency operation missions, by looking for possible failure modes, classified according to the Strategy-Action-Decision functions (SAD model), which are commonly associated with behaviour of human operators.

Other issues: A specific feature of the French PSAs is the high level of detail in the modelling of systems and sequences, relying on very detailed functional analysis and supporting studies. For example particular attention was paid to the modelling of supporting systems and of recovery possibilities, including the shared equipment with another unit.

6.2.17 Finland

Licensee perform the PSA model in-house: It is essential that the plant staff performs the PSA in-house as far as possible in order to become well prepared for using the PSA for decision making purposes. The regulatory guide on the use of PSA includes specific prerequisite for the quality of PSA. Accordingly the licensee has to use state-of-the-art PSA methods including human factor analysis, best estimate thermal hydraulic analyses and to perform quantitative uncertainty and sensitivity analyses. In addition the licensee has to draw up and maintain guidelines for ensuring an adequate quality level of evolving PSA model and for using the PSA for safety management activities. These prerequisites mean that the licensee has to allocate a considerable amount of resources to perform PSA. Level 1 PSA which includes only internal initiators required typically 10 or more man-years and the full-scope PSA level 1 and 2 including internal events, fire, flooding, harsh weather conditions and seismic for at power and low power operations requires approximately 50 man-years depending on the plant design. Much more man-years have been needed altogether in the annual updating and extension of the studies since 1989.

Initiating events: The identification of initiating events defines the purpose and scope of a PSA. Initiating events directly affect the core damage frequency. In order to achieve results that adequately reflect the plant’s state, the list of the initiating events identified needs to be as complete as possible. Incomplete consideration of initiating events adversely affects the quality of a PSA, thus leading to results that underestimate the level of risk.

For the Loviisa initiating events, the EPRI and EG&G lists were used, which includes about 40 initiating events based on more than 600 reactor year experience. In addition to these 40 initiating events, 30 Loviisa specific transients have been found. Altogether more than 100 initiating events are grouped into 34 categories. Such initiating events which have dependencies with the unavailability of safety systems, have been well taken into consideration (e.g. cooling ventilation of control room and service water system), i.e., full scope set of initiators.

For the Olkiluoto PSA, plant-specific initiating event data were supplemented with generic data from previous PSAs and the EPRI initiating event list. Regarding the estimation of LOCA frequencies, piping and related components were analysed, and the leak/failure rates were estimated from literature. Plant-specific characteristics, e.g., the length of piping, the number of welds and joints, were also taken into account. LOCA rates during refuelling and shutdown were based on human error analysis. Valve configurations were considered for external leaks.

Systems modelling and event sequence modelling: The Loviisa and Olkiluoto PSAs use the fault tree technique to model the system performance in terms of unavailability per demand and / or the unreliability during mission time. The systems modelling includes analyses of success criteria for safety functions, systems and support systems, systems disabled or degraded by the initiators, dependencies on support systems and other systems, component failures: random and common cause, human errors prior to an initiating event, e. g. during maintenance, calibration, etc., operator errors after occurrence of an initiating event, recoveries and minor repairs. Once the safety functions are identified, then the safety systems, support systems and the effects of the initiator are analyzed, respectively. The identification of causes of unavailability of a system is usually based on systematic analysis of each system (Failure mode and effect analysis (FMEA).

The purpose of the event tree and associated event sequences is to represent the plant response to the initiating event. Since the results of the PSA are sensitive to dependencies, it is important that they are not lost if some simplifications are introduced. The dependencies must pass through the whole sequence from initiator to the last top event of the event tree.

In the Olkiluoto BWR PSA the small event trees and large fault trees were used. The SPSA software automatically takes care of that each cut set appears only in one sequence. The PSA model was constructed by starting from the analysis of all safety systems. Thereafter all support or back-up systems included in the safety systems function were analysed, modelled and linked in the safety system models. Different timings were taken into account with attributes. E.g., one of the most important time-dependent probabilities that varies from sequence to sequence is the probability of restoration of off-site power in a certain time (e.g. before the batteries deplete).

In the Loviisa PWR PSA event trees were not used. Thus the resulting fault tree produces cut sets leading to the core melt.

<u>Example of analysis of dependencies</u>: The analysis of dependencies in Loviisa PSA is mainly made by qualitative method. The explicit modelling is the primary method in taking dependencies into account in Loviisa PSA. In order to recognize the dependencies, the circumstances resulting in different factors were mapped by special dependency lists. In these lists the stress factors of components are addressed. The impact of dependency factors due to circumstances, operation, instructions, calibration, maintenance and surveillance testing on redundant components were recognized as follows:

- statistical dependency: In order to recognize statistical dependencies walk-through method is used. Potential CCFs are listed using standard question lists getting through rooms and related systems. The standard list involves:

    - process deviations (leakages, pressure hits, temperature transients, loose parts, chemical phenomena),
    - environmental decisions (temperature, shaking, humidity, radiation),
    - plant accidents (explosions), and
    - natural phenomena (storms, lightning, earthquake), man-machine interactions (design, installatio common cause failures: The residual CCF is described by multiple failure probabilities that are based on generic (system based) CCF databases by EPRI and NEA/ICDE and some plant-specific data. Because the CCF data do not contain

all various systems, parametric methods (beta and multiple greek letter) are used for some systems. Plant-specific test intervals and schemes were used to calculate the common-cause unavailabilities for different failure multiplicities. All CCFs were modeled as basic events in the system fault trees, connected by OR-gates to the components affected.

- functional dependencies: Functional dependencies between systems (including dependencies between front line systems and its support systems and electrical and instrumentation systems) are modelled directly in fault trees. The dependency matrix is used to represent the intersystem dependencies.

In addition to the functional dependencies the type of dependency (immediate, delayed, shall be activated, continuous etc.) is recognized.

The dependencies between front line systems and its support systems and electrical and instrumentation systems were taken into account in the initiating event identification. Examples of such CCFs are loss of ventilation cooling of electrical and instrument room, partial loss of service water system, loss of conventional intermediate cooling system and 24 V DC supply.

CCF dependencies on initiating event are dealt with external initiators (fires, floods, storms etc.).

Example of collection and analyses of reliability data: The plant specific data and operating experiences have been used as far as possible in Loviisa PSA. The acquisition and analysis of plant specific data is well arranged at Loviisa plant. The LOTI-information system contains all failure history files since 1989 and provides all necessary raw data to the reliability data processing system. The LOTI system gives a sound basis for using Living PSA at Loviisa plant. Just recently a more sophisticated LOMAX system replaced the earlier LOTI system. The old operating experiences (before 1989) have been collected from work orders, control rooms logs and inspection reports. A special empirical Bayesian method was developed during PSA project which estimates mean failure rate and uncertainty distribution for single component. In addition to failure rates of components also trend analysis (aging, learning) is made for failure rates, the processing of data involves an automatic comparison between plan specific and generic data. In few cases generic data have been used instead of plant specific data (e.g. relays in reactor scram systems), if the quality of plant specific data is not adequate.

A combination of the plant specific and Swedish BWR data has been used in Olkiluoto PSA. The operating experience from Olkiluoto has been analysed by the Swedish TUD data system.

Thermal-hydraulic calculations: Thermal-hydraulic calculations are used for estimation of success criteria, consequences and available timings. Calculations performed for a FSAR are usually conservative and their use in determining success criteria for a PSA is possibly limited. A common approach is to perform thermal-hydraulic calculations for representative sequences in an event tree and to use these values for the remaining sequences. While this may be justifiable from the success criteria point of view, there could be much larger differences in related timings.

The use of conservative success criteria can have a large impact on the PSA if the conservative configuration of the system functions requires more redundancies than the configuration based on best-estimate success criteria.

In the Loviisa plant response analyses, the timing and scale of incidents as well as determining of success criteria were analysed with RELAP5 and SMABRE computer codes utilising also former analyses (FSAR etc.). Steam generator leaks were analysed mainly with the ATHLET code. Later on APROS code has been used and COCOSYS for analyses of environmental consequences of leaks. Loviisa plant simulator has also been used to analyse the timing of incidents, but not directly to determine success criteria. Loviisa PSA success criteria are mainly the same as in Final Safety Analysis Report.

In the Olkiluoto PSA, the success criteria were first determined with the help of conservative FSAR analyses. Additional analyses were ordered from plant vendor for PSA purposes in order to get less conservative estimations of safety systems ability to fulfil their safety functions. The plant vendor used GOBLIN and BISON codes to support the development and updating of the PSA models. During the development and updating of the PSA models, TVO has performed hundreds of MAAP-runs. Another very large set of MAAP-runs has been executed during the development of the Level 2 PSA and the results of these runs have been used to refine the accident sequences of the Level 1 PSA.

In the Olkiluoto PSA, the basic success criterion is that the plant must survive a transient for 24 hours after an initiator. Further, it is assumed that all safety systems must function at least for 24 hours, even if the core damage occurs earlier. A number of sequence-specific simplifications have been made, but these are mostly conservative and are mostly related to timings (e.g. it is assumed that something can not be done during the available time).

Normally only those protection signals that appear at every sequence in an event tree are credited (conservative assumption). The most important exceptions to this rule are the signal for automatic supply of boric acid, which is modelled for sequences where the control rods fail to function, and the depressurisation signal, which is modelled for relevant sequences.

Some sequences containing the depressurisation of the containment go up to about 40 h.

Analysis of human errors: In Loviisa PSA the human reliability analysis (HRA) is performed using combination of well known ASEP-HRA and TRC methods (simulator runs) which have been partly modified and developed in the PSA project. The analysis of human errors is made in three distinct phases:

- errors before initiating events (surveillance tests, maintenance and calibration),
- errors that lead to initiating events, and
- errors that are made after initiating event.

The human error data involved 180 human errors which had taken place during 15 years of operation.

The errors of third category were handled in two parts: a) errors in diagnosis, and b) operator errors during accidents.

The full-scale Loviisa simulator was used to create the time-reliability correlations which were used to estimate the probability of too long diagnosis time. In the analysis of incorrect diagnosis a confusion matrix method was used.

In Olkiluoto PSA the HRA is performed using SHARP approach (Systematic Human Action reliability Procedure). The Full scale Olkiluoto simulator was used to provide the operator error probabilities.

Model quantification: The quantification process requires the use of qualified computer codes. The computer codes used in solving fault trees may use the rare event approximation when event probabilities are below about 0.1. Computer codes use minimal cut set upper bound or provide an exact solution to avoid overly pessimistic results. For the examined PSAs various computer codes are used. (SPSA, CAFTA, Risk Spectrum). As seen in some benchmark exercises, not all the codes are based on the same basic methods (e.g. simulation versus analytic approach). Also the implemented features (e. g. the importance measures) and the fault tree modularization procedures are slightly different. Finally, the user friendliness, the capabilities to solve large fault trees, and the computational speed are different for the various codes. However, the benchmarks results have shown that identical fault trees have resulted in sound results independent of the code used.

6.2.18 Czech Republic

For the PSA main tasks (accident sequence delineation, system modelling, human reliability analysis, CCF modelling, HRA, accident sequence quantification, etc.) methodologies have been adopted within the individual plant PSA projects. Several reference documents and giudelines (NUREGs, IAEA guidelines, other PSAs, etc. [4,5,6]) have been considered for this purpose.

The PSA for Dukovany contains three unit specific models, one for unit No. 1, one for unit No. 3 and common one for units No. 2 or 4. The RiskSpectrum PSA Professional code is used for model development and calculation. Models for both units in the twin co-unit are maintained in the common RiskSpectrum database. Such approach allows explicit modeling of shared systems including their neighbor unit support systems.

In the Dukovany PSA model developed by the end of 2005, the whole plant operation was split into 13 Plant Operating States (POS's) in PSA model. The comprehensive set of 31 initiating event (IE) groups has been defined. Each IE group contains one or more sub-events, which are analyzed separately in specific event trees within the particular POS.

The identification of IEs is based on:

- generic IE list from IAEA-TECDOC-749 and IAEA-EBP-WWER-09,
- events considered in SAR and EOP's,
- list of IE's from other PSAs for WWER 440/213
- events occurred in plant history,
- systematic analyses (internal fires & floods, heavy load drops, man-induced LOCA's, boron dilution, etc.).

For each of the identified events that survives the screening, the applicability to the POSs has been assigned. All those events are then analyzed separately in each relevant POS.

The (relatively) small event tree - large fault tree approach is used for accident development. The challenge of critical safety functions Reactivity Control, Decay Heat Removal, Primary Reactor Coolant Boundary Integrity and Primary Reactor Coolant Boundary Inventory is addressed in modelling of plant response to an IE.

System fault trees are linked to event trees via fault tree top logic called interface, which addresses success criteria for one of more systems for a given safety function. The system modelling includes all identified sources of component/ system unavailability, such as random component failures, their common cause failures (CCFs), disabled or degraded components by the initiators, dependencies on support systems and other systems, pre- and post-accident human errors, unavailabilities due to test, repair or maintenance, recoveries, etc. [19]

Different system configurations as well as zero maintenance state can be set in the fault trees using boundary conditions, so the model is prepared for various PSA applications.

The CCF modeling is based on the Alpha factor models. The basis for quantification of CCF events has been formed by new sets of generic data (NUREG/CR-5497). In addition, a detailed analysis of Dukovany operational experience regarding CCF occurrence covering last 40 reactor years was performed. This analysis provided some plant specific data used for modification of selected CCF parameters.

Both pre- and post-initiating-event human errors are modeled in HRA using methodology SHARP as well as some inputs from the new analytical framework ATHEANA. The quantification has been largely based on THERP, ASEP and decision tree methodologies. Test and maintenance activities are covered in a very detailed pre-initiating event human reliability analysis. Errors of commission are included to some extent. [20]

The approach to component data analysis is driven with specific processes defined and followed at NPP Dukovany. According to plant procedures, an up-date of the component and initiating event data is performed regularly every five years. A general strategy is to use plant specific data as much as possible. The methodology of quantitative data analysis corresponds to current standards. In the field of initiating event frequencies, Bayesian approach is used for combination of generic and plant specific data. All failure rates of components with relatively high importance measures are based on plant specific data exclusively.

At Temelin site the methodology used in the PSA update was the same as that used in the original PSA being in line with standard PSA development procedures and recommendations. The PSA model has been developed using small event tree/large fault tree linking methodology using the WINNUPRA™ code. The event trees are „Plant Damage State„ event trees, which have been developed with the Level 2 in mind, to give a smooth interface between Level 1 and Level 2 models. The Level 2 model has been developed using WINNUCAP software.

During the update of the original PSA care has been taken to ensure that all comments raised by reviews of the earlier work are incorporated in the models. In addition, all plant equipment and procedure changes and the latest transient analysis information were included. To ensure that this work was done in a methodical manner a specific update task plan, covering all tasks was developed. The primary reference for this plan was the IAEA document, „Living probabilistic safety assessment (LPSA)“[7].

Quality Assurance Plan for the performance of the Temelin PSA was developed incorporating the elements of an acceptable Scientech QA Program designed to meet 10 CFR 50, Appendix B [8] requirements to the extent possible. The key features of the program involved: design and documentation control, verification, review of interim and final work products, and software control. The findings of the review have been documented and are maintained in the Project files.

The original IE analysis was reviewed by the expert missions conducted in the frame of two IAEA IPER missions. The first IPERS review of the Temelin PSA Level 1 (internal events) model, conducted by international experts took place in April/May 1995 and the second one reviewing external events and Level 2 model in January 1996. For the updated PSA Level 1 and Level 2 the IAEA IPSART mission took place in late 2003.

Both the VVER-specific and the non-VVER specific and generic information from various sources were examined for initiating events estimation task. The analysis starting point was a detailed generic list of IEs for WWER 1000 based on the IAEA effort in the TC Project RER/9/005 [9]. Other information was obtained from VVER operational experience [10,11,12] as well as IAEA-PRIS (AIRS) outage records. US PWR operating experience was considered on the basis of the IEs rates developed by US NRC in NUREG/CR-5750.

For some special cases however, such as Interfacing System LOCAs, and common cause initiators, simple plant specific analytical models have been created. For these cases, the models themselves are constructed to generate the parameter of interest.

In addition, an FMEA of support systems was performed to find out potential initiating events specific to the Temelin design. Initiating events taken from above mentioned sources were examined for their applicability, and grouped into several general groups based on their similarities with respect to the plant response. These subevents were grouped into 5 LOCA and 14 transient groups. The frequencies of each IE group were estimated as the sum of the subevent frequencies.

For system analysis at Temelin PSA the standard approach used in [3,14,15] has been adopted for the modeling of system failures. For the level 1 PSA, the methodology is current state-of-the-art methodology. The small event tree - large fault tree methodology (using fault tree linking) is used. All Level 1 models (both at power and shutdown) are managed with the WinNUPRA code, the Level 2 analysis is done using WinNUCAP code.

The Temelin equipment is provided by various Czech, Eastern Europe and Western suppliers. Therefore, for the original PSA model quantification, several sources of both VVER specific and non-specific data parameters were used: Dukovany NPP (VVER 440) data collection, VVER 1000 data for LHI pumps, DGs and turbine bypass valves [16], the IAEA data compilation [17], the Swedish Reliability Data Book [18], and the IREP NUREG/CR-2728.

While construction of the plant has been completed, there is still insufficient operating history to support data collection, and therefore, there is no plant-specific data upon which to base estimates. However, in some cases, additional information has become available from other studies completed since 1996. This new information has been considered for components that were important to the results of the initial PSA and for those components where the new data based on VVER units operation experience differs notably from the previous Temelin analysis.

Currently, the plant specific data gathering system is being developed to enable introduce the plant specific data to the PSA models as soon as sufficiently representative statistical sample will be available for different populations of components.

The quantification of parameters of basic events modeling residual common cause failures was performed as a part of the common cause failure analysis. In the original study, the Beta Factor method for CCF analysis was used for the screening level and Alpha Factor method for those common cause component groups which were found to contribute significantly to the CDF.

A more detailed method for the analysis and quantification of CCFs was selected for the current PSA, the Multiple Greek Letter (MGL) method. The quantification of CCFs was performed in two phases. In the first phase, a screening phase, the basic screening generic values of MGL parameters obtained from a table in NUREG/CR-5801 were used for CCF groups. More realistic CCF parameter values were used replacing the screening values in the final quantification obtained from NUREG/CR-5485.

A combination of several well-known methods was used for detailed analysis and quantification of pre-accident human failures in Temelin PSA. Basically, the probabilities of more complex phenomena connected with human reliability (pre-accident errors) have been estimated by decomposition of possible scenarios, and quantification of elementary points, using simple rules for combining probabilities based on probability theory. The quantification of probability of elementary phenomena has been performed by means of well known THERP and ASEP methods.

For post-accident events in the DDD phase, using the methodology adopted, a distinction was made between time-critical and non-time-critical responses because of different HRA models are usually used for these two modes. In the time-critical mode, the time reliability curves (TRCs) in ASEP (NUREG/CR-4772) are used for HEP quantification. In the non-time-critical mode, a modification of the decision tree approach developed for EPRI has been chosen for more detailed analysis.

Analysis of severe accident progression has been performed in order to support Level 1 and Level 2 interface, containment event tree (CET) model, and the definition of source term categories (STC). The main computer code used in the severe accident analysis for Temelin was MELCOR 1.8.3. This version has been certified by the Czech regulatory authority (SUJB). Some older analyses were conducted using the STCP code. In addition to MELCOR integral code, some mechanistic separate effects codes have also been used – ICARE-2 for the analyses of fuel damage progression during SAs and CONTAIN code (version 1.12) for the analyses of containment phenomena including DCH aspects. The code WECHSL, which is part of the integral code ASTEC being developed in EU, was used for MCCI calculations. Quantification of the Level 2 model is conducted using WinNUCAP software that was used in sorting and grouping of PDSs and handling CET/DET model.

6.2.19 Canada

For the multi-unit Candu plants, OPG uses for the level 1 PSA, the small event tree-large fault tree methodology (using fault tree linking). All models are managed with the CAFTA code. Because of the need to represent shared systems between multiple units, the integrated level 1 model involves 40 systems and up to 60,000 basic events. Results are obtained for a single representative unit and assumed to apply to any unit, because differences between units are usually minor.

Data is obtained partly from plant-specific records and partly from generic data from the Candu industry where available and elsewhere if not.

As far as is possible, all common cause events are modelled explicitly in the fault trees. Where equipment redundancy exists within a system and no explicit CCF event is identified, residual CCF treatment is based on the Alpha model and uses generic CCF-parameter data.

For human reliability, pre- and post-initiating-event human errors are modelled by using a methodology that is largely based on the THERP approach. Test and maintenance activities are covered in the pre-initiating event human reliability analysis. Some errors of commission are included and extensive recovery events are modelled using the Qrecover feature of CAFTA.

The level 2 analysis is based on about 20 plant damage states, not including the status of containment systems. These are integrated into the containment event tree along with top events representing failures of containment system functions, early and late containment failure. Sequences are binned to release categories using MAAP and level 1 and level 2 sequences integrated in CAFTA to obtain frequencies.

MAAP release estimates representative of each release category are used as input to the offsite calculations, performed by using MACCS2.

The BBRA essentially employs the same methodology as the OPG PRAs above with two notable exceptions. The original model was developed under the SETS solution framework and methodology. It is currently being migrated into a CAFTA-based environment with event-tree based integration. As much as practical, identifiable common causes are covered in the PRA models. In updating the BBRA following migration to CAFTA, Bruce Power will follow recommended COG guidelines on intrinsic common cause.

As much as possible, the BAPRA methodology was patterned from the BBRA. Notable differences are the use of Windows Risk Spectrum as platform for the PRA, simplification of process system modelling, and the use of the limiting human error concepts. Intrinsic CCFs are also modelled for selected highly-redundant components but are not quantified at this time.

For CANDU 6 and ACR, the PSA methodology, using fault tree event tree integration is being employed. The CANDU component database is taken from CANDU operating experience. The human reliability assessment (HRA) employs THERP and ASEP methodology for pre- and post-initiating event. CCF modeling is based on the Unified Partial Beta Methodology (UPM).

Level 2 PSA will follow IAEA guideline as much as practicable for a CANDU design. Severe core damage consequence analyses will be performed using MAAP-CANDU computer code.

6.2.20 Belgium

For the level 1 PSA, the methodology is current state-of-the-art methodology. The small event tree - large fault tree methodology (using fault tree linking) is used. All models are managed with the RiskSpectrum code.

Initiating events: Usually generic data are used (NUREG 5750 for instance), however the operating experience is analyzed and incorporated in the updated PSA by using specific transient data when available or specific simplified fault tree for support system failures.

Thermal-hydraulic calculations: Thermal-hydraulic calculations have been used for the estimation of success criteria and acceptable (operator or system) intervention times. These were performed for representative sequences in an event tree. RELAP was the code used. For the level 2 severe accident phenomena have been analysed through the use of MELCOR.

Common Cause Failure: The CCF-modelling is based on the Multiple Greek Letter and Binomial Failure Rate models and uses generic CCF-parameter data.

Human Reliability Analysis: For human reliability, as well pre- as post-initiating-event human errors are modelled, by using a methodology that is largely based on the THERP and ASEP methodologies. Test and maintenance activities are covered in the pre-initiating event human reliability analysis. Errors of commission are included to some extent.

During the update of the models, errors of commission will be identified in a more systematic way by the CESA method.

PSA data: The safety related component data handbook, the T-Book (6^{th} version) - Reliability Data of Components in Nordic Nuclear Power Plants, will be used for the on-going update of the models.

System Analysis: For the system analysis, particular attention had to be devoted in the Doel 1 and 2 PSA, because of some shared systems (twin unit).

PSA Level 2: As the PSA studies for both Tihange 1 and Doel 1/2 were not integrated PSA1/PSA2 a detailed Level1/Level2 interface study had to be performed.

For Doel 1/2 level 2 study a total of 33 plant damage states (PDS) was identified, with each PDS characterized with 13 attributes. For Tihange 1 a total of 9 attributes were used to characterise 64 Plant Damage States. For both Doel 1/2 and Tihange 1, the large Accident Progression Event Tree (APET) approach has been adopted. This large APET is the result of an extensive decomposition process. In this case, instead of considering the physics of accident progression implicitly when evaluating branch point probabilities in a simple containment event tree, a sufficient number of events as well as logical interrelations between these events are added to the APET to be able to model all relevant aspects of accident behaviour. This results in a single, large event tree with many events (including PDS attributes) and more than 100000 significant branching points. Subtrees have been developed to represent the event tree structure associated to specific phenomena or accident progression aspects. The logical structure of any event in the APET can be determined by such a subtree.

The results of the PSAs were mainly explored via analysis of the dominant accident sequences and their main contributors.

7 PSA APPLICATIONS

7.1 Summary

Design evaluation: The main application of the PSA has been for design evaluation where the insights from the PSA have been used in combination with the insights from the deterministic analysis in a risk-informed approach. The PSA has been used to: identify the dominant contributions to the risk (CDF and LERF); identify weaknesses in the design and operation of the plant; determine whether the design is balanced. This has been done at the design stage for new plants or during periodic safety reviews for existing plants.

It is often the case that, during the lifetime of the plant, the scope of the PSA that is carried out has increased – for example the PSA has been extended to include external hazards, cover low power and shutdown conditions, and extend the analysis to a level 2 PSA. This identifies additional weaknesses that need to be addressed.

There are many instances of where the PSA has identified weaknesses where plant improvements have been made. For example, the PSAs carried out in France for shutdown conditions identified significant contributions to the risk related to excessive drainage of the primary circuit during mid-loop operation and of heterogeneous boron dilution that could lead to a reactivity accident. Improvements to the design and operation were made to reduce the risk.

The PSA has also been used to compare the options for design changes to determine the relative reductions in risk that they would give. This is often done as part of a cost-benefit approach to determining what plant improvements should be made.

The PSA has been used to identify issues that have arisen such as: increasing the time between refuelling outages; increasing the power level of the core; and carrying out more maintenance at power so that the length of the refuelling outage can be shortened. The PSA has been used to provide risk information in making the decisions on these issues.

Accident management: Often, the Level 2 PSA has been used to identify accident management measures that could be carried out to mitigate the effects of a severe accident. This has led to the incorporation of hardware in the plant (such as the catalytic hydrogen recombiners installed in the containment for all 7 nuclear power plants in Belgium) and the implement of Severe Accident Management Guidelines to guide operators in the event of a severe accident. An example of this is the large programme of work carried out in Japan to produce Level 2 PSAs for each of the types of plant in the country and to incorporate plant specific hardware and guidelines in all the plants.

PSA-based event analysis: The analysis of operating events using the PSA is carried out in many countries as part of the analysis of operating experience. The process usually involves a deterministic screening process to identify the significant events and the PSA is then used to determine the extent to which safety margins were reduced. This indicated the relative seriousness of the event.

Evaluation of Technical Specifications: The Tech Specs define the Limiting Conditions for Operation (LCOs), the Allowed Outage Times (AOTs) and the Surveillance Test Intervals (STIs). In the past these have been based on deterministic considerations. In many counties the PSA has been used to justify and optimise the LCOs, AOTs and STIs.

Where the PSA that has been carried out addresses both operation at power and low power and shutdown conditions, it has been used as part of the justification for moving some of the maintenance activities from being carried out during plant shutdown to being carried out during power operation. This has the economic benefit of shortening the refuelling outages without leading to a significant increase in the risk.

The PSA has also been used to justify an exemption from a Tech Spec. An example of this arose at Borssele when a reserve cooling water pump was found to be unavailable at a time when there was no spare at the plant. The PSA was used to show that the level of risk would be higher from shutting down the plant as was required by the Tech Specs than if the plant was allowed to continue operation at power.

Training of operators and plant staff: The PSA is being used at a number of plants to provide an input into the training programme of plant staff. The aim is to focus the training on risk significant systems/ structures/ components, accident scenarios, maintenance activities, etc. In particular, the PSA is being used to identify risk significant scenarios to use in simulator training. Risk Monitors are also being used in training since they give a very direct indication of how activities being carried out on the plant affect the risk.

Risk-Informed In-Service Inspection: RI-ISI is being carried out for a number of plants. Both the Westinghouse and the EPRI methodologies are being applied.

Risk Monitors: These are now in operation at a very large number of plants and this is one of the most widely accepted PSA applications. They are being used on a day to day basis in making decision on plant safety issues relating to maintenance activities, They have generally been introduced to provide a tool for addressing maintenance rules e.g. the US 50.65 (a)(4).

The Risk Monitors are used: to avoid simultaneous plant unavailabilities that would lead to a high point-in-time risk; to plan the maintenance outages over a period of time to minimise any risk increases, and to monitor the plant performance over time by addressing the cumulative risk.

There are a number of Risk Monitor software packages that are commercially available such as the Safety Monitor and ELOOS, In addition, software packages have been produced and are in use in some countries – for example, the Taipower Integrated Risk Monitor (TIRM-2) in Taiwan and the Essential System Outage Programme (ESOP) in the UK.

Risk informed treatment of structures, systems and components: The PSA has been used, along with the deterministic insights, to identify the systems important to safety and these have been monitored using an enhanced surveillance programme. The same approach has also been used to identify the active components that need to be given special attention as part of the programme for the management of ageing.

Emergency planning: The source terms and frequencies produced by the Level 2 PSA have been used as the basis for emergency planning. For example, the information from the Level 2 PSA for Borssele has been used to define the emergency planning zones for sheltering, the issue of stable iodine tablets and evacuation. In Switzerland, the results of the Level 2 PSA have been used to identify the reference scenarios for emergency planning.

Risk informed regulation: The risk information provided by the PSA is increasingly being used by regulatory authorities in planning their activities. This includes: the prioritisation of inspection tasks so that they focus on risk significant issues; determining the significance of inspection findings; the response to non-compliances. An example of this is in Mexico where plant specific Risk Inspection Guides have been developed.

An example of this is the Reactor Oversight Process (ROP) carried out by US NRC. Similar processes to this are carried out in other countries.

A risk informed approach is used in a number of countries as an input to changing the regulations. In the USA, this approach has been used to change the regulations relating to: fire protection, combustible gas control, emergency core cooling system requirements and pressurised thermal shock. Details of how there changes were made are given below in country answers.

7.2 Country replies

7.2.1 USA

This section provides examples of PSA applications. In addition to the specific examples given below, PSAs are used to provide insights to support the design certification for new reactor types.

Reactor Oversight Program (ROP): The NRC's operating reactor oversight process (ROP) provides a means to collect information about licensee performance, assess the information for its safety significance, and provide for appropriate licensee and NRC response. Because there are many aspects of facility operation and maintenance, the NRC inspects utility programs and processes on a risk-informed sampling basis to obtain representative information. PSA results are used in many ways to support the oversight program, including inspection planning for both the baseline inspections and supplementary inspections. The ROP relies on a combination of information concerning performance indicators and inspection findings to monitor licensee performance. PSA methods are used to determine the risk significance of inspection findings using the Significance Determination Process (SDP). This process relies initially on simplified PSA models, with the option, if a more refined assessment of the risk significance is warranted, of using more sophisticated models, such as NRC's SPAR models or the licensees' PSA models.

Recently, the Mitigating Systems performance index (MSPI) was developed as a replacement for the existing safety system unavailability (SSU) performance index (PI). The MSPI is a risk-informed PI, relying on individual licensee PSAs for the CDF estimates to be used in the calculation of the index.

Additional information can be found at: http://www.nrc.gov/reactors/operating/oversight.html.

Using PSA results and perspectives to identify possible changes to NRC's reactor safety requirements

Risk-informed treatment of structures, systems, and components (SSC): In 1998, the Commission decided to consider promulgating new regulations that would provide an alternative risk-informed approach for special treatment requirements in the current regulations for power reactors. Special treatment requirements are requirements imposed on structures, systems, and components (SSCs) that go beyond industry-established requirements for equipment classified as "commercial grade." Special treatment requirements provide additional confidence that the equipment is capable of meeting its functional requirements under design basis conditions. These requirements include additional design considerations, qualification, change control, documentation, reporting, maintenance, testing, surveillance, and quality assurance requirements. The final rule was published in the *Federal Register* on November 22, 2004 (69 FR 68008). The accompanying Regulatory Guide, RG 1.201, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance" was published for trial use in 2006.

RG 1.201 endorses, with some clarification, a process described by the Nuclear Energy Institute (NEI) in Revision 0 to its guidance document NEI 00-04, "10 CFR 50.69 SSC Categorization Guideline." This process groups SSCs into one of four categories:

"RISC-1" SSCs: safety-related, safety-significant
"RISC-2" SSCs: nonsafety-related, safety-significant
"RISC-3" SSCs: safety-related, low-safety-significant
"RISC-4" SSCs: nonsafety-related, low-safety-significant

The categorization approach employed by NEI 00-04 uses the Fussell-Vesely and Risk Achievement Worth importance measures (considering both CDF and LERF) to determine SSC safety significance.

Risk-informed, performance-based approach to fire protection (10 CFR 50.48(c)): In 2004, a revised version of 10 CFR 50.48, "Fire Protection," was published. This revised rule allows licensees to adopt a risk-informed, performance-based approach to fire protection as described in the consensus standard NFPA 805, "Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants." NFPA 805 describes how fire PSA results are used in performance-based evaluations of fire protection features and in assessments of the impact of changes in a previously approved fire protection program element.

The revised rule provides a means to establish a well defined fire protection licensing bases and enable licensees to manage their fire protection programs with minimal regulatory intervention. To support implementation of the rule, NEI has developed NEI 04-02, "Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)," and NEI 00-01, Rev. 1, "Guidance for Post-Fire Safe Shutdown Analysis". The staff has endorsed these two guidance documents in RG 1.205, "Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants," with a few exceptions.

In related efforts, the NRC Office of Nuclear Regulatory Research (RES) has worked with the Electric Power Research Institute (EPRI) to develop a fire PRA methodology (NUREG/CR-6850 / EPRI 1011989) that addresses lessons learned from the IPEEEs and from subsequent fire-risk related research. This work is supporting the American Nuclear Society's development of a fire PRA standard, discussed in Section 4.2.1. RES and EPRI are also collaborating in a program aimed at verifying and validating selected fire models.

<u>Combustible gas control (10 CFR 50.44)</u>: As part of the NRC staff's program to risk-inform the technical requirements of 10 CFR Part 50 (discussed under Option 3 from SECY-98-300), the staff identified 10 CFR 50.44, "Standards for Combustible Gas Control System in Light-Water-Cooled Power Reactors," as a regulation that warranted revision.

The NRC completed a feasibility study that evaluated the combustible gas control requirements against risk insights from NUREG-1150 and the IPE program. The study concluded that combustible gases generated from design basis accidents were not risk-significant for any LWR containment types. Specifically, combustible gas generated from severe accidents was not risk-significant for boiling water reactor (BWR) Mark I and II containments, provided that the inerted atmosphere was maintained; for BWR Mark III and pressurized water reactor (PWR) ice-condenser containments, provided that the required igniter systems were operational, or for PWR large dry containment because of their large volumes, high failure pressures, and the likelihood of random ignition to prevent the buildup of detonable hydrogen concentrations. Based on these findings, 10 CFR 50.44 was modified in September, 2003 to remove existing requirements for hydrogen recombiners for design-basis accidents and to reduce the safety grade classification of hydrogen and oxygen monitoring systems.

<u>Emergency core cooling system requirements (10 CFR 50.46)</u>: As part of the staff's program to risk-inform the technical requirements of 10 CFR Part 50 (discussed under Option 3 from SECY-98-300), the staff identified 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors," Appendix K to 10 CFR Part 50, "ECCS Evaluation Models," and General Design Criteria (GDC) 35, "Emergency Core Cooling," of Appendix A to 10 CFR Part 50, as regulations that warranted revision.

In SECY-01-0133, "Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria)," and SECY-02-0057 (an update to SECY-01-0133), the staff recommended rulemaking to change the technical requirements for the emergency core cooling systems (ECCS). The staff recommended separate rulemakings for proposed changes to (1) ECCS functional reliability requirements, (2) ECCS acceptance criteria, and (3) ECCS evaluation model requirements. In March 2003, the Commission instructed the staff to prepare a proposed rule to allow for a risk-informed alternative to the present maximum LOCA break size. In SECY-04-0037, the staff sought further direction from the Commission on policy issues related to the proposed LOCA redefinition rule. The Commission indicated that the proposed rule should determine an appropriate risk-informed alternative break size and that break sizes larger than that size be removed from the design basis category. The Commission indicated that the proposed rule should be broadly structured to allow operational as well as design changes. It should include requirements for licensees to maintain capability to mitigate the full spectrum of LOCAs up to the double-ended guillotine break of the largest reactor coolant system (RCS) pipe and the mitigation capabilities for beyond design-basis events should be controlled by NRC requirements commensurate with the safety significance of these capabilities. The Commission further stated that LOCA frequencies should be periodically reevaluated and that if increases in frequency required licensees to restore the facility to its original design basis or make other changes, the backfit rule (10 CFR 50.109) would not apply.

The rule would establish an alternative set of risk-informed requirements with which licensees could choose to comply in lieu of meeting the current ECCS requirements in 10 CFR 50.46. It would divide the current spectrum of LOCA break sizes into two regions. The division between the two regions is delineated by a “transition break size” (TBS). The first region includes small size breaks up to and including the TBS. The second region includes breaks larger than the TBS up to and including the double-ended guillotine break (DEGB) of the largest RCS pipe. Pipe breaks in the smaller break size region are considered more likely than pipe breaks in the larger break size region. Consequently, each break size region would be subject to different ECCS requirements, commensurate with likelihood of the break. LOCAs in the smaller break size region must be analyzed by the methods, assumptions and criteria currently used for LOCA analysis; accidents in the larger break size region would be analyzed by less stringent methods based on their lower likelihood. Although LOCAs for break sizes larger than the transition break size would become “beyond design-basis accidents,” licensees would have to maintain at least a single train of equipment capable of mitigating all LOCAs up to and including the DEGB of the largest RCS pipe.

Licensees who perform LOCA analyses using the risk-informed alternative requirements might find that their plant designs are no longer limited by certain parameters associated with previous DEGB analyses. Reducing the DEGB limitations could enable licensees to propose a wide scope of design or operational changes up to the point of being limited by some other parameter associated with any of the required accident analyses. Potential design changes include optimization of containment spray designs, modifying core peaking factors, optimizing set points on accumulators or removing some from service, eliminating fast starting of one or more emergency diesel generators, and increasing power. Some of these design and operational changes could increase plant safety since a licensee could optimize its systems to better mitigate the more likely LOCAs.

The proposed §50.46a would require that future changes to a facility, technical specifications, or operating procedures made by licensees who adopt 10 CFR 50.46a be evaluated by a risk-informed integrated safety performance (RISP) assessment process which has been reviewed and approved by the NRC via the routine process for license amendments. The RISP assessment process would ensure that all plant changes involved acceptable changes in risk and were consistent with other criteria from RG 1.174 to ensure adequate defence-in-depth, safety margins and performance measurement. Licensees with an approved RISP assessment process would be allowed to make certain facility changes without NRC review if they met §50.59 and § 50.46a requirements, including the criterion that risk increases cannot exceed a "minimal" level. Licensees could make other facility changes after NRC approval if they met the §50.90 requirements for license amendments and the criteria in §50.46a, including the criterion that risk increases cannot exceed a "small" threshold.

The proposed rule was published in the Federal Register on November 7, 2005. In response to NEI and the Westinghouse Owners Group requests, the comment period was extended 30 days until March 8, 2006. On December 20, 2005, a report on "Seismic Considerations for the Transition Break Size" was posted for comment on the NRC rulemaking web site. A public stakeholder meeting was held on February 16, 2006, to allow stakeholders to ask questions and discuss the proposed rule before submitting written comments. The NRC is now analyzing public comments received on the proposed rule.

Pressurised thermal shock rule (10 CFR 50.61): In 1986, the NRC established the pressurized thermal shock (PTS) rule (10 CFR 50.61) in response to an issue concerning the integrity of embrittled reactor pressure vessels in pressurized-water reactors. The results of extensive subsequent research on key technical issues indicated that there may be unnecessary conservatism in the rule, and the staff initiated an effort to reevaluate the technical basis for the rule.

This work involved the development of a PTS PSA methodology and the application of this methodology to the Oconee, Beaver Valley, and Palisades plants. The PTS PSAs integrate event sequence analyses performed to identify scenarios that had the potential lead to a through-wall crack of a PWR reactor pressure vessel (RPV), thermal-hydraulic analyses performed to determine the thermal hydraulic behavior of the RCS during the scenario, and probabilistic fracture mechanics analyses performed to determine the likelihood of RPV failure. State-of-the-art methods were used in all phases of the analysis. In the event sequence analysis, for example, the ATHEANA method was used to identify and quantify human failure events.

NUREG-1806, which summarizes the results of the technical assessment and presents the bases for possible changes to 10 CFR 50.61, was published in June 2005. The staff initiated rulemaking in October 2005. Several technical issues have been identified during this process and the staff is resolving these while the rulemaking process proceeds.

Operational Events Analysis: To analyze operational events, the NRC uses PSA techniques to provide estimates of operating event significance in terms of the potential for core damage. The types of events evaluated include initiators, degradation of plant conditions, and safety equipment failures that could increase the probability of postulated accident sequences. The accident sequence precursor (ASP) program systematically evaluates nuclear power plant operating experience using PSA methods to identify, document, and rank those operating events or conditions that were most significant in terms of the potential for inadequate core cooling and core damage. In addition, the program also does the following: (1) categorize the precursors for plant-specific and generic implications; (2) provide a measure that can be used to trend nuclear power plant core damage risk; and (3) provide a check on PSA-predicted core damage scenarios.

ASP analyses utilize information obtained from: (1) inspection reports and standardized plant analysis risk (SPAR) models; (2) industry-wide analyses reported via initiating event studies, component reliability studies, system reliability studies, common cause failure (CCF) studies, and special issue studies such as those addressing fire events and service water system events; and (3) operational data contained in the sequence coding and search system (SCSS) of the licensee event report (LER) database, reliability and availability data system (RADS), the CCF database, and the monthly operating report (MOR) database.

NRC uses comparisons between ASP analyses and significance determination process (SDP) assessments of inspection findings as part of their ROP self-assessment program. Trending information from the ASP program is part of the NRC's annual performance report to Congress. The ASP program provides the Commission with annual assessments of the significance of events/conditions occurring at commercial power plants and the trends in industry performance.

Licensing actions

Risk-informed technical specifications: Consistent with the Commission's policy statements on technical specifications and the use of PSA, the NRC and the industry continue to develop risk-informed improvements to the current system of technical specifications (STS). Proposals for risk-informed improvements to the STS are judged based on their ability to maintain or improve safety, the amount of unnecessary burden reduction they will likely produce, their ability to make NRC's regulation of plant operations more efficient and effective, the amount of industry interest in the proposal, and the complexity of the proposed change. The staff is re-evaluating the priorities for its review of risk-informed technical specification initiatives. The staff intends to follow the process described in NRC Regulatory Issue Summary 2000-06, "Consolidated Line Item Improvement Process For Adopting Standard Technical Specifications Changes for Power Reactors," for reviewing and implementing these improvements to the STS.

The industry and the staff have identified eight initiatives to date for risk-informed improvements to the STS. They are: 1) define the preferred end state for technical specification actions (usually hot shutdown for PWRs); 2) increase the time allowed to delay entering required actions when a surveillance is missed; 3) modify existing mode restraint logic to allow greater flexibility (i.e., use risk assessments for entry into higher mode limiting conditions for operation (LCOs) based on low risk); 4) replace the current system of fixed completion times with reliance on a configuration risk management program (CRMP); 5) optimize surveillance frequencies; 6) modify LCO 3.0.3 actions to allow for a risk-informed evaluation to determine whether it is better to shut down or to continue to operate; 7) define actions to be taken when equipment is not operable but is still functional; and 8) risk-inform the scope of the TS rule. Initiatives 1, 2, 3, and 7 have been completed. Initiatives 4b and 5b are discussed in more detail below.

Initiative 4b,"Risk-Informed CTs, use of a configuration risk management program (CRMP): Current technical specifications (TS) contain equipment-specific outage times; known as TS completion times (CTs) and also referred to as allowed outage times (AOTs). The TS contain limiting conditions for operation (LCO) action statements and associated CTs (e.g., if the diesel generator is inoperable, restore within 7 days; if not restored, take actions to proceed to plant shutdown within 24 hours). Current TS address systems independently, and do not generally account for the combined risk impact of multiple concurrent equipment out of service conditions. The maintenance rule configuration risk assessment requirement was added to address this consideration, but does not obviate compliance with current TS requirements. These current TS requirements may present inconsistencies with the maintenance rule requirements, and may require plant shutdown, or other actions, that are not the most risk-effective actions given the specific plant configuration. The proposal involves a combination of the current TS CTs, a quantified risk assessment to determine CT extension feasibility, and CT backstop limits. The CT backstop limits ensure that low risk safety functions are not permitted to be inoperable for an indefinite period of time. This initiative would permit, contingent upon the results of a plant configuration risk assessment, temporary revision of the existing CT within an LCO using a quantitative implementation of 50.65(a)(4). A risk management guidance document, which addresses the use of the PSA to determine CTs is being developed by the Nuclear Energy Institute, and is nearing approval by NRC. Two pilot plants have submitted license amendments that are under review.

Initiative 5b, "SR Frequency Control Program in TS: Current technical specifications provide specific surveillance requirements and surveillance test intervals (frequencies). Compliance with these requirements are necessary to retain operability of the equipment, and avoid entrance into action requirements. The goal of this initiative is to develop a risk-informed process that would establish surveillance frequencies based on risk insights, equipment availability and reliability factors, performance history, etc., to determine an "optimum" SR frequency. The intent is to retain the existing surveillance requirements in the technical specifications, but to remove the equipment-specific surveillance frequencies. Surveillance frequencies would be controlled through an NRC approved process that is defined in the Administrative Controls Section of TS, and contained in a licensee controlled document. The process/methodology documents for Initiative 5b are nearing approval for the pilot plant.

Risk-informed in-service inspection: The objective of an in-service inspection (ISI) program is to identify degraded conditions that are precursors to pipe failures. Regulatory requirements for ISI are specified in 10 CFR 50.55a(g) that references ASME Code Section XI for ISI requirements. However, 10 CFR 50.55a(a)(3)(i) provides for authorization of alternative ISI programs by the Director of NRR. The staff and industry recognized that the ASME code in-service inspection requirements would be more efficient and effective if risk insights instead of ASME guidelines were used to determine the number and locations of welds to inspect. The NRC issued risk-informed ISI

(RI-ISI) Regulatory Guide 1.178 and Standard Review Plan Section 3.9.8 in September 1998 (Revision 1 was issued September 2003). NRC also approved well defined generic methodologies via Safety Evaluations for Westinghouse Owners Group (WOG) and EPRI Topical Reports in December 1998, and October 1999, respectively. All requests to implement RI-ISI programs have referenced one of the two approved Topical Reports.

The use of an alternative is only authorized for one 10-year ASME interval. At the end of each 10-year ASME interval, licensees must update their ASME Code of Record and request authorization for all alternatives proposed for the next interval. Licensees briefly discuss updates to their RI-ISI program during the 10-year update of their ASME Code of Record.

The staff has also approved EPRI (June 2002) and WOG (March 2004) methodologies for use in identifying the number and location of inspections in the Break Exclusion Region (BER) inspection programs. The BER inspection programs are normally part of the licensing basis as described in the Final Safety Analysis Report (FSAR). When the BER program is in the FSAR, the application of RI-ISI to the BER program may be done via the 10 CFR 50.59 process.

ASME has issued three Code Cases and a non-mandatory Appendix R for RI-ISI applications that include both EPRI and WOG methods. NRC may endorse the Code Cases in RG 1.147, with limitations and conditions where appropriate. The NRC may use 50.55a rulemaking to incorporate Appendix R by referencing the ASME Code addendum

There are 78 units with risk-informed in-service inspection programs, 54 units using the EPRI methodology, and the remaining 24 using the WOG methodology. To date, these programs have been used to expand the in-service inspection to piping within the break exclusion region via the 10 CFR 50.59 process.

Risk-informed in-service testing: In August 1998, the NRC issued Regulatory Guide 1.175, "An Approach for Plant-Specific, Risk-Informed Decision-making: In-service Testing," which provides guidance regarding changes to the risk-informed in-service testing program. The agency subsequently completed a pilot application of risk-informed in-service testing in 1998, and has approved or is reviewing several other applications, generally of limited scope.

Risk-informed containment integrated leak rate test (ILRT) interval: In 1995, regulations were amended to provide Option B to 10 CFR 50, Appendix J. Option B allows Type A containment integrated leak rate test intervals to be extended based on test performance history. This test interval could then be extended from 3 in 10 years to once in 10 years. By 2001, licensees began requesting one-time test interval extensions from once in 10 years to once in 15 years based on performance history and risk insights. Due to the widespread interest in applying for one-time ILRT extensions, NEI proposed an industry guideline based on a generic risk impact assessment. If the assessment was found to be acceptable, ILRT test intervals could have been extended permanently from 10 years to 20 years.

The NEI industry guideline and a supporting Electric Power Research Institute (EPRI) technical report were officially submitted and review of the documents began in 2004. Due to insufficient industry data on failures that could result in a risk-significant large early release, an expert elicitation process was used for determination of risk-significant large failure magnitude and frequency in the reports. During review of this expert elicitation process, several technical and documentation concerns were identified by NRC staff reviewers lead to the conclusion that 20 year ILRT intervals could not be supported.

As a result, NEI resubmitted both the industry guideline and technical report to address permanent 15 year ILRT test intervals in lieu of 20 year ILRT intervals based on previously submitted licensee requests for one-time 15 year extensions and additional considerations provided by NRC staff reviewers at a public meeting in June 2005. Safety evaluations for 75 nuclear plant unit licensee submittals have been completed. Amendment reviews for an additional 6 units are in progress.

Search for Vulnerabilities: The Individual Plant Evaluation (IPE) program and the Individual Plant Evaluation for External Events (IPEEE) program successfully resulted in the nuclear power industry identifying safety improvements that substantially reduced the risk of accidents. Over 80% of the licensees have identified and implemented or proposed plant improvements to address concerns revealed through the IPEEE program. These voluntary licensee improvements have led to enhanced plant capability to respond to external events (such as earthquakes and floods) which can be important contributors to total plant CDF. The generic insights from this effort are being used to support development of PSA guidance and standards, while plant-specific risk information is supporting the risk-informed reactor oversight program.

7.2.2 United Kingdom

Risk Monitors: Risk Monitors have been in operation at Heysham 2 and Torness since 1986. These were based on the Level 1 PSAs that were produced as part of the Pre-Operational Safety Case. Although these reactors were built to the same design, they were originally operated by different utilities and this resulted in different approaches being adopted for the two Risk Monitors.

The Essential Systems Status Monitor (ESSM) at Heysham 2 carries out a comparison with the deterministic requirements covering safety system availability and a probabilistic analysis which is done using a fault tree model of the Level 1 PSA that is solved for each plant configuration input into the Risk Monitor.

At Torness, compliance with the deterministic operating rules in assessed using the Essential Systems Outage Program (ESOP) and a separate probabilistic assessment is carried out using LINKITT which contains the pre-solved cut-sets from the Level 1 PSA model. As plant becomes unavailable, the basic events corresponding to those plant items are removed from the cut-sets. This revised list of cut-sets is minimalised and the overall risk is quantified. This produces an approximation to the exact solution but, even with a large amount of plant unavailable, it has been shown that the LINKITT results are acceptable.

The Risk Monitors at Heysham 2 and Torness have been uprated to reflect the Level 2 PSAs that were produced in 1999 as part of the Periodic Safety Review and subsequently developed into four-quadrant models which correctly represents initiating events arising in each of the four quadrants (as required for a Risk Monitor application). This four-quadrant model is being maintained as a Living PSA.

A common approach to the Risk Monitors at the two stations has now been introduced. The new software, ESOP2000, draws on the ESOP/ LINKITT approach and calculates risk using a full re-quantification of the four-quadrant PSA model. The pre-solved cut-set manipulation technique used with the present Level 1 PSA model was found to be unsuitable when used with the new, more complex Level 2 four-quadrant model. Improvements in computer processing speeds now allows re-quantification to be performed in a sufficiently short time to permit its use as an “on-line” Risk Monitor. This approach preserves a key requirement for the Risk Monitors, namely that updating of the software to reflect the Living PSA is both easy and quick.

A trial of Relcon’s Risk Spectrum software Risk Watcher is currently underway at Sizewell B PWR nuclear power station; the trial is limited to only full power operation. Initial results are encouraging as to the usefulness of such a monitor to assist in enhancing efficient and safe operations.

For the UK’s two remaining Magnox reactors no Risk Monitors are planned due to their short remaining operational life.

Risk Informed Technical Specifications: The traditional approach in the UK is to define Operating Rules and a Maintenance, Inspection and Test Schedule which are derived from the safety case to define the operational envelope of the plant. Over time, these have become increasingly sophisticated and have made use of PSA insights, including the incorporation of Risk Monitors at Heysham 2 and Torness.

For Sizewell B, it was decided that this traditional approach would be replaced by developing Technical Specifications which was in line with normal practice for light water reactors. The Tech Specs which were produced were based on the Methodically Engineered, Restructured and Improved Tech Specs (MERITS). However, these needed to be developed to take account of the changes to the SNUPPS design that had been made for Sizewell B.

The PSA was used to support the development of the Tech Specs. In particular, it was used to confirm Allowed Outage Times (OATs) and Limiting Conditions of Operation (LCOs), and to justify the inclusion or omission of systems from the Tech Specs. The basic approach was to use the PSA model to determine acceptable completion times based on limiting both the average risk and the point-in-time risk. This provided the basic input into the Action Completion Times (ACT). For systems where the ACT was greater than 3 months for system restoration for either single train or all train failures, this provided the case for either the relaxation of the requirement to have all trains operable, in the former case, or for the omission of the system from the Tech Specs, in the latter case. In addition, the PSA was used to justify surveillance frequencies.

7.2.3 Taiwan

Risk Monitor: A Risk Monitor named Taipower Integrated Risk Monitor (TIRM) was developed collaboratively by INER and the Licensee. It was first released in 1999 with the capabilities of motoring at-power and shutdown risk by providing risk profile of CDF. Because of the robust features of providing shutdown risk directly from outage schedule, TAEC requested the Licensee to perform shutdown risk analysis using TIRM before entering refueling outage. The second generation risk monitor (TIRM-2) was released in 2002 which includes the LERF evaluation and the enhancement of calculation speed and accuracy. By introducing a powerful risk model solver INERISKEN developed by INER, a PSA model can be completely resolved in less than one minute. It means that the user will obtain a complete hourly risk profile of a typical 50-day outage schedule in less than 5 minutes. In addition to the high speed, the results from TIRM-2 (MCSs and Importance Measurements) had been demonstrated to have exactly results compared with those obtained from WinNUPRA.

Online Maintenance: The TAEC originally didn’t encourage any online maintenance performed in NPPs from the interpretation that voluntarily entering LCO should be treated as a violation to the Technical Specification. The quality of PSA model to support the evaluation of online maintenance risk was also questioned during 1990’.

The situation changed when the PSA peer review was completed. Following the acceptance of PSA peer review by TAEC, Chinshan NPP submitted a risk-informed application to perform online maintenance on the RHR system in 2003. The risk change for online maintenance was calculated by PSA considering the plant configuration change and the administrative control plan. The TAEC reviewed and approved this application. The TAEC also agreed to review applications of online maintenance on limited systems on a case-by-case basis. The Licensee still has to apply to get the permit from TAEC each time even though those systems had been previously approved.

In light of the growing needs of more online maintenance to enhance the performance of the NPPs, the Licensee negotiates with the TAEC to perform a wider scope of online maintenance and decides to voluntarily implement the Maintenance Rule in the beginning of 2007. The TAEC also declares its regulatory position to allow for rolling-scheduled online maintenance when the Maintenance Rule is in place.

Risk-Informed Fire Analysis: In order to apply the exemption to cable tray fire wrapping requirements, the Licensee contracted with INER to perform detailed fire analysis for Chinshan NPP by using the developed living PSA in 2001. It was the first attempt to utilize the developed risk-informed performance-based fire protection regulatory guidance in the application of fire wrapping exemption in Taiwan. The purpose of the project was to identify the risk significance fire zones by enhancing the fire risk models in the PSA in the beginning and then to provide practical alternative suggestions of plant design changes in order to take exemption from the cable tray fire wrapping requirements. All suggestions are derived in a risk-informed process by calculating the risk changes if all cable trays in a risk significance fire zone are not wrapped. The exemption application was intensively reviewed to confirm that the risk change is still within the acceptable region and the alternatives are in conformance with fire safety principles. The TAEC approved the exempted application and the associated design changes to the cable tray fire wrapping of Chinshan NPP at the end of 2005.

The applications of the other two plants are now under review by TAEC.

Risk Significance Evaluation Tool for Inspector: A computer tool named PRA Model Based Risk Significance Evaluation (PRiSE) was release to the TAEC at the end of 2003. The PRiSE is designed to help the resident inspectors of the TAEC to determine the risk significance of inspection findings. The risk significance is determined by the change of CDF and is categorized into four color codes (green, white, yellow and red). A screen process is provided to help the inspector screen out the inspection finding which has no risk significance. The criteria and procedure is quite the same as the Significance Determination Process (SDP) developed by the USNRC. The difference is that PRiSE replaces the table that the USNRC has developed for performing Phase 2 of the SDP. To determine the color code of inspection finding, the inspector needs to specify a proper plant status change which properly reflects their inspection findings. Those changes could be the degrade or unavailable of safety systems, the increase of likelihood of initiating event frequencies, the availability of components, and the probability change of special events in the PSA model like the common cause failure or human error. Once the changes of plant configuration are specified, the increase level of CDF will be calculated by resolving the PSA model which can be done in less than one minute. The TAEC has announced to adopt PRiSE in daily inspection activities from the January of 2006. The results will be posted on the website each quarter and will provide an important index to determinine the future regulatory plans in response to the inspection findings.

7.2.4 Switzerland

The initial PSA applications concentrated on the determination of the overall plant safety level, the assessment of the balance of the plant safety concept and the identification of procedural and hardware improvements. Other applications have included the assessment of the risk impact of power uprate, justification of reference scenarios for emergency planning, categorization of accidents and selection of risk-significant components to be considered in an ageing surveillance programme. It should be noted here, that to date, not all of these PSA applications are formalized and/or “regulated” to the same degree.

Design Evaluation: To date, the main application of PSA has concerned the re-evaluation of various Swiss plants, in terms of identification of potential plant-specific vulnerabilities. This has been the main focus of HSK’s PSA evaluation activities, within the framework of plant-specific licensing actions and/or the periodic safety review, as a complementary tool to the deterministic safety analysis. The benefit of using PSA in this framework is illustrated in detail in Section 82.4.

Evaluation of Technical Specifications: The plant-specific PSAs are increasingly used by the Swiss utilities in order to evaluate the risk of the proposed changes of technical specifications. Vice versa, risk-beneficial changes to technical specifications have been suggested and implemented based on PSA insights. HSK makes use of its own PSA models in dealing with specific utility applications in this regard. This is an area where increased activity on the parts of both the utilities and HSK is anticipated over the coming years.

Accident Management: Insights from the plant-specific level 2 studies are used as a part for the technical basis of the development of Severe Accident Management Guidance (SAMG) in order to provide information on the possible accident progressions and plant states. Furthermore, level 2 PSAs are also used for the preparation of emergency exercises dealing with severe accidents.

Use of the PSA for Emergency Planning: For the purpose of planning for nuclear power plant emergencies and any countermeasures, HSK has defined three "reference" accident scenarios as being the most probable representative scenarios. Plant-specific level 2 PSAs were used to justify these reference scenarios, and based on a full spectrum of release categories, HSK selected those releases that are representative of these reference scenarios. For each nuclear power plant, the cumulative frequency of accident sequences not covered by the reference scenarios was calculated and was shown to be small (i.e., of the order $\sim 10^{-6}$ per reactor-year excluding earthquakes).

Assessment of the Operational Experience: As a first step, HSK performed a probabilistic analysis of the operational experience of all Swiss nuclear power plants for the year 2000. With the help of this study, a systematic approach for the probabilistic event analysis was defined.

In the next phase, HSK required a probabilistic event analysis from all licensees expanded to cover events recorded back through 1998. (1998 is the starting point for introduction of the safety indicators.) Based on this additional experience, two probabilistic safety indicators (one for the assessment of the accumulated risk and one for the assessment of risk "peaks") have been defined.

All relevant data for the assessment of the operational experience have been collected and incorporated into a databank, allowing various analyses to be performed (e.g. computation of probabilistic safety indicators, determination of the contribution of planned and unplanned maintenance and of initiating events to the safety indicators, trend analysis, etc.).

Ageing Surveillance Programme: Various aspects are considered in order to select those active components that underlie a detailed ageing surveillance programme. The selection criteria encompass deterministic rules, considerations of system engineers and radiological protection experts, and consideration of risk-based criteria. This integrated selection approach is implemented as part of a regulatory guideline.

Based on several pilot studies performed by both the licensees and HSK, risk-based selection criteria in terms of importance measures have been developed. The risk criteria are applied independently to consider components of safety classes 2 through 4 and non-safety class components. (Safety class 1 components are always part of the ageing surveillance programme.) The following criteria were considered to be acceptable: a component shall be selected for the detailed ageing surveillance programme if the Fussell-Vesely (FV) or the Risk Achievement Worth (RAW) of that component fulfils the following condition:

$$FV \geq 10^{-3} \text{ or } RAW \geq 2$$

These risk-based selection criteria are not yet part of a regulatory guideline, but have been accepted by HSK. In order to identify all risk-relevant components, not only the full power level 1 model, but also the shutdown and the level 2 PSA models should be considered. The licensees have started to refine their PSA-models and PSA codes in order to facilitate the calculation of risk importance of components.

Categorization of Accidents: The new Swiss nuclear energy act requires that sufficient preventive and mitigative measures shall be implemented in order to ensure the safety of nuclear power plants in Switzerland. The process to demonstrate that sufficient measures have been taken is described in a regulatory guideline. A comprehensive list of accidents is designated in that guideline. These accidents are categorized according to their frequencies. The accident frequency is defined as the product of the initiating event frequency and the probability of the most limiting independent single failure event. To the extent possible, the corresponding initiating event frequencies and probabilities are based on plant-specific PSA insights (note that the single failure event probability is restricted to the interval of 0.01 to 0.1). The accidents are then categorized by their frequencies. Category 1 covers frequencies greater than 10^{-2} per year. Category 2 covers the frequency in the interval of 10^{-2} to 10^{-4} per year and Category 3 represents the frequency interval 10^{-4} to 10^{-6} per year. Accidents with a frequency smaller than 10^{-6} per year are considered to be beyond the design-basis accident envelope. Dose limits are defined for accidents in Categories 1, 2 and 3.

7.2.5 Sweden

The PSA models are being used in following applications in Sweden today for;

- design evaluation
- identification and reduction of the risk from dominant contributors, also support for back-fitting activities and plant modifications at comparison of design options.
- providing an input into risk-informed Technical Specifications
- risk informed configuration control
- risk monitors are at present tested and evaluated at some of the domestic NPP:s
- Reliability Centred Maintenance
- providing an input into emergency operating and other procedures
- accident management strategies
- emergency planning
- training of significant plant operating and maintenance staff.
- the development and monitoring of plant safety indicators.
- analysis of operational events or of PSA based event analysis.
- risk informed regulation.
- risk informed in-service inspection, in-service testing.
- review of security arrangements.
- verification of deterministic analyses in SARs: e.g., in level-1/2 studies, shut-down, fire, flooding studies, external hazard analyses.
- identification of safety significant scenarios (e.g., functions, systems, components, human errors).
- Technical Specifications (AOT, maintenance, testing, instructions).
- impact and planning of plant modifications.
- Living PSA.
- trend analyses.

The information provided should focus on the most recent applications of the PSA and describe how the PSA was used, the quality requirements for the PSA before it could be used for the application and any changes that needed to be made to the PSA to make it suitable for the application.

Use of risk-informed approaches in Sweden

- the risk-informed approach has been applied more or less all the time at SKI. It is a natural ingredient in a regulators way of solving the daily commissions. Most of the missions are not treated with aid of PSAs, but rather are the feelings of deterministic approaches used, as well as a long knowledge and experience of how certain factual questions have evolved and been treated by time.
- use of probabilistic risk-informed approaches is a new technique, especially in applications dealing with optimizing the control and testing of piping systems. In 2005 SKI reviewed the very first application on this matter from one of our PWR plants. Other plants are in the preparation phase with similar applications to SKI.

In our Westinghouse PWR plants, the licensee has adopted a new standard for the Technical Specifications (TS). The PWR plants have now a TS authorized by SKI according to the NUREG-1431 and interpreted against the domestic regulation SKIFS 2004:1.
As a result of this reviewing work SKI has demanded the licensee to perform PSA of changed (relaxed) LCOs, before the Improved Technical Specifications (ITS) could be adopted.

Applications of interest include:

– Risk informed decision making
– Standard Technical Specification according to NUREG-1413 principles.
– Specific regulatory body activities, involving usage of PSA.
– Establishing of inspection, reviewing practices according to the results of the PSA-results and PSA-activities in Sweden.
– SKI site specific and annual safety assessment. PSA-results and PSA-activities are input to this SKI internal process.
– Trend analyses of impact of occurred event on safety barriers and on work & activities belonging to the defence-in-depth principles.
– Probabilistic & deterministic impact of introduced new technique (e.g., digital technique).

International projects with coupling to PSA issues: Sweden do e.g., participate in the following OECD/NEA projects

– OPDE, FIRE, ICDE

The reliability data to be used for safety related components in Swedish PSA studies, are presented in the T-Book 6th edition (see section 4.2.5)

PSA Program: See appendix a for summary, also section 4.2.5 domestic guidances development.

Reliability Centred Maintenance: The RCM technique is used and practised at the Swedish NPPs.

Technical Specifications: The domestic licensees are requested to use PSA and to measure impact of changes in Technical

Specifications, plant modifications: Risk informed approaches are used, when changes of AOTs are discussed.

Living PSA: The domestic licensees are in varying ways practising the LPSA applications in their follow-up of their safety work e.g., at evaluating operating experience, measuring impact of changes in Tech. Specs, plant modifications.

Safety monitor: Safety monitors are at present goal for evaluation at e.g., the Oskarshamn and Ringhals plants.

In early 2007, an interesting research project will be established by the SKI.A research project titled "Assessment of Defence in Depth using PSA", will be initiated by the Swedish Nuclear Power Inspectorate (SKI) during late 2006 and performed mostly during 2007. The aim of the project is to evaluate the possibilities of use PSA models and results as a tool to risk assess and rank the structures, systems, components and procedures that are part of the defence in depth of a nuclear power plant. Such a ranking might be used as a complement to the event classification based on Plant Conditions (PC1 to PC5) according to ANSI/ANS-51.1 (PWR) and 52.1 (BWR). An important background to the project is the recently released regulation SKIFS 2004:1,

There are a number of risk-informed applications where parts of the defence in depth are analysed and risk assessed with PSA – this is in fact one of the basic aims of PSA. PSA results can generally be seen as an assessment of the overall safety of a plant, giving information about the capability of the plant as such and of its various safety functions to handle various types of disturbances, both relatively frequent ones and disturbances that are expected to occur extremely infrequently.

However, there is at this time no explicit connection between PSA and the various levels of defence in depth as defined in SKIFS 2004:1 and INSAG-10.

Within the project planned, it is expected to be of interest to perform a systematic and focused analysis of the connections between the levels of defence in depth, and the risk measures utilised in existing applications in order to make efficient use of available information on risks. This review may lead to the definition of new risk measures that may be used in the risk assessment procedure, and which may be of use in assessing the safety level of a plant, evaluation of occurred events with safety impact, and evaluation of proposed plant changes, including changes in SAR or technical Specifications.

7.2.6 Spain

The IP Edition 2 main objective is the promotion of PSA applications. Several points of the Program are devoted to it and described in the following.

The CSN has promoted the use of the PSA in regulations (applications) and inspections. Two aspects of the PSA applications can be considered, those related to regulatory actions and those related to inspections and oversight.

Spanish Regulatory Authority started in 2002 a Program with the utilities in order to get a more effective regulation process (Improvements in the Regulatory Process). This program includes eight tasks, one of the tasks was to analyse and to adapt the Reactor Oversight Process to the Spanish oversight on NPPs. For this analysis people from utilities and regulatory body were appointed.

The aim for this change was to make a more systematic inspection being concentrated in main risk areas and areas with the worst performance.

The activities related to the risk informed inspections and oversights have been initiated and currently after a pilot phase have been applied.

The Reactor Oversight Process (ROP) from the USNRC has being implemented in Spain adapting procedures and practices. The Spanish adapted ROP is called Integrated System of Nuclear Power Plants Oversight (SISC). In this process the PSA is used in many ways, selecting the components and systems impacting risk to be object of the inspections and also in the categorization of the inspections findings.

In this area the most significant activities are: (a) the risk informed baseline inspections and (b) the Significance Determination Process at power, fire protection, containment integrity, SG tube rupture and shutdown. Performance indicators related to initiating events, mitigations system barrier integrity are also carried out.

On the other hand, for regulatory actions the CSN and the licensees have developed a procedure following the Westinghouse methodology for the PSA applications of In-service inspections. After two pilot applications on Garoña (BWR) and Asco (PWR) the process have been implemented and applied to the pressurized water reactors Ascó and Almaraz with the scope of piping class I and for the boiling water reactor Cofrentes for class I and II.

CSN is also promoting the training of inspectors and the planning and performing the inspections programs through a friendly intra-web PSA information system. The content of all the PSAs is accessible to the CSN inspectors so the acceptance of the PSA as a tool for helping the inspections is greatly increased.

Typical external applications submitted by the utilities to the CSN for approval are: exemption of Technical Specifications related to the allowed outage times (AOT), extension of the fuel cycle shutdown, on-line preventive maintenance during power operation, power increasing. All these submittals are evaluated by the CSN complementing the deterministic safety criteria and for those objective internal procedure is issued establishing the composition of a multidisciplinary team of specialists of deterministic and probabilistic experts.

For these external PSA applications, a consensus was reached on specific methodologies for carrying out diverse types of applications. Examples are the PSA applications to technical specifications, in-service inspection or graded quality assurance. In that process of consensus, experience was gained with applications by means of using guides developed in the USA, as much on the part of the industry as on the part of the regulator of that country.

Other IP point makes reference to a somewhat new aspect, but extremely necessary, since PSA can be systematically applied to the many fields where these techniques can contribute with their vision, simultaneously global and detailed, on the factors that affect safety. For it, training plans on PSA and dissemination of the knowledge and results of each PSA are needed as much within the CSN as within each NPP organization. As for the CSN concerns, most of the technical staff has already taken a basic course on PSA techniques.

An internal networked web-based PSA information system has been developed and it includes the PSA information on Level 1, Level 2 and LPSD of the Spanish NPPs. Also external event are being included in the system. This information system is being very useful to spread the PSA knowledge within the CSN.

Strategic objective of the CSN is the use of the PSA to make more efficient use of resources, both licensees and the CSN.

7.2.7 Slovenia

Applications at the Krško NPP

The Krško PSA model is used to support various plant-specific applications, referred to as PSA applications:

- Support to various plant design-related modifications and associated issues. Examples include supporting evaluation of BIT Boron Concentration reduction or evaluation of CC check valve 10075. Two major applications in this category were:
    - Fire Protection Action Plan;
    - Integrated Safety Assessment of the NPP Krško Modernization;

- Risk assessments to support on-line maintenance (OLM). The assessments are performed to support macro and micro-scheduling of activities. At the beginning of the cycle rough estimate is done on the basis of the preliminary list of activities proposed to take place in the cycle to come. Iterations are done as necessary. During the cycle evaluations are done on a weekly basis. Interactions take place primarily between OLM coordinator and responsible PSA engineer. Two types of OLM weekly reports are generated by a PSA group. First type is the so called “assessment-type” report, which contains an assessment of the risk associated with OLM activities in the forthcoming week. It is generated two weeks prior the week it concerns and it is based on the projected time-schedule of activities (e.g. projected durations). Second type is referred to as a “quantification-type” report. It is generated after the week of concern is over and it contains an assessment, which is based on the actual schedule of the activities that took place. Once the OLM cycle is over, then all the weekly evaluations are summarized in the technical report providing the overview of the risk assessments for the OLM activities done in the cycle of concern.

- Risk assessments to support planning and implementation of plant outages. The Krško NPP outage risk management is based on ORAM (which is currently being updated/substituted), which contains a qualitative assessment module (Shutdown Safety Functions Assessment Trees (SSFATs)) and a Shutdown PSA module. Assessments are done to support both outage planning and its implementation. Upon completion of an outage, the associated risk assessment is documented in the report together with the OLM cycle to provide an overall perspective.

- Importance analyses and risk rankings to support various plant programmes. Examples: Importance Analysis of Safety Injection (SI) and Essential Service Water (SW) System; Importance Analysis of the Krško NPP Systems Equipment and Components; Risk Importance Ranking Analysis of the Krško NPP MOV for the Krško, and NPP MOV Program, the Krško NPP AOV PSA Methodology Risk Ranking Report;

- Support to the Krško NPP Maintenance Rule programme: PSA Input to SSC Risk Significance Determination for the Purpose of the Krško NPP Maintenance Rule Programme and OLM risk assessments;

- Support to Operators’ Simulator-based Training Programme.

- Monitoring of the plant risk profile and providing input into the development of long-term strategies. Technical reports that accompany the issuance of new revisions of plant Baseline PSA Model provide the interpretations of quantification results and contain the information on the overall plant risk profile.

- Envisioned applications: support to the development of ISI / IST strategies, graded QA programme, evaluation of TS requirements, etc.

Applications at the SNSA

The SNSA also uses PSA for its applications such as plant systems configuration impact on safety, plant vulnerabilities evaluations. The most important application is a PSA based event analysis. Feedback of operating experience has always been an important issue in nuclear industry. A probabilistic safety analysis (PSA) can be used as a tool to analyse how an operational event might have developed adversely in order to obtain a quantitative assessment of the safety significance of the event. This process is called the PSA-based Event Analysis. A procedure for such an event analysis was developed at the SNSA. The main goal of evaluation and assessment regarding operational events is:

- identification of open safety issues, appearing during the Krško NPP operation with intent to maintain and upgrade nuclear safety;
- allocation of acceptable solutions regarding unresolved safety ques
- identification of the event causes, failure mechanisms and operational faults; improvement of inspection techniques and procedures, identification and resolution of common safety issues, evaluation of proposed corrective actions
- improvement of event scenario and transient conductance knowledge (system and components behavior, operational personnel actions) and implementation of knowledge in the processes of the SNSA (analyses, assessment, preparedness of the SNSA in case of nuclear events);
- to upgrade the SNSA decision making process and regulatory positions regarding nuclear safety;

The procedure deals with authorization and responsibilities, event inputs (sources of information), event screening, detailed investigation (root cause analysis and PSA analysis) and preparation of the Final Report.

7.2.8 Slovak Republic

The plants have well established living PSA programs which are being continued and the PSA studies are being periodically updated. In addition, the following PSA applications are used:

<u>PSA support of plant modifications</u>: The PSA results are used to evaluate the proposed changes within the plant safety upgrading. The PSA is able to show the effects of the change on the risk. The plant PSA models were step-by-step updated, to take into account the modifications, implemented into the V1 and V2 J. Bohunice NPP during their reconstruction. The PSA studies presented the PSA results and quantified the benefit of the modifications from the risk reduction point of view. In some cases, based on the PSA results, changes were proposed to reduce the risk.

<u>PSA support for termination of plant operation</u>: After termination of the unit 1 operation of the V1 J.Bohunice NPP, the risk for the unit 2 was calculated. The risk of the unit 2 is increased. The objective of PSA application was to quantify the increased risk and to propose changes to reduce the risk to the former level. In addition, the risk was calculated for the unit 1 with terminated operation. The risk was compared for two cases: 1) storage of spent fuel in reactor vessel in operating mode 5 and 2) storage of spent fuel in the spent fuel pool.

<u>Risk monitors</u>: The EOOS risk monitor is used for the V1 and V2 J. Bohunice NPP. The Safety Monitor is installed in the Mochovce NPP. These monitors are used to determine the instantaneous risk based on the actual status of the systems and components of the plant. So, the plant staff is supported in its operational decisions. In addition, the monitors are used to optimize the preventive maintenance activities. In the Slovak plants, the operators use the risk monitor daily, the PSA experts use it monthly to prepare the monthly reports about the risk profile. The maintenance schedulers activities in this area is now only limited. The risk is given in the form of core damage frequency (CDF). In addition to CDF, the EOOS risk monitor calculates also the LERF (Large Early Release Frequency) for the V1 plant. Only the CDF is calculated in case of the V2 and Mochovce plants. The EOOS risk monitor was developed also for the spent fuel pool of the V1 J. Bohunice NPP for the state after termination of the unit 1 operation. The risk is given in the form of fuel damage frequency in the pool.

<u>Optimization of the technical specifications:</u> Support of decisions to modify individual plant technical specification (TS) is important activity in this area. Using the PSA model the AOTs (Allowed Outage Time) were evaluated for all safety systems of the V2 J. Bohunice plant. The main conclusion from

the analysis is that the current deterministic AOTs are conservative and should be extended for the majority of the safety systems. Similar analyses are performed or being performed for the V1 J.Bohunice NPP and Mochovce NPP.

Other applications: The analysis of operating events using the PSA model is also applied. Training of operators and the plant staff for the most dominant accident sequences being performed. The level 2 PSAs are used to support the development of SAMGs, etc.

7.2.9 Netherlands

The PSAs for the HFR and Dodewaard were only used for design review. The PSA for the Borssele NPP is used for several applications. Therefore, the remaining part of this chapter exclusively deals with applications of the Borssele PSA only.

PSA support of upgrade, backfitting and plant modifications (design review): In 1993 the first 10-yearly periodic safety review took place. At that time the PSA was not yet finalised. This resulted in a major modification program. Therefore, the new safety concept was mainly derived from a deterministic safety concept of the German Convoy plants. However the PSA could play a large role in the optimisation and evaluation of the deterministic safety concept, study of alternative solutions and in the license renewal (Environmental Impact Assessment). Examples of the use of PSA to study alternative solutions were: - second grid connection, and – turbo against electrical driven aux. Feed pump. The Modifications reduced the TCDF from $5.6x10^{-5}$ /year to $2.8x10^{-6}$ /year.

In 2003 the second periodic safety review took place. The PSA played an important role. All issues were weighed (Low, Medium and High impact) on the risk significance (TCDF and Individual Risk (IR)). Recently the licensee presented an improvement plan. For each echelon of defence-in-depth concept modifications have been suggested:

- installation of igniters and igniters at site boundary to counteract external gas clouds. Reduction of TCDF by 6% and IR by 54%.
- increase of DG oil supply in the bunkered systems from 24 hrs to 72 hrs leads to a reduction of TCDF by 20% and IR by 7%.
- improved seals of the low pressure ECCS pumps (TJ) lead to a reduction of TCDF by 20%.
- improvement of EOPs with regard to avoiding boron dilution of the primary circuit after start-up of the main coolant pumps.
- implementation of SAMGs for Low Power and Shutdown POS.

Assessment of Errors of Commission (EOC): In 1989 an IAEA IPERS/IPSART mission recommended to study EOCs. The Regulatory Body (KFD) transformed this into a requirement. The Licensee contracted G. Parry (at that time NUS, now US-NRC) and professor A. Mosleh (university of Maryland). This resulted in a study similar to the ATHEANA approach. Qualitative results; no direct quantitative results. For both Power POS and Low Power and Shutdown States several important EOCs could be identified

In the reports NEA/CSNI/R(98)1 (critical Operator Actions-Human Reliability Modelling and Data Issues) and NEA/CSNI/R (2000)17 (Errors of Commission in Probabilistic Safety Assessment) detailed information regarding this study can be found.

Change of Testing Strategy: The analogue signals of the reactor protection system of the Borssele NPP form mainly a 2v3 voting system. Via transmitters and comparators the measurements are continuously checked on deviations. All 3 channels of this system were once a year sequentially tested. Borssele made a proposal to test each year only one channel (staggered testing). PSA demonstrated that changes in CDF ranged from risk neutral to risk beneficial. The reason was that the dependencies in the calibration tasks could largely be reduced by staggered testing.

Method HRA: THERP
Probability of miscalibration 1 transducer P_0 = 1E-2
Dependency of sequential calibration tasks =

- Low dependency: $(1 + 19\ P_0)/20$
- Medium dependency: $(1 + 6\ P_0\ )/7$
- High dependency: $(1 + P_0\ )/2$

Complete dependency: 1

- Sequential testing + hard to verify results --> high dependency. Thus, probability of dependent failure due to decolourisation of 3 or 4 transducers = $1x10^{-2}\ ((1 + 10^{-2})/2) = 5x10^{-3}$.

Resolution of Hydrogen Issue: The PSA level-2 codes RELAP/MAAP and WAVCO (Siemens) calculations (PSA-level2) could not exclude that after core melt, despite the installed catalytic recombiners, in certain areas some small pockets of Hydrogen could be formed with a concentration near the detonation limit. Detailed CFD calculations (with RELAP/MAAP and WAVCO input) showed that active opening of the explosion windows inside the containment would prevent these pockets. Thereby, the Hydrogen issue can be resolved.

Exemption of Tech Spec: In 2002 the reserve cooling water pump TE (see figure 1) was found to be non-available. The TE pump is a special canned pump that can operate submerged (flooding in ECCS pump room). According to the Tech. Spec. the AOT was 8 days. After that, the plant should go to a cold shutdown state. A spare TE pump was not on the shelf. Borssele made a plea for an exemption to extend the AOT time. The request was accompanied with a PSA assessment. The assessment showed that under these circumstances the cold shutdown state had a higher risk level than the Power POS.

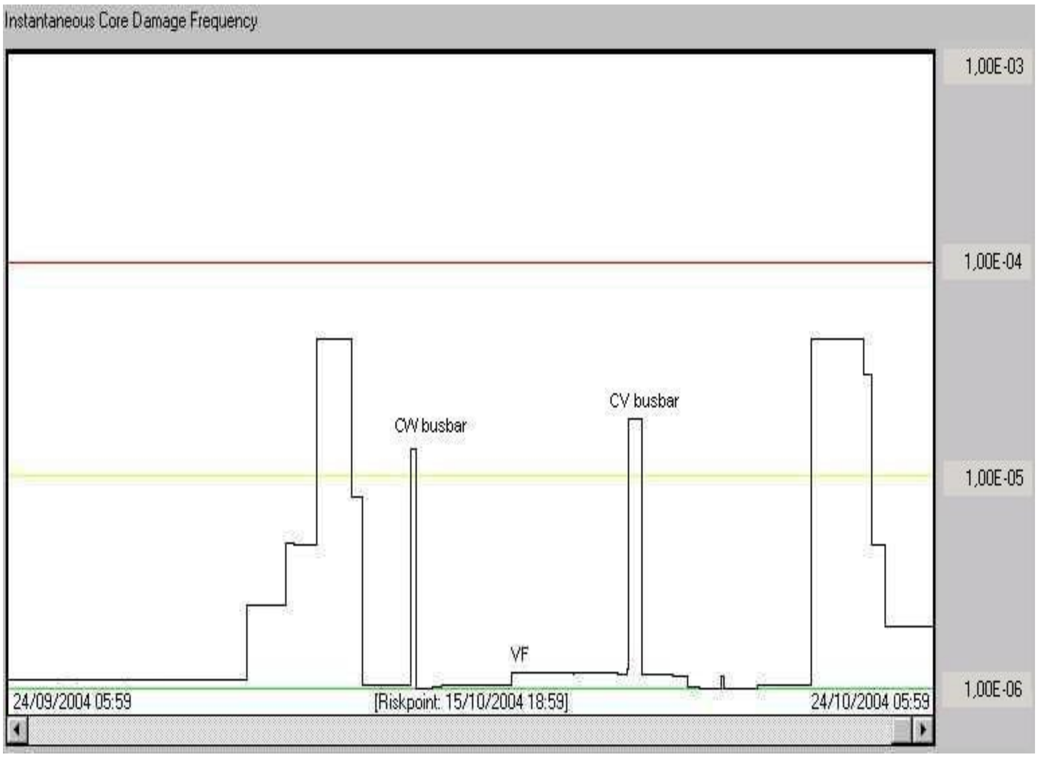
CDF Power POS = $1.1x10^{-6}$ /year
CDF Power POS + TE unavailable = $1.6x10^{-6}$ /year
CDF Power POS + alternate pump with 10 times higher failure rate =$1.15x10^{-6}$ /year
CDF cold shutdown POS = $1.0x10^{-5}$
CDF cold shutdown + alternate pump with 10 times higher failure rate =$9.9x10^{-6}$ /year

Regulatory Body agreed that Borssele didn't need to go to cold shutdown, but that an alternate spare pump should be installed in case the TE pump couldn't be repaired within the 8 days.

PSA supported SAMGs: The level-2 PSA demonstrated that SGTR events with a dry secondary side of the SG could cause the largest source terms and thereby, a large contributor to the public health risk (Source Terms up to 50% Cs and I). The most promising strategy was the scrubbing of the source term through the water inventory in the SGs. By installing extra pathways ways to keep the SGs filled (including flexible hose connection with the fire-fighting system) with water a factor 14 reduction in the magnitude of the source term (CsI and CsOH) could be achieved. Although, a closer look at the MAAP4 results showed that the major effect was not the scrubbing effect, but by deposition of fission products on the primary side of the SG tubes. This deposition effect plays also a large role in other core melt scenarios such as ISLOCA.

When core damage in ATWS scenarios cannot be prevented, opening of the PORVS is suggested. Loss of primary inventory is much faster, but creation of steam bubbles will stop the fission process. Also induced SGTR is less probable because of lower primary pressure. In case induced SGTR cannot be prevented lower pressure still helps. Opening of the secondary relief valves is less probable in that case.

Risk Monitors (Outage Planning & Configuration Control): In the figure below an example is given of the result of the outage planning for the refuelling outage in 2004.



One of the main objectives for the use of the risk monitor for configuration control is to minimise the TCDF increase as a result from planned component outages by:

- mastering simultaneous component outages
- rescheduling component outages with high TCDF impact in a certain plant operating state to an operating state where the component outage has a lower impact,
- reduction of duration of the refuelling outage.
- As a decision yardstick several numerical criteria have been developed by the licensee:
- the total cumulative TCDF increase caused by planned as well as unplanned component outages < 5%
- cumulative TCDF increase caused by planned component outages < 2 %.
- instantaneous TCDF shall never exceed the value of $1x10^{-4}$ /year.

Optimisation of Tech Specs: Recently Borssele has finished a project where the AOTs have been optimised. US-NRC Regulatory Guide 1.177 was partly taken as a basis. Borssele has modified the numerical criteria from this guide by lowering them with a factor of 10.

For optimisation of AOTs the licensee has adopted a value of $5x10^{-8}$ for ΔTCDF x AOT and ΔTCDF shall always < $1x10^{-4}$/year.

Apart from the PSA an expert team participated in the project to determine the maintenance times, repair times, whether or not spare parts were on the shelf, availability and duration of supply of components on the market, etc.

PSA Source Terms for off-site Emergency Planning & Preparedness: In case a severe event occurs at the plant with a serous threat for an off-site emergency, the 16 defined source terms in the PSA of Borssele are used as a standard source term for the prognosis.

For the definition of the planning zones for evacuation, iodine prophylaxis and sheltering the PWR-5 source term from WASH-1400 (Rasmussen Study) is still taken as the reference source term. However, the dose criteria for evacuation, iodine prophylaxis and sheltering will be lowered in the near future. As a result the planning zones would be significant larger. Therefore, a more realistic and Borssele Specific source term will be developed.

7.2.10 Mexico

During the development of the Laguna Verde PSA level 1 analysis and as a result of the high contribution of the station blackout scenarios (loss of offsite power plus the failure of the emergency diesel generators division I and II), a decision was made to implement a cross connection between the diesel driven pump of the fire protection system with the reactor heat removal system (RHR). This connection provides an alternative way to inject water into the reactor vessel or to spray the containment during this kind of accident.

A PSA application was submitted by the utility following the USNRC regulatory guide 1.174 to complement the deterministic analysis presented to support a plant modification request that involved the increase of the thermal power in 5%. The calculated increase in core damage frequency was $2.87x10^{-6}$ per reactor year. This increase is in the range of 10^{-6} per reactor year to 10^{-5} per reactor year. The regulatory guide establishes, in this case, that the application can be accepted if it can be reasonable shown that the total core damage frequency, considering internal events, external events, full power, low power and shutdown, is less than 10^{-4}. The IPE for Laguna Verde currently covers only internal events for full power operation. The contribution of the out-of-scope portions of the model was allowed to be addressed by bounding analysis, since significant margin exist between the calculated change in risk metrics and the acceptance guidelines. The application also covers the large early release frequency. The increase in this frequency was very small and therefore acceptable. The regulatory authority concluded that the application complies with the regulatory guide as well as with the key principles associated. These principles establish that the proposed change meets the current regulation, that is consistent with the defense-in-depth philosophy, that maintains sufficient safety margins, that the risk increase associated is small, and finally the impact of the proposed change should be monitored using performance measurement strategies.

Based on the USNRC regulatory guides, the CNSNS has assess and issued, for trial purposes, two Regulatory Guides, similar to the NRC/RG 1.174 and 1.177, which formally settles an approved methodology for using probabilistic safety assessment in risk informed decisions on permanent plant-specific changes to the licensing basis for Laguna Verde NPP and for Technical Specifications changes. These regulatory guides establish numerical safety criteria as in the NRC guides. Currently, the utility and the regulatory authority are engages in such PSA applications to support changes to the technical specifications of Laguna Verde NPP.

Due to the events occurring of Barsebäck-2 a Swedish BWR, at Perry Nuclear Plant a US BWR 6 and at Limerick a US BWR 6, the regulatory authority initiated a study to evaluate the contribution to Core Damage Frequency of ECCS strainer blockage due to LOCA generated debris at Laguna Verde NPP. The study included both deterministic and probabilistic analysis to evaluate the potential for loss of ECCS NPSH (Net Pump Suction Head) due to strainer blockage. The deterministic analysis was focused on determining whether or not a postulated break in the primary system of the Laguna Verde NPP results in ECCS strainer blockage and loss of NPSH. The probabilistic analysis was focused on evaluating the likelihood of ECCS strainer blockage and blockage-related core damage frequency from LOCA initiators. The ECCS original strainers were removed for new strainers, as well as improvements in the suppression pool clean program.

Laguna Verde NPP has a Risk Monitor to comply with the maintenance rule requirement established in the appendix (a)(4) of the 10CFR50.65, which states that the utility should assess and manage the risk associated with maintenance activities. Its models are being updated according and consistent with the approved and updated version of the PSA. The Risk Monitor for Laguna Verde NPP is limited to the full power operation mode and includes only internal initiating events.

The PSA results from the regulatory authority were used to prioritize inspection tasks. The use of risk-based information for inspection purposes started in the early 1995 with the development of plant specific risk inspection guides (RIGs). These RIGs provide the risk-based ranking of systems, components and operator actions. The RIGs along with the USNRC inspections and enforcement manual, the USNRC regulatory guides and the plant specific procedures are being used to set-up what it is referred to as improved inspection practices. The inspection teams have been trained in the efficient application of these practices in the field, and the RIGs are currently being used to focus the inspection effort to those aspects important from a risk point of view. Also, a procedure to link deterministic and probabilistic event evaluations, was developed with a view to an integral decision making process. Modifications of the NRC/SDP were performed to include in the event screening a flow chart instead of a questionnaire; the simplified PRA model was validated with the LVNPP IPE model.

Although there is no formal ordinance to apply the PSA to the examination of operators by the regulatory authority, the results of its Internal Event Analysis (Level 1 PSA), namely the main accident sequences, have been used to test the operator's ability response at the plant simulator. From the experience gained the utility has included PSA insights into their operator training program.

7.2.11 Korea

Many plant specific PSAs, which were finished according to severe accident policy, need to enhance the quality, therefore, they are in progress in order to gain more risk insights in the light of risk-informed applications. In addition, risk monitoring system is being installed to observe risk change due to test and maintenance activities. Because of these infrastructures for risk-informed regulation being established, PSA applications such as technical specifications optimization and risk-informed in-service inspection are actively performed.

The first risk-informed application project is the relaxation of surveillance test interval (STI) and allowing outage time (AOT) of reactor protection and engineered safety actuation system of Kori units 3,4 and Yonggwang units 1,2 which was performed in 1999. After that, several technical specifications optimization projects are launched and submitted to KINS, which are being reviewed. The following lists are past and current PSA applications projects:

<u>Relaxation of STI and AOTs</u>: This was done for the reactor protection and engineered safety actuation system of Kori units 3,4 and Yonggwang units 1,2:

- the test interval relaxation from 1 month to 3 month based on level 1 PSA insights
- risk increase by relaxation of STI and AOT is less than 2%
- KINS considers both risk insights and system enhancements such as hardware upgrade and circuit card test program

<u>Relaxation of STI and AOT</u>: This was done for the LPSI, CS, SIT, and EDG of Yonggwang units 3,4 and risk increase by relaxation of STI and AOT is less than 10% being reviewed by KINS.

Risk-Informed In-service Inspection for piping of Ulchin unit 4:

- Optimization of inspection points based on risk insights from level 1 and 2 PSA
- Reduction amount of inspection points is half of previous inspection points
- Be submitted to KINS in this year

ILRT(Integrated Leakage Rate Test) Interval Extension for Yonggwang units 1,2: the first phase of the overall project of containment ILRT interval extension based on risk insights from level 1, 2 PSA and population dose analysis the containment ILRT interval extended from 5 years to 10 years approved by KINS.

Safety Analysis for Containment ILRT Interval Extension: This was done for Yonggwang units 3,4 and Ulchin units 1,2,3,4 and Kori units 2,3,4. The second phase of the overall project of containment ILRT interval extension based on risk insights from level 1, 2 PSA and population dose analysis. The containment ILRT interval extended from 5 years to 10 years.

The application for Yonggwang Units 3,4 is approved by KINS. Other analysis report be submitted by 2007.

Turbine valve test interval relaxation: This was done for Yonggwang units 1,2 and Kori units 1,2. The satisfaction of safety target with respect to turbine valve test interval relaxation from 1 month to 3 month is shown through analysis of turbine missile probability with the operation and maintenance records and reliability analysis.

Risk-Based Inspection Program: The risk-based inspection (RBI) can be understood as an interim regulatory inspection scheme that, for the system and components important to safety, regulatory inspections are conducted more intensively and extensively whereas they are relaxed for the others. By doing so, we can utilize the regulatory resources in such manner that both the efficiency in regulation and the improvement of safety can be achieved.

A comprehensive RBI program has been under development since 1995 to improve regulatory inspection system in Korea. Up to now, two system risk-based inspection guides and two full plant risk-based inspection guides were developed and implemented to four operating units with a view to improving plant safety and tailoring the developed guides. The RBI guides have been developed based on plant-specific PSA results and operating experiences, so they can identify important inspection items in the order of risk significance (importance). It is also included the inspection insights and checklists derived from domestic and worldwide experiences in both operations and PSA results.

A significant number of safety-related findings have been identified by KINS inspectors through two times of special risk-based inspections at the sites and most of them have been voluntarily resolved by plant management and staffs. In addition, identified findings have been imparted to the other nuclear units with a view to investigating voluntarily and taking proper actions, if necessary. Moreover, in the light of these inspection results, the contents of risk-based inspection guides can be further improved.

7.2.12 Japan

Accident Management Strategies based on PSA: NSC issued the severe accident management policy statement in May 1992 as follows; Though the frequencies of core damage and containment failure due to severe accidents at Japanese typical NPPs are evaluated to be sufficiently small from an engineering perspective, NSC decided to introduce accident management based on PSA in order to further reduce plant risks, which does not directly lead to the licensing conditions for constructing or operating NPPs.

Based on NSC's decision, the competent regulatory authority Ministry of International Trade and Industry (MITI), prepared own policy on implementing accident management to cope with severe accidents, and in July 1992 strongly recommended and encouraged the owners of NPPs to take the appropriate measures to perform PSA and establish PSA-based accident management.

The utilities together with vendors conducted 43 level 1 and level 2 PSAs on each of all Japanese operating NPPs (Individual Plant Examination: IPE)(51 NPPs including several NPPs under construction). Since Japanese NPPs have been progressed in improvement and standardization and can be classified into several groups from the viewpoint of plant design and operation, their own accident management strategies have been fundamentally established for respective groups. Results of 43 PSAs were submitted to MITI at the end of March 1994.

MITI and the Technical Advisory Committee in support of NUPEC have executed the virtual review on the results of IPEs after the formal submission by the utilities at the end of March 1994. MITI and the Advisory Committee have approved the fundamental adequacy of the methodologies, database and results of IPEs from viewpoints of sate-of-the-art of PSA methodology and the recent objective of comprehensive and quantitative understanding for safety characteristics of individual NPPs in order to develop accident management program. The review report written by MITI was presented to NSC in October 1994. NSC reviewed and admitted it to be approvable in November 1995.

METI[5] has studied basic requirements in implementing AMs, taking expert opinions of Technical Advisors for Nuclear Power Generation into consideration, and in April 2002 issued the "basic requirements for implementing AMs" related to the following from a standpoint of securing the effectiveness of the AM as counter-measures to SA.

a. Implementation system for AM
b. Facilities and equipment, etc. related to implementation of AM
c. Knowledge base related to implementation of AM (procedures of actions which are deemed to be effective and appropriate to be studied beforehand)
d. Notice and communication related to implementation of AM
e. Education and training of personnel engaging in implementation of AM

Utilities have implemented AM (preparing the equipment for AM and preparing procedures related etc.) for operating and constructing NPPs. Implementation Reports for each NPP-site were submitted to METI in May 2002. The effectiveness of the AM on CDF and containment failure frequency were evaluated through level 1 and level 2- PSAs centering for eight typical NPPs, namely BWR3 with Mark-I containment vessel (CV), BWR4 with Mark-I CV, BWR5 with Mark-II CV, ABWR with ABWR CV, 2 loop-PWR with dry-type CV, 3 loop PWR with dry-type CV, 4 loop-PWR with dry-type CV and 4 loop-PWR with ice-condenser type CV. Some additional PSAs were also made for the plants with AM measures different from typical ones to evaluate effectiveness of AMs.

METI reviewed these AM Implementation Reports for 8 kinds of typical NPPs including the effectiveness of the AM measures on CDF and containment failure frequency (CFF) in an AMWG (Accident Management Working Group). NUPEC has also performed level 1 and level 2- PSAs for the above eight NPPs to support technical reviews by METI. Review Reports by METI was presented to NSC in October 2002 and review report by NUPEC was also issued in October 2002.

In March 2004, Implementation Reports on the remaining individual NPPs were submitted to NISA. NISA has reviewed the appropriateness of these reports, focusing attention on the differences from that of the typical NPP. JNES has supported NISA to make level 1 PSA for the particular NPPs. The review report will be submitted to NSC in near future.

---

[5] MITI was reorganized to METI in January 2001.

PSA in PSR: In Japan PSR is introduced as so-called voluntary measures for safety activities done by utilities under close deliberation with MITI, which requested utilities PSR in June 1992, in order to assess periodically (about every 10 years) and comprehensively the current situation of safety and reliability of each existing NPPs in the light of up-to-date technical knowledge.

In the first two PSRs, PSA was not included. In the third PSR PSAs conducted in 1994 to examine candidates for accident management were quoted without update. From the fourth PSR, PSAs were updated to take into account accident management measures prepared for its realization. Especially plant-specific AMs different from the standard AMs are taken into account in PSA. From the seventh PSR, PSAs for shutdown operation states were included to secure safety during shutdown operation. METI reviewed the PSAs for shutdown operation in PSR under the support of NUPEC, when the above procedures guide for probabilistic safety assessments of NPPs during shutdown conditions (AESJ-SC-P001:2002) was referred. The review reports were reported to NSC in August 2002.

PSA on Pipe Rupture of Steam Condensation Line at Hamaoka-1: While operating at rated power, on November 7, 2001, a pipe rupture occurred in the steam condensation line of the residual heat removal system at the Hamaoka Nuclear Power Station Unit-1 operated by the Chubu Electric Power Company, resulting in steam release with radioactivity into the reactor building and the high-pressure coolant injection being unavailable. The reactor was manually shut down immediately after the pipe rupture and there was no radioactive release into the environment.

NISA formed the task force on November 9, 2001 in order to identify event causes and examine corrective actions for preventing recurrence. NISA requested the Chubu Electric Power Company to perform the investigation of this incident including the event causes and to report the results. In order to perform the investigation independently from the Chubu, the Agency asked the Japan Atomic Energy Research Institute (JAERI) to carry out metallurgical examination and analysis of the pieces taken from the ruptured pipe section and NUPEC to analyze the mechanism that might have led to the pipe rupture and the risk significance of incident and corrective actions to be taken from the viewpoint of core damage frequency (CDF). On May 13, 2002, the Agency issued the report that describes the investigation results including the event causes identified, the Agency's positions and lessons learned.

The emphasis of risk analysis by NUPEC was concentrated on evaluating risk significance of corrective actions to be taken not only in Hamaoka Unit-1 but also BWR-4 and -5 plants with the same steam condensation line as Hamaoka Unit-1. The risk analysis by NUPEC concluded that the three corrective actions are acceptable from the viewpoint of risk. The evaluation of incident and corrective actions with PSA is attached in appendix 1, exerted from 'Investigation Report on Pipe Rupture Incident at Hamaoka Nuclear Power Station Unit-1.

Evaluation of Allowed Outage Time (AOT) based on PSA: In Japan the technical specifications in NPPs have been required to be made detailed with accountability and transparency especially since JCO accident. Japanese utilities now have revised the technical specifications as detailed as those in Standard Technical Specification of USA. In the process of the revision the applicability of level 1 and 2 PSAs has been pursued in both utilities and NUPEC in order to have the accountability and the transparency of setting up AOTs for the safety systems with redundancy. NUPEC, under the sponsor of METI, has estimated incremental conditional core damage probabilities (ICCDP) and incremental conditional large early release probabilities (ICLERP) during AOT for Japanese BWR and PWR, using level 1 and 2- PSAs. The effects on ICCDP of surveillance tests, conducted for the remaining system during AOT, are taken into account. Allowed ICCDP should be essential to setting up AOT using PSA. The allowed ICCDP was provisionally set up taking into account ICCDP under the current technical specification, ICCDP for outage experiences, ICCDP during manual trip and the conceivable safety goal.

BWR sump strainer blockage: A large amount of unexpected foreign material that could induced the potential strainer plugging for ECCS pump suction water source in the containment vessel had been found at domestic BWR plants. Then the regulatory authority required all BWR licensees to evaluate effectiveness of ECCS pump suction strainer installed in pressure suppression pool in containment vessel in 2004. At that time licensees had been required to plan tentatively-revised operation procedure to mitigate the impact of the strainer plugging until permanent improvement of the components was going to be determined and implemented, and had applied PSA as one of the validation for the revised procedure. JNES had implemented PSA independently and compared with the results of licensees, based on the proposed revised-procedure by licensees, and the impact on the core damage frequency due to the revised procedure had been evaluated quantitatively. These results had been applied to approve the revised procedure as reference by the regulatory authority.

Implementation Plan for utilization of risk information in nuclear safety regulation: According to the Basic Concept, NISA, in collaboration with JNES, developed Near Term Implementation Plan for utilization of risk information.

The Near-Term Implementation Plan was developed according to the Basic Concept of Risk Information in Nuclear Safety Regulations to cover the range of regulation activities in NPPs. The Implementation Plan will finally cover all types of nuclear facilities that NISA is responsible for regulation, however, the Near-Term Implementation Plan was mainly focused on the regulations of NPPs. Items in the Near-Term Implementation Plan were selected based on the criteria (see below) in the Basic Concept and the current status of PSA technique, reliability database development and practicability. Through this implementation plan, NISA and JNES would accumulate the experiences of PSA usage in the decision making of regulation. The Implementation plan will be modified according to the accumulation of experiences, advancement of PSA techniques and reliability database development, change in needs of nuclear industries and so on. The Near-Term Implementation Plan was accepted through public comments in May 2005.

The items in the Near-Term Implementation Plan were selected using following criteria:

(A) Items which could improve the rationality of the safety regulation and contribute to realize the effective and efficient regulation, without impairing the total safety level of a nuclear power plant.

(B) Items of which PSA methods and database needed are already developed or will be developed in relatively short term, and which have the adequate quality to support the risk informed application.

(C) Items of which application can be implemented within the reasonable resource for regulatory agencies, utilities and/or the public.

(D) Items which have no factor other than the above that considerably restricts the implementation of the risk informed application?

If the items comply with these criteria, they are selected as the application items of the Near-Term Implementation Plan. The Plan covers items listed in the following.

a. Design & Construction Area
    - Evaluation of the adequacy of SSCs (structure, system and components) that are subjected to the approval or notification of a construction plan
    - Recommendation of the voluntary safety upgrade activities for seismic PSA by the utilities
b. Operation & Inspection Area
    - Review related to the introduction of online maintenance
    - Evaluation of the adequacy of the requirements in the Technical Specification
    - Evaluation of the adequacy of SSCs that are subjected to inspections
    - Review the role of the PSA to be carried out in PSR
c. Accident & Emergency preparedness
    - Review the expansion of the scope of AM for LP & SD operation
    - Evaluation of Accident Sequence Precursors

d. Technical Infrastructures
  - Advancement and Sophistication of PSA methodologies for performing a plant specific PSA reflecting the operating experience and the characteristics of plants including plant degradation, reliability analysis of digital reactor protection system, internal fire events and flooding events PSA.
  - Reliability database development that reflects the Japanese operating experiences.

7.2.13 Italy

No information provided.

7.2.14 Hungary

The PSA models and results for Paks NPP have been used in a number of PSA applications ever since the completion of the first level 1 PSA study for unit 3. Both utility and regulatory activities have been supported by these applications. The most important PSA applications initiated by Paks NPP have been as follows:

- development of recommendations for safety improvement,
- prioritisation of measures for safety improvement included in the safety upgrading program for Paks, most of the modifications have been scheduled in accordance with that priority,
- use of PSA during design and implementation of plant modifications,
- case study demonstration of PSA based revision of technical specifications,
- PSA based review of operator training at Paks simulator.

Development of unit specific risk monitors and tools for analysis of precursor events to severe accidents and development of a special risk monitor to be used for risk prediction by the nuclear regulatory authority in an emergency were initiated by the Nuclear Safety Directorate of the HAEA in 1995. The objectives of the precursor event analysis program using probabilistic methods are as follows:

- determination of the risk significance of the operational events on different levels of risk (e.g. core damage, system/component unavailability, etc.), identification of the most significant ones and their ranking,
- early signalisation of negative trends in performance,
- drawing conclusions based on the impact of the operational events,
- feedback to the PSA model and data used.

A computerised tool has been developed and used for the precursor event analysis. The Licensee Event Reports are evaluated quarterly and the summarised results are used as risk based indicators of operational safety at the Paks NPP.

Since the start-up our units undergo a continuous upgrade process. This is why the systematic PSA based change analysis that supports this upgrade process has became the most important PSA application. According to the regulatory approach, it should be proved that each modification preserves or increases the safety level. In order to gain the most complete insights not only deterministic principles but also probabilistic evaluations are systematically undertaken for any significant plant changes or any significant considerations of additional initiators or any significant considerations of other plant operational modes. In the justification of the plant modifications is a tendency to show that the calculated overall risk impact (in terms of core damage probability change) is negative or at least negligible. In many cases designs of the plant modifications have been optimised based on calculated risk characteristics.

The overall risk figure for internal events has been decreased by an order of magnitude during the last five years. Safety improvement has been achieved during full power operation and during low power and shutdown conditions as well. The PSA has quantitatively shown that this considerable risk reduction can be attributed to the safety enhancement measures that have been implemented at Paks up to now.

The other important application of PSA is supporting Periodical Safety Review required by our nuclear authority. These periodical reviews held after 10 years of operation offer the possibility – and obligation for the licensee – to perform a comprehensive assessment of the safety of the plant, to evaluate the integral effects of changes of circumstances happened during the review period. The goal of these reviews is to deal with cumulative effects of NPP ageing, modifications, operating experience and technical developments aimed at ensuring a high level of safety throughout plant service life.

A set of unique PSA applications were carried out to support recovering from the consequences of the ex-core fuel damage event at Paks in April 2003. The core damage risk and the necessary risk reduction measures associated with a special long lasting shutdown operational state of unit 2 was determined by PSA. PSA also helped to choose from among three design alternatives of a so-called autonomous cooling circuit that was designed and constructed to enable a full separation of the service pit from the adjacent spent fuel storage pool so that safe and stable cooling of water in the pit could be ensured. Probabilistic analysis was performed to determine the probability of heavy load drops and other malfunctions during irregular fuel handling operations when the service pit cannot be normally used.

7.2.15 Germany

In Germany there is no formalized approach to apply the results of PSAs to be performed for all NPPs. It is up to case-by-case decisions of the regulatory authorities how to apply the PSA insights. In practice, safety deficiencies from design and operation, identified by a PSA, are discussed between the utility, the regulator and expert organizations, acting on behalf of the regulator, in order to make decisions on backfitting and upgrading measures.

There is no unified approach of the utilities how to apply PSA insights for decision making on operational issues.

The analysis of plant operational events by using PSA has been integrated in the operational experience feedback process in Germany supplementing the deterministic analysis of operational events.

7.2.16 France

<u>Use of PSA for reducing the risk related to dominant contributions</u>: Historically the first PSA applications had the objective of reducing the risk related to dominant contributions. A first example was the implementation of specific measures (procedures and additional equipment) aiming to cope with the loss of redundant systems.

The high contribution of shutdown situations in the 1990 PSA results led to several plant safety improvements, for example:

- A dominant sequence was related to a loss of heat removal system due to an excessive draining of the primary circuit during mid-loop operation. Several safety improvements were implemented to reduce the risk related to this sequence: e.g. modifications of the Technical Specifications, of the Emergency Operating Procedures, implementation of a supplementary level measurement in the primary loops, of a vortex signal, and of an automatic water make-up.

- Another problem underlined by PSA results was the risk of heterogeneous boron dilution which could lead to a reactivity accident. The solution includes a certain number of automatic processes and improvements of operating procedures in normal or emergency situations.
- The probabilistic analysis highlighted a risk of cold overpressure in the primary circuit, in case of inadvertent isolation of the heat removal system when the primary circuit is closed and monophasic. On the basis of PSA evaluations, modifications were decided concerning the EOPs and the set point of the pressurizer safety valves.

Use of PSA for Periodic Safety Review: The periodic safety review procedure, applicable to existing reactors, is a periodic process implemented for a given reactor type, which incorporates recent operating experience and updated knowledge.

In the first step, the periodic safety review procedure aims to demonstrate the conformity of the “reference plant situation” with the “safety reference system”. The “safety reference system” consists of all the safety rules, criteria and specifications applicable to a reactor type resulting from the safety analysis report. The “reference plant situation” consists of the state of the installation and its operating conditions.

In the second step, the safety reference system is assessed. The assessment is based on an analysis of national or international operating experience or on special studies, and on examination of the provisions adopted on the most recent reactors.

In application of the general procedure, PSAs are used during the periodic safety review to assess the core damage frequency and its change compared with the assessment made on completion of the previous review, including an analysis of the changes in system characteristics (equipment reliability, for example) and in operating practices.

In addition, identification of the main contributions to the core damage frequency highlights any weak points for which design and operation changes can be studied, or even judged necessary. They can be ordered so as to target the priority work.

During the second 900 MWe Periodic Safety Review (first use of PSA in Periodic Safety Review), the main following backfits were required by the Safety Authority:

- Functional redundancy of AFWS for all modes of operation (by MFWS or RHRS)
- Improvement of the ventilation system
- Diversification of the reactor scram function
- Modifications which could mitigate the consequences of 6.6 kV switchboards common cause failure (improvement of SG feedwater and of RCP seals injection functions).

For the second 1300 MWe Periodic Safety Review, PSA was used with a more formal method. For the purpose of the more recent PSR of the French plant series, the EDF reference PSA model is used according to a new methodology. In that process, the risk is no longer distributed in accident families, but in functional sequences, which are characterized by the ultimate measure (equipment or operator action) preventing the core degradation.

The method allows plant modification ranking according to their impact on safety. The main findings of this review were a follow-up of the control rods reliability, and modifications which could mitigate the consequences of 6.6 kV switchboards common cause failure (improvement of RCP seals injection functions).

Recently the third 900 MWe Periodic Safety Review was carried out, and the use of PSA was increasing with the introduction of PSA level 2 and of Fire PSA. The EDF proposals were analysed by IRSN on the basis of its own studies. The findings of level 1 PSA are that the results do not lead to particular requirements, but some sequences and systems need supplementary investigations (ISLOCA, heterogeneous dilution, Containment Spray System).

The Fire PSA identified two sensible rooms (containing electrical equipment), and improvements are studied.

The level 2 PSA, for which it was the first use in Safety Analysis, led to the following remarks:

- The overall LERF is not a sufficient criterion to appreciate the safety level and to identify potential weak points. Analysis of the dominant contributions of « functional sequences » has also to be carried out.
- Some necessary studies and potential improvements have been identified (example: implementation of iodine filtration in the containment venting system…)
- Several aspects of the reference PSA have to be completed or revised.

<u>Use of PSA for Beyond Basis Design Accident</u>: In Safety Analysis Reports of EDF NPP, the existing Beyond Design Basis Accidents (BDBA) come from a historic and conventional list of events, and are studied to according deterministic rules similar to Design Basis Accidents, but without margins or single failure criteria. A PSA-based methodology was developed at EDF to provide a renewed list of BDBA, and to define the representative scenarios to be studied for each of the accidents retained. IRSN analysed the proposal and the Safety authority accepted the principles of the method in 2002. Applications of this methodology, based on the 900 and 1300 MW PSA, have led to new lists of Beyond Basis Design Basis Accidents in SAR. Assessment of the results of the corresponding transient studies have been completed with the reference PSA model and sent by EDF to the French Safety Authority.

In 2004 and 2005, the results of this application have been discussed by EDF and IRSN

<u>Probabilistic analysis of Operating Events</u>: The probabilistic analysis of operating events, which occur in the plants is on going, by EDF for all the events, and by IRSN for some representative examples.

An operating event is considered as a Precursor when the conditional CMF (Core Melt Frequency) due to this event is higher than 10-6 /reactor/year. Moreover the Safety Authority has required from EDF, for the most important events (conditional CMF higher than 10-4), to define, in a short term, corrective measures and to assess the corresponding risk reduction.

EDF has been performing a systematic PSA-based precursor event analysis program since 1993. This analysis consists firstly in using deterministic methods in order to select main events to be analyzed. Secondly, the outstanding events are analyzed using PSA models in order to imagine and assess degradation scenarios. It led in 2005 to a certain number of Precursor events.

With this approach, the potential consequences of event are highlighted and corrective actions are adapted to their importance. The results of the event analysis program are periodically presented to the French Safety Authority.

<u>Other PSA applications for operating plants</u>: PSA insights were used for several improvements of plant operation (Technical Specifications, Emergency Operating Procedures, Maintenance Optimisation….)

Moreover, PSA is often used in day to day safety analysis as a complement to deterministic analysis for decision making, for example in case of technical specifications waiver authorisations.

In 2004, EDF developed and formalised a safety cost/benefit evaluation approach for the third PSR of the 900 MWe PWR units and was presented to the Standing Advisory Committee for Nuclear Reactors in 2005. Using this approach the safety gains can be ranked according to the resources mobilised to achieve them. About forty modifications have been evaluated in this way. The approach consists in evaluating all the costs of a modification (direct costs of defining and implementing the modification, plus indirect costs: negative or positive impacts on unit availability, maintenance costs, etc.) and the safety benefit(s) brought by the modification using PSAs. This approach is presently analysed by IRSN and by the regulators.

PSA application to plants at the design stage: As for the operating reactors, demonstration of the safety of the design of future reactors is based on deterministic studies. For the new generations of reactors, PSA is used as a supplemental tool in safety assessment during the design phase.

For the future EPR plant safety analysis, the place of PSA is increasing. The French and German regulators, during the preliminary discussions about the EPR project, agreed upon Safety Objectives (see section 3):

A CMF reduced compared to existing plants

"Practical elimination" of sequences which could lead to early releases. If these sequences are not physically impossible, they have to be designed out.

In the design phase, a minimal reference PSA is required covering all the accident situations of internal origin which, in view of the PSAs conducted on operating reactors, are considered to be important for safety. During the design of future reactors, PSAs are developed in consecutive steps throughout the reactor development cycle: they are enriched as the design studies advance.

For the EPR project a PSA has been performed since the early beginning of the design, starting with simplified assumptions. This preliminary PSA indicated the importance of Common Cause Failures and of support systems, and led to several design improvements.

A more complete assessment was provided by EDF for the French EPR safety report in March 2006. This PSA covers internal events and level 1+ and is presently analysed by IRSN. It will be extended and updated during further steps.

7.2.17 Finland

Applications for a Construction Licence: The applicant for a construction licence for a new plant unit has to submit level 1 and 2 design phase PSA to STUK. One purpose of a design phase PSA is to ensure that the plant safety is in compliance with the numerical design objectives. In addition the licensee has to indicate by means of the design phase PSA that the foundation of the plant design is fit and the design requirements used are adequate. This concerns especially events like harsh weather or other exceptional environmental conditions and seismic events, the frequencies and consequences of which may comprise large uncertainties. Further the safety classification of systems, structures and components has to be assessed by the help of PSA. The probabilistic review of the safety classification has to be submitted to STUK in conjunction with the safety classification document. The safety classification document is an integral part of the application for a construction licence to be submitted to STUK.

STUK will review the design phase PSA and makes an assessment of the acceptability of the design phase PSA prior to giving a statement about the construction licence application.

TVO submitted the OL3 EPR design phase PSA to STUK in conjunction with the application for the construction licence.

Applications for an Operating Licence: The applicant has to submit level 1 and 2 construction phase PSA to STUK at the latest in conjunction with the application for an operating licence. The purpose of the level 1 and 2 construction phase PSAs is to ensure the conclusions made in the design phase PSA on the plant safety and to set a basis for the risk informed safety management during the operation phase of the plant.

The balance and coverage of technical specifications must be reviewed by the aid of PSA. The review must cover all operating states of the plant. Especially such failure states, in which the change of operating state of the plant may result in a greater risk than the repair of the plant during operation, should be reviewed with PSA. The results of review must be submitted to STUK in conjunction with the application for an acceptance of technical specifications.

The insights from PSA must be applied in the review of safety classification as in the design phase if extensive changes are performed in the plant design in the construction phase. Further, the results of PSA must be applied in the drawing up of programs of safety significant systems testing and preventive maintenance during operation, and in the drawing up of disturbance and emergency operating procedures.

The insights from PSA must be used in the drawing up and development of the inspection programs of piping. Combining the information from PSA and the damage mechanisms of pipes and the secondary impacts of damages, the inspections are focused in such a way that those are weighted on those pipes whose risk significance is greatest. While working up the risk informed inspection program, the systems of safety classes 1,2,3,4 and non-code must be regarded as a whole. Similarly how far the radiation doses can be reduced by focusing inspections and optimising inspection periods must be regarded.

STUK reviews the construction phase PSA before giving a statement about the operating licence application.

TVO in cooperation with Framatom ANP is in progress of conducting the aforementioned PSA applications for the operating licence of OL3 EPR.

Applications for Risk Informed Safety Management during Operation: The licensee has to prepare and to regularly update the level 1 and 2 PSA to correspond to the operating experience. In addition, the PSA model must be updated always when a substantial change is made in the plant design or in the procedures or when a new substantial risk factor is found. The licensee has to provide the PSA model in computerised form to the use of the regulator. The licensee has to maintain a database of the reliability of safety related components, initiating events and human errors. STUK reviews the updates of PSA and evaluates their acceptability.

Living PSA models have been developed for both the Olkiluoto and Loviisa NPPs. The PSA studies include level 1 and level 2 models. Level 1 comprises the calculation of severe core damage frequency (probability per year) and level 2 the determination of the size and frequency of the release of radioactive substances to the environment. At the moment, level 1 studies for full power operation cover internal events, area events (fires, floods), and external events such as harsh weather conditions, and seismic events. The shutdown and low power states of level 1 PSA cover internal events and some area and external events. The Level 2 studies include internal initiating events, flooding and harsh weather conditions in full power state.

Plant changes: PSA insights have to be applied to the upgrade of safety and to the manifestation of needs for plant changes and to the evaluation of their priority. Accordingly the licensee has to submit to STUK a probabilistic assessment of the impact of the change on the plant safety in conjunction with the preliminary inspection document. A proposal for a safety class has to be submitted to STUK in conjunction with the preliminary inspection document of a system modification. In conjunction with extensive changes concerning whole systems, the safety class has to be re-evaluated with PSA as in the design phase.

PSA has got an important role in the evaluation of needs for plants modifications of operating plant units. The licensees have provided STUK with the assessment of safety significance of each proposed modification. The risk assessment has to be submitted to STUK independent of the safety class of the systems to be changed. For example, in the course of past several years the estimate of the core damage frequency of the Loviisa plant has decreased with a factor of ten thanks to the plant modifications

Technical Specifications: The insights from PSA must be applied to the assessment of needs for changes in the technical specifications in conjunction with extensive plant changes in a corresponding way as in the construction phase. In the same way, the needs for the changes of technical specifications must be evaluated if new unidentified risk factors are found. Further, the PSA has to be used for identifying such situations in which the plant shut down may cause higher risk than continuing power operation and fixing the failures. The preliminary inspection document for a plant modification should include a preliminary proposal for the change of Technical Specifications.

Certain inconsistency of AOTs in comparison with the respective risk impact has been identified between various safety systems. Risk assessment has also questioned the traditional conclusion that in all faulted states the shutdown of the plant would be the safest course of action. If systems used for decay heat removal are seriously degraded (CCF), it may be safer to continue operation than to shut down the plant immediately, although shutdown may be required by the current Technical Specifications. Hence the licensees has to re-evaluate the relevance of allowed outage times (AOT) of most important front line safety systems and to figure out those failure states of the plant when it is safer to continue operation than to shut down the plant immediately.

Exemption of Tech Specs: If a licensee applies for an exemption of Tech Specs the licensee has to submit a risk analysis to STUK and indicate that the risk from the exemption is tiny. STUK reviews the licensees´ analysis and makes its own risk assessment for comparison as necessary. The licensees have applied for an exemption of Tech Specs typically two or three times a year.

Condition of systems, structures and components: PSA can be used to effectively optimize the test intervals and procedures of those components and systems which contain the major risk reduction potential. PSA can also be used for the identification of potential failures and common cause failures.

The testing program of safety significant systems and components which is set forth in context of technical specifications must be argued by the aid of risk assessment and the results of analysis have to be submitted to STUK for information. The testing program must be regularly evaluated on risk basis during operation of the plant.

The on-line maintenance of safety significant systems and components is allowed during operation in accordance with the restrictions set by technical specifications. If the preventive maintenance would be performed during operation, an estimate of risk significance of preventive maintenance must be presented.

STUK accepts on-line preventive maintenance during power operation provided that the deterministic safety criteria are fulfilled (e.g. single failure criterion) and the risk contribution is small. According to the first Olkiluoto PSA study in 1989, the risk contribution of on-line preventive maintenance was about 5 % of the total core damage frequency. When the maintenance schedule was optimised with PSA, the risk contribution of on-line preventive maintenance could be reduced to less than 1 % of the total core damage frequency.

The insights of PSA must be used in the working up and development of the inspection programs of piping as per guide YVL 3.8. While drawing up the risk informed inspection program, the systems of classes 1,2,3,4 and non-code must be regarded as a whole. Similarly how far the radiation doses can be reduced by focusing inspections and optimising inspection periods must be regarded.

Pilot projects on in-service inspections of piping both in a pressurized water reactor plant (Loviisa) and a boiling water reactor plant (Olkiluoto) have been completed by STUK in cooperation with the licensees. STUK's risk-informed procedure combines both the plant specific PSA information and the traditional insights in support of the system specific detailed in-service inspection program planning. Finnish licensees are in progress of risk-informing their in-service inspection programmes. RI-ISI approach is used also in the context of the on-going EPR project.

Reporting of operating events: The new regulatory guide YVL 2.8 does not require the licensee to set up a special program for analysing operational events with PSA techniques. Instead the licensee has to provide qualified information of the operational events and submit the information to STUK. STUK performs the PSA based event analyses itself.

In the area of operational events, PSA is a standard tool to assess the safety significance of component failures and incidents. Today risk follow-up studies are a common practice at STUK. Since 1995 STUK has performed systematic risk follow-up studies on the annual basis for each Finnish nuclear power plant unit.

Disturbance and emergency operation procedures: In order to ensure the coverage of disturbance and emergency operating procedures PSA must be used to determine those situations for which the procedures shall be drawn up. Accordingly, should shortages in the coverage to be appeared, the licensees have to write new Emergency Operation Procedures (EOP) to provide guidance for operators to better manage certain accident sequences which the PSA indicated to be of high importance to risk.

Personnel training: The results of PSA must be taken into account in the planning of personnel training. The most important accident sequences and significant operator actions in terms of risk have to be trained at least in the period of three years which is used in the planning of training of control room crew. In the planning of maintenance crew training, attention needs to be paid to risk significant measures which are identified in context of PSA. STUK evaluates the training programs of the personnel *inter alia* in context of the inspection program of operation control.

Data and methods to be used in PSA applications: In the design phase PSA, operating experiences collected from similar plants or corresponding applications shall be used. As to the PSA of an operating plant, the plant specific data and if necessary, combined with data received from other similar plants or corresponding applications have to be used. In the absence of such a data, general data shall be used. The feasibility and uncertainty of the data has to be justified.

Provided that no adequate design, site and reliability data are available for the design phase PSA or if some safety related systems are constructed using a technology such that there are no well established methods available for computing the system reliability estimate, one can replace the missing data with expert judgment, experiences and information from corresponding applications and corresponding sites. In that case the estimation procedure must be justified and the uncertainties associated need to be studied and documented. The methods used in PSA have to be demonstrated.

Quality management: The licensee has the responsibility of the drawing up, maintenance and application of PSA. Accordingly, the licensee shall prepare guidelines for the working up and application of PSA which includes the responsibilities and acceptance procedures associated with PSA, references to PSA procedures guides and procedures for PSA applications. In addition, corresponding guidelines need to exist for the maintenance of PSA computer program, handling of errors and flaws, dealing with changes, time schedules for update, internal review and acceptance, documentation and submission to STUK. The licensee must submit the aforementioned guides to STUK for information. The licensee has to keep account of changes made in the PSA model and data, reasons for the changes and impacts on PSA results and to submit this information to STUK with the updated PSA.

Risk -Informed Regulatory Inspections

STUK is in progress of training inspectors to understand and use the PSA insights while planning the regulatory inspection programs and conducting the inspections at site. A special PSA Info system has been developed in order to use the insights of PSA for training the inspectors, to upgrade their risk perception and to demonstrate the importance of most significant accident sequences.

7.2.18 Czech Republic

Level of use of PSA applications is dependent on PSAs status and scope, particular NPPs needs and objectives, on Regulatory body requirements and PSA policy. In the Czech Republic several types of PSA applications have been in use.

Evaluation of modifications: At Dukovany site there is a systematic process with aim to decrease units risk level and therefore PSA is permanently used for identification of weak points, evaluation of design and procedures modifications and improvements, comparison of alternatives and making priorities for implementation of safety measures.

A lot of safety improvements have been made in Dukovany since 1991 and PSA insights have helped significantly in this still ongoing systematic process, which helps in Dukovany achieve a comparable risk level of WWER unit with “western” design. [21]

At Temelin a comprehensive safety improvement program has been started before 1989 by the identification of potential design vulnerabilities list and it has been substantially extended following 1990 -1992 through various safety audits conducted either by nuclear safety consultant companies, by the IAEA, GRS, WENRA, etc. or in the frame of bilateral relationship.

Evaluation of Technical Specifications: NPP Dukovany raised an issue of TS (Technical Specifications) acceptability in 2000 when the plant enhanced its TS to match the modern TS format. A broad spectrum of Limiting Conditions for Operation (LCO) was evaluated in UJV Rez using PSA model for NPP Dukovany to determine the risk associated with an Allowed Outage Time (AOT) on full-power operation. The results were then used as a support to submittal of enhanced TS for the licensing. Most of the results were later recalculated using PSA model updated with new plant modifications. The evaluation was also extended to all plant operating modes where the particular LCO was applicable.

Along with that, further studies were performed to find the possibility to grant some AOTs for outages of redundant components. New results were again used as a support to TS submittal for the licensing of some AOT extensions. Feasibility of TS changes necessary to allow relocation of scheduled maintenance from refueling outage to power operation was evaluated in UJV Rez using current PSA model for NPP Dukovany as well. [22]

The evaluation of AOT risk was based on single-event AOT risk comparison with fixed criterion as described e.g. in NUREG/CR-6141, or RG 1.177 respectively:

$$\mathrm{ICCDP} = \Delta\mathrm{CDF} \times \mathrm{AOT} < 5 \times 10^{-7}$$

$$\mathrm{ICLERP} = \Delta\mathrm{LERF} \times \mathrm{AOT} < 5 \times 10^{-8}$$

The values 5×10^{-7} for ICCDP and 5×10^{-8} for ICLERP were taken from RG 1.177 and they have been used exclusively in the recent calculations.

For the Czech Regulatory Body (SUJB) UJV Rez provided a technical support for SUJB to develop a methodology guideline for the more comprehensive evaluation of TS changes or adequacy. It is based on three-tiered approach from RG 1.177 and utilizes also RG 1.174 criteria.

The risk-informed evaluation of TS should include the following considerations (tiers):

1. Insights from PSA
2. Avoidance of Risk-Significant Plant Configurations
3. Risk-Informed Configuration Management

This three-tiered-approach has been used by UJV PSA department in the recent evaluation of those TS changes in NPP Dukovany that are necessary to allow on-line maintenance at power operation, namely permanent service water system AOT extension from 3 to 15 days.

Based upon the PSA evaluation, the Czech Regulatory Body (SUJB) approved a temporary (time limited) increasing of AOTs for safety systems at Temelin from 3 to 12 days. This allowed to perform safety system necessary maintenance during plant at power operation, thus decreasing plant outage duration when doping safety system division maintenance during shutdown. PSA team provided risk informed evaluation of any configuration occurred during the safety system outage, to confirm that SUJB defined criteria were not exceeded by any real configuration.

So far, the Temelin PSA is used for probabilistic support of risk informed AOT change request. For the risk informed AOT application, RG 1.174, RG 1.177 methodology and acceptance criteria have been adopted.

<u>Event Sequence Analysis</u>: The analysis of operational events using PSA has been integrated in the operational experience feedback process at Temelin. The objectives of the Precursor Analysis precursor program are mainly focused on the determination of the quantitative importance of selected operational events per year, as a common basis for discussions on actual event safety significance with regulatory body and on the subsequent identification of potential safety issues for improvement. So far, three selected operational transients during the plant commissioning and afterwards (*2002, 2003, 2004)* were assessed to evaluate the impact of such events to the risk margin. Similar activity has also been organized under regulatory project for Dukovany plant and selected events were evaluated.

<u>RI-ISI</u>: RI-ISI has not been formally applied for the Czech NPPs so far; however there is a pilot activity ongoing at both sites. The project is focused on selected parts of primary loops piping at Dukovany and on steam and feedwater lines at Temelin site. The pilot projects are based upon the EPRI methodology for RI ISI.

<u>Operational Risk Monitoring</u>: In order to provide a risk model for daily use by the other technical staff at the plant, the original PSA project has been extended, and the risk model developed within the PSA was transferred to a real-time risk calculation software analyzing both real and scheduled plant conditions for determining the impact of plant configurations on operational risk level - Risk Monitor.

The major purpose of the Safety Monitor is the ability to provide an on-line risk measure based on the current plant configuration, on-line preventive/corrective maintenance or testing status, so enabling plant staff to plan and perform maintenance activities in such a way that safety is maximized, and at the same time unnecessary plant shutdown is avoided. The risk level in the manner of either CDF or LERF (full power only) associated with that specific configuration is then calculated within the software and displayed on a meter. The meter shows four risk operating bands, acceptable, low, warning and high. At the same time a suggested allowed configuration time associated with that risk level is displayed on the screen.

The Safety Monitor models for both at power and shutdown states are available to the end users through the Safety Monitor ver. 3.5 (CZ) software installed in the plant LAN environment TEMNET since 2003 and DUKNET 2002 respectively. The implementation of new 3.5a version of Safety Monitor software at the plant LAN was performed to enable on-line use of the risk-monitoring tool by various plant staff. In such manner, through the Safety Monitor, the PSA becomes a tool for active influence on operational risk level without detailed knowledge of PSA techniques and terminology, at the same time providing means to optimize safety within Technical Specifications constraints, planned maintenance activities and storing history of plant configuration changes and component outages with associated risk levels.

The particular unit specific PSA models of NPP Dukovany were developed and are periodically updated to reflect all major modifications (both technological and procedural), new findings and PSA practices. All those improvements are subsequently converting into the Safety Monitor. Moreover the continual enhancement is done in each of these steps (usually once a year), [23].

In order to bring the risk monitoring to everyday configuration follow-up at control room the effort is currently undertaken to provide Safety Monitor with semi-on-line data input from existing databases and planned CR electronic log.

Risk Monitor is also used to justify temporary relaxation of Tech Specs AOTs within negations with regulator.

Risk Assessment of Outages and Configuration Control: Using the PSA based Safety Monitor models all plant outages are evaluated from configuration risk point of view along recommendations to the outage schedulers for plant configuration control to minimize the operational risk. Schedule of every planned outage is quantified and analyzed from the risk point of view using Safety Monitor models and recommendations for the risk minimization are made before the outage begins.

In addition, the planned schedule vs. real outage configuration risk profiles is compared to find out and analyze potentially significant risk differences and reasons for to get a feedback for future outage planning.

In such manner both the cumulative risk during outage and number of actual configuration risk peaks exceeding established thresholds is substantially decreasing in the last two years.

Training of operators and plant staff: One of PSA objectives was identification of plant risk dominant accident sequences and critical human interventions contributing to the CDF. Both risk dominant accident sequences and critical human actions in these sequences were identified and provided to both Emergency Operating Procedures cognizant engineers for the EOPs development and improvement process and to the operating crew training center to establish list of such risk significant sequences to be trained on the plant MCR full scope simulator.

7.2.19 Canada

REGULATOR

As mentioned above, the CNSC reviews the technical quality of the PSAs against the objectives established for each particular PSA. As a minimum, CNSC looks to the insights regarding the plant weaknesses, and the level of risk posed by the new, operating plants or those requiring refurbishment. The licensees prepare the safety case that includes results and insights from the PSA and CNSC reviews for acceptance of licensees' proposal.

Internally, the PSAs have been used for many years now, in a more or less formal manner, to support the traditional safety approach. In time, the PSAs application to various situations is expected to become more prominent in a risk-informed decision making environment as promoted and supported by CNSC management. At present, the PSAs insights are being used in conjunction with other assessment tools and factors to identify in a systematic and documented manner the solutions for complex issues.

By the end of 2002, CNSC staff produced a replica of the Level 1 PRA model for the Bruce B NPP (BBRA), which was originally developed using SETS. In 2003, the CNSC model has been extended to Level 2 (includes Containment systems and release assessment). The replica is able to run using the CNSC computer tools (SAPHIRE).

The BBRA replica is:

Used to interrogate the licensees' PRAs, and

Intended to be used to independently evaluate events, submissions, and non-compliances.

CNSC staff plans to develop procedures to assess the risk-significance of issues, and to use PRA insights to prioritize regulatory inspections.

It is expected that in the future, PRA applications will cover other areas, such as configuration management, significant event analysis, maintenance, operator training, operating procedures, design changes or backfit, operational safety system test program, etc., to support safe operation of nuclear plants [5].

Another aspect of interest to CNSC is the progress that both the industry and CNSC are making to develop Severe Accident Management programs and Emergency Planning. The CNSC is promoting the use of PSA insights in defining the strategies to cope with the consequences of severe accidents.

INDUSTRY

Design Assist and Safety Demonstration: The first applications of PRA at Ontario Power Generation (OPG) were in design assist to the Darlington station (1980's) and Pickering A refurbishment (mid-1990's). A number of changes were introduced during the refurbishment (Pickering A being the first commercial nuclear generating station in Canada) to reduce the severe core damage frequency to a value comparable to other Candu plants.

Subsequently, the PRA has been extended to confirm design adequacy of all plants with respect to safety goals. The PRAs are also used to support design changes that affect system reliability and in event investigation (e.g., loss of offsite power).

Systems Important to Safety: A6t OPG, the PRA results are used to identify systems and components important to safety through risk importance indices (FV and RAW). These systems are subject to enhanced surveillance and annual reliability performance reporting as part of the regulatory reporting requirements

Severe Accident Management Guidelines: Accident progression analysis performed for level 2 PRAs was used to help develop generic SAMG for the Canadian industry and then to customize it to each of the 7 operating stations in Canada.

Operational Support: OPG has developed risk monitors for both the at-power and shutdown states for Darlington and Pickering B stations using the EOOS software, and plans to do so for Pickering A as part of the current PRA update. These will be used in conjunction with OPG's internal guidance on management of risk under abnormal plant conditions to assist in operational decision making.

Bruce Power: The BBRA and BAPRA were developed (a) to demonstrate the safety adequacy of the station design and operation, and (b) to assist the safety-related decision-making process throughout the life of the station in conjunction with ancillary application tools.

Bruce Power has generated risk monitors for both the at-power and shutdown states for Bruce B using the EOOS software. These are presently being used at the station to manage operational risk.

The Bruce A shutdown risk model in Windows Risk Spectrum has been filtered to generate an operational shutdown risk monitor in the EOOS platform. This is currently being tested and verified. A similar process is planned for the Bruce A at-power model to generate an on-line risk monitor in the EOOS platform.

The Bruce PRA models are also being used to support the regulator's S-98 Reliability Program in determining systems important to safety as well as developing the required reliability models.

The BAPRA is being used at this time to support the Unit 1 and 2 Restart requirements. Important applications are (1) cost-benefit assessments of potential modifications, (2) licensing requirements such as IAEA's singleton failure criterion review and (3) comparison with modern safety codes.

The BBRA Level 2 framework provided input in support of the development of the Bruce Severe Accident Management Guidelines (SAMG).

Atomic Energy Canada Ltd. (AECL): AECL applies the PSA in making design decisions to determine system configuration. AECL performs PSA as a design tool to improve the safety of operating CANDU 6 and ACR-1000 nuclear power plants.

A "Risk Baseline" document was prepared to support design improvements for Point Lepreau refurbishment. The Risk Baseline provided input for cost benefit assessments for approval of the implementation of the design change. The results of the Risk Baseline will be confirmed via the more rigorous site specific PSA.

Hydro Quebec is presently planning for Gentilly-2 refurbishment. The PSA scope is presently being defined. Inputs to perform the Gentilly-2 PSA are being worked on: e.g. site seismic hazard, PSA methodology, and the parameter file for consequence analyses using the MAAP-CANDU code.

For the operating units, PSA provides a support activity to design and operation.

For the new build, PSA provides input to the design process, so that the safety goals can be achieved. The PSA provides design assist analyses to support detailed design activities. The items in the Figure 1 refer to finalized PSA analysis that demonstrates design robustness and no dominant event sequences.

ACR-700 PSA effort has provided input on design decision in implementing quadrant design in the ACR, as well as assessing diversity in the design of systems to minimize the impact of common cause failure.

ACR-1000, the PSA is ongoing with a continuous dialogue providing PSA input to the designers.

7.2.20 Belgium

Design evaluation: Up to now, the main application concerns design evaluation. Indeed, the primary objective is to use the PSA, in the framework of the periodic safety review, as a complementary tool to the deterministic safety analysis. It should mainly provide valuable insights in the balance of the design, identify important contributions to the core melt frequency and constitute a useful tool to evaluate the effectiveness of proposed plant modifications.

Accident management: Based on the results of the first level 1+ studies performed for the Doel 3 and Tihange 2 plants, the utility decided to install catalytic hydrogen recombiners in the containment, for all 7 nuclear power plants. This action is implemented for all units.

PSA based event analysis: The analysis of operational events by using PSA has been integrated in the operational experience feedback process at AVN. The objectives of the AVN precursor program are mainly focused on (1) the determination of the quantitative importance of a few well-selected operational events per year, and – if sufficiently significant – on (2) the subsequent identification of potential safety issues for improvement (based on the real best-estimate case as well as on relevant what-if questions). More information can be found in papers presented at PSAM7 and PSAM8 conferences. Event analysis are planned to be performed by the utility too.

Evaluation of Technical Specifications: Insights gained from the PSAs have been used by AVN for arguing in some Technical Specifications related matters (for instance, requirements on the availability of some systems in shutdown). Until now, this has not yet led to formal modifications of the Technical Specifications.

So far, no requests have been discussed with the utility for modifications to the Technical Specifications based on PSA insights.

In the opinion of AVN PSA can contribute to the optimisation (not only relaxation) of Technical Specifications. This is especially the case for the Technical Specifications in shutdown conditions, where the justification for allowed unavailabilities for instance is even weaker than in the power conditions.

It is AVN’s expectation that in future this kind of application will be discussed with the utility.

8 RESULTS AND INSIGHTS FROM THE PSAS

8.1 Summary

Numerical results

Concerning the numerical values, the information given by the different countries is rather heterogeneous. In some cases a very complete presentation of results is provided, including relative contribution of the dominant initiating events. In several cases there is only a general indication about the fact that probabilistic objectives or orientations are met. Very often there also are some considerations about the fact that the risk is decreasing, due to safety improvements.

In fact the numerical results give only limited information and the problem with absolute values is well summarized in the USA contribution:

"It should be emphasized that comparisons of PSA results should be made with great caution. The PSA results are dependent on design- and operations-specific details, and on modeling approaches and assumptions. (Variations in modeling can be due to a number of reasons, including differences in the purpose of the PSA, associated differences in the PSA scope and level of detail, and differences in the level of maturity of the state-of-the-art for analyzing different accident classes and contributors.) It can be seen that this caution applies to comparisons of results for a single plant over time, as well as to comparisons of results between plants. Contextual information regarding the dominant contributors to risk and the reasons for their dominance (including modeling approaches and key assumptions as well as physical factors) will enable the reader to better compare and contrast study results."

Dominant risk contributors:

Much more interesting insights are given by the relative contributions.

One fact is particularly outstanding: the high contribution of external hazards. It can be noted among others:

- Fire (USA, Finland, Hungary, …)
- Earthquake (Hungary, Switzerland, ...)
- Flooding (Netherlands.)
- Harsh weather (Finland)
- Typhoon (Korea)

One reason for these high contributions is perhaps that several hazards were not covered by the first PSA versions, and safety improvements were implemented for the dominant internal initiators, while the introduction of hazards in the PSA led to identify new problems. This is illustrated by some examples of plant modifications due to the treatment of external hazards and leading to a lower contribution to the results.

It has also to be noted that Low Power and Shutdown situations contribute also significantly in several results.

Safety improvements:

Another particularly interesting part of Section 8 is the presentation of plants safety improvements due to PSA results.

All the countries indicate that their PSAs led to safety improvements. In some cases a very precise (and long) list is given, for others there is only indications about the most important and recent improvements.

Logically the main safety improvements correspond to the dominant risk contributors, and in particular the hazards PSAs led to several important plant modifications. Among the large number of improvements, it could be noted many examples of modifications aiming to reduce human errors (signals, automatisms,..), many improvements relating to electrical problems, to water intake problems, and several examples of solutions including cross connections between units.

More generally it can be noted that:

- All the countries indicate some (or many) PSA based plant safety improvements.
- These improvements concern plant operation (EOPs, SAM measures) as well as plant design (a lot of examples).
- all the parts of PSA are used for safety improvements: level 1, level 2, internal and external initiators, full power and shutdown situations.

A general conclusion could be that PSA development is growing (number and scope of the studies) and each new step can be the source of safety improvements. Moreover the PSA results are considered as sufficiently credible to be used as a contribution to important safety decisions.

8.2 Country replies

8.2.1 USA

As is widely recognized and confirmed by the PSAs discussed in Section 5.US, the results and insights of PSAs are dependent on plant-specific design and operational characteristics. Details regarding such characteristics as the level of redundancy and diversity of front-line mitigation systems, the design of support systems and the dependency of front-line systems on support systems, the plant operational procedures, and the layout of key equipment (including cables) can and typically do make a difference to overall risk as well as to the importance of risk contributors. In addition, differences in study-specific modeling approaches (e.g., assumptions regarding the allowable credit for alternative mitigation systems) can have an observable effect on PSA results.

With these caveats in mind, a number of broad observations are worth noting.

First, the general classes of accidents (e.g., transients, station blackouts, loss of coolant accidents – LOCAs, internal floods, seismic events, internal fires) potentially important to risk, their general importance to risk for different classes of plants (e.g., boiling water reactors vs. pressurized water reactors), and the reasons for their importance, are reasonably well understood.

Second, the total plant risk is often determined by a number of different sequences in combination (rather than by a single sequence or failure mechanism). The degree of distribution among sequences varies from plant to plant.

Third, as noted previously, the largest contributors to risk vary considerably among the plants. NUREG-1560 notes that variations in support system designs and in the dependency of front-line systems on support systems explain much of the variability in CDF observed in the IPEs.

Fourth, seismic and fire events are important CDF contributors for many plants. The CDF contribution from seismic or fire events can, in some cases, approach (or even exceed) that from internal events. As discussed in NUREG-1742, the important seismically-induced failures reported by the IPEEEs include failures of offsite power, electrical system components (e.g., motor control center, switchgear, relays, emergency diesel generators, batteries), block walls, building structures, front line and support system components (e.g., pumps, heat exchangers, pipes), and major tanks. The important fire areas reported in NUREG-1742 include the main control room, emergency switchgear rooms, cable spreading rooms, cable vault and tunnel areas, and turbine buildings.

Fifth, the results of plant PSAs have been considered sufficiently robust to support changes to plant design and operations. Some specific examples of PSA-spurred improvements reported by Gaertner et al include the replacement of pressurized water reactor (PWR) reactor coolant pump seals with a more rugged type; the provision of additional cross-connections between the service water systems at a two-unit site; numerous changes (e.g., sealing of penetrations, strengthening of watertight doors, installation of level alarms, valve alignment changes, rewriting of emergency operating procedures) to reduce internal flooding risk; modification of emergency operating procedures to support the controlled venting of boiling water reactor (BWR) containments; modification of practices during shutdown operations to reduce plant vulnerability to draindown events; and improving equipment condition monitoring and preventive maintenance practices to lower the failure rates of risk-significant equipment. Gaertner et al also discusses observed improvements in plant performance (e.g., reduced numbers of plant trips and significant events per year) which also contribute to reduced plant risk.

Finally, it should be emphasized that comparisons of PSA results should be made with great caution. As mentioned previously, the PSA results are dependent on design- and operations-specific details, and on modeling approaches and assumptions. (Variations in modeling can be due to a number of reasons, including differences in the purpose of the PSA, associated differences in the PSA scope and level of detail, and differences in the level of maturity of the state-of-the-art for analyzing different accident classes and contributors.) It can be seen that this caution applies to comparisons of results for a single plant over time, as well as to comparisons of results between plants. Contextual information regarding the dominant contributors to risk and the reasons for their dominance (including modeling approaches and key assumptions as well as physical factors) will enable the reader to better compare and contrast study results.

8.2.2 United Kingdom

In the UK, PSAs have been carried out either as part of the design process (for example, Heysham 2, Torness and Sizewell B) or as part of the Periodic Safety Reviews for the other older reactors. In all cases the PSA has identified areas where improvements have been made to the design and operation of the facility. This has ranged from major improvements – for example, the addition of a set of diverse safety systems which carry out the safety functions for frequent initiating events, to relatively minor improvements to operating procedures and training.

PSA for Sizewell B

The Sizewell B design is based on the Westinghouse Standardized Nuclear Power Plant System (SNUPPS). However, changes were required to meet the UK safety requirements which included dose reduction requirements (similar to those achieved on AGRs), an RPV incredibility of failure approach, 30 minute operator action rule, deterministic requirements (for redundancy/ single failure criterion, diversity, etc.) and probabilistic/ reliability targets.

PSA work was carried out throughout the design and construction phases of the plant and continued into operation which included the following:

- a Level 1 PSA for a range on internal initiators at power which was carried out during the design phase and which forms part of the Pre-Construction Safety Report (PCSR)
- a Level 3 PSA for a range of internal initiators at power which forms part of the evidence presented to the Public Inquiry, and

- a comprehensive Level 3 PSA for all initiating events and hazards, and addresses all modes of operation (including full power, low power and shutdown modes) which form part of the Pre-Operational Safety Report
- a 'Living' PSA to support plant operations and provide up-to-date best estimate of station risk.

The most important probabilistic target that influenced the design was that related to the frequency for uncontrolled releases for single accidents. This requires that the frequency of fault sequences which could give rise to a large uncontrolled release of radioactivity should be less that 10^{-7} per year and the sum of all such fault sequences should be less that 10^{-6} per year.

In addition, it was recognised that common cause failure limited the reliability that could be claimed for a safety system that incorporated redundancy only. A CCF value of 10^{-4} failures per demand was chosen for design purposes for active safety systems thus the requirement that:

[initiating event frequency] x [safety system failure probability] < 10^{-7} per year

meant that for initiating events with a frequency of $>10^{-3}$ per year, diverse safety systems would need to be provided for each of the required safety functions. This led to the following safety systems being added to the SNUPPS design to <u>increase diversity</u>:

- a Secondary Protection System (SPS) using magnetic logic devices (LADDICS) which was diverse from the computer based Primary Protection System (PPS),
- an Emergency Boration System (EBS) which was a fast acting system to inject a highly concentrated boron solution into the reactor coolant system following failure of control rods to drop into the core,
- the auxiliary feedwater system was replaced by two diverse systems one using electrical motor driven pumps and one using steam turbine driven pumps,
- an Emergency Charging System (ECS) which used steam turbine driven pumps which was diverse from the Chemical and Volume Control System (CVCS) which used electrical motor driven pumps. This provided diverse protection for the reactor coolant pump seals and boration of the primary circuit, and
- a seismically qualified air-cooled Reserve Ultimate Heat Sink (RUHS) to provide diversity from the seawater cooling system.

The PSA related design work lead support to further changes to the SNUPPS design to <u>increase reliability and segregation</u>:

- 4 x 100% Essential Diesel Generators,
- 4 High Head Safety Injection (HHSI) pumps,
- Interchangeable RHR and Containment Spray pumps (4 LHSI in total),
- Automatic switchover to recirculation mode for all safety injection pumps (HHSI+LHSI) on depletion of the RWST,
- 4 x 100% Component Cooling Water System (CCWS) pumps, and
- SEBIM valves to replace the pressuriser's PORVs+block valves.

Further design changes were made as a result of the PSA carried out at the PCSR stage. As a result of the Level 1 and 3 PSAs, further changes included:

- provision of two battery charging diesels to give long term DC power for control and instrumentation following an extended loss of all AC power,
- the additional, diverse provisions for isolation of the containment mini-purge system,

- changes to provide a Cavity Flooding System to provide better protection (basemat protection/ debris coolability) for the containment following a severe accident,
- additional isolation valves and interlocks to the RHR suction lines to reduce the frequency of an interfacing-systems LOCA which would discharge outside the primary containment, and
- diversity of supply to the CCWS/Reserve Ultimate Heat Sink fan cooler to enhance containment over-pressure protection.

In support of station operation, the PSAs developed during design and construction, were developed into a 'Living' PSA (LPSA) to provide an up-to-date best estimate of station risk to station staff. In particular, it has been used to address the risk arising from increasing the enrichment of the fuel used in the reactor and the consequent increase in the time between refuelling outages. In considering the options available for maintenance work during shutdown/refuelling, the LPSA has been used to determine the risks which would arise if the reactor coolant level was reduced to mid loop level.

The 'Living' PSA is regular updated to ensure that it correctly reflects the operational plant; since initial inception the LPSA has been updated 7 times and a further update is planned.

The current LPSA for all initiating events and hazards, and all modes of operation (including full power, low power and shutdown modes) indicates that the division of the risk of core damage between operating modes is:

Operating mode contribution to the Core Damage Frequency	
- Modes 1,2 & 3 - Full Power, Low Power & Hot Shutdown	42%
- Mode 4 - Cooldown (SG or RHR)	7%
- Mode 5 - RCS Intact	22%
- Mode 5 - RCS open-refuelling pool not flooded up	27%
- Mode 6 - Refuelling pool flooded-up	2%

With the major fault contributors to core damage being:

Major contributors to Core Damage Frequency	Mode	% Contribution
Total loss of RHRS faults	4 to 6	14%
Small Auxiliary Building leaks	5 & 6	8%
Total loss of CCWS faults including Seawater Blockage	All	8%
Large RHRS leak in the Auxiliary Building	4 to 6	7%
Loss of Off-site Power faults	All	6%

Taking account of mitigation and containment the major contributors to a large uncontrolled release are:

Major contributors to Large Release	Mode	% Contribution
Large RHRS leak in the Auxiliary Building	4 to 6	12%
Small RHRS Auxiliary Building leak	5 & 6	10%
Internal Flooding (ESWS)	All	8%
SG Tube Rupture (Multiple/Single rupture(s))	1 to 4	8%
Seismic $1E^{-4}$ and $1E^{-5}$ events	All	7%

Currently the LPSA has been utilised by station support and operational staff to:

- support the Technical Specifications, primarily with
  - increased in fuel cycle length (18 to 24 months),
  - action completion times, and
  - operability requirements for various systems (e.g. EBS).
- support to Maintenance strategies, primarily with
  - battery maintenance,
  - mid-loop operations, and
  - RPV head seal replacement/repairs
- Hardware modifications
- Cat 1 MOV Surveillance Programme.

PSA for the AGRs

The PSAs carried out for the AGRs, either in support of the design process (Hartlepool and Heysham 1, and Heysham 2 and Torness) or latterly as part of the Periodic Safety Review (PSRs), have led to, or supported, a number of significant design changes.

Changes which have been made to the design or operation which are based (in part) on probabilistic considerations include:

- the change from 2 to 3 year outages. The design PSA for the Heysham 2 and Torness AGRs was revised to reflect the new regime of three year statutory outages and was able to demonstrate that the move did not unduly increase the risk. This move has major financial implications for the operation of the plant,
- the provision of diverse safety systems. For the older AGRs, the emergency feed system and the back-up cooling system shared common pipework and valves. The relevant PSA identified that this limited the reliability of post trip cooling and was used to investigate the options for improvement, and
- changes to operating procedures and training. Whilst the newer AGRs have control rods and a rapid nitrogen injection system for reactor shutdown, the older AGRs only have control rods. The PSAs were used to investigate a number of options for enhancing the reliability of the shutdown system. The option chosen was to separate a group of rods - the grey rods, which are used to trim the power of the reactor and hence are constantly in motion. These are now wound into the core on reactor trip as opposed to the other rods which fall in under gravity.
- change to the Maintenance Schedule definition of a calendar month from 30 to 35 days to align with station shift rotas (Heysham 2),

More recently, there have also been a large number of other modifications which have been supported by the AGR's PSR PSAs as follows:

- modifications to the functionality of the Vessel Overpressure Protection Equipment to reduce the level of water ingress following a boiler tube leak, together with a revision to the boiler tube leak faults safety case (Hinkley Point B and Hunterston B),
- Provision of a Vessel Overpressure Protection Equipment to reduce the level of water ingress following a boiler tube leak, together with a revision to the boiler tube leak faults safety case (Hartlepool and Heysham 1),
- enhancement to the fire hydrant system to provide an alternative heat sink for the PVCW and installation of backup diesels for the PVCW pumps to provide diversity following loss of grid faults (Hinkley Point B),
- installation of an Additional Feed System to provide increased post-trip cooling reliability, particularly following loss of grid faults and hazards (Dungeness B),
- installation of an Electrical Overlay System to provide dedicated electrical supplies following hazards (Dungeness B),
- enhancement of CO_2 and N_2 injection systems to provide enhanced post-trip cooling and shutdown capability (Dungeness B), and
- enhancement of the LPBUCS (backup PVCW system) to provide increased protection against loss of pressure vessel cooling (Hartlepool and Heysham 1).

In addition there are many other revisions to the AGR safety cases, where the PSAs have been used to support the revision and where hardware modifications have not been required - a prime example being the Gas Circulator Run-on safety cases which have now been completed for most of the AGRs.

The current AGR PSR PSAs consider all initiating events and hazards for the full power mode of operation; although results vary dependent on age, location and operational practise typical results indicate that the most likely contributors to an uncontrolled large release are:

Fault Contribution to Large Release frequency	
Over-pressurisation Faults	34%
Depressurisation Faults	19%
Other Plant Based Faults	19%
Gas Circulator Run-on Faults	7%
Loss of Feed Faults	7%
Loss of Grid Faults	5%
Loss of Electrical Supplies Faults	3%
Reactivity Faults	5%

Note, for AGRs over-pressurisation faults (mainly boiler tube leaks into the reactor core) are more dominant than depressurisation faults as they grossly inhibit heat removal by gas circulation, in severe cases the water/steam injected into the core can cause gas circulator failures resulting in a complete loss of forced circulation.

PSA for the Magnox reactors

The PSAs for the Magnox reactors were carried out as part of the safety cases produced for the Long Term Safety Reviews (LTSRs); an aim of the LTSRs being to consider whether it would be safe to operate the reactors beyond 30 years. More recently the PSAs of the more modern Magnox reactors were updated as part of the programme of Periodic Safety Reviews (PSRs). Currently only the two youngest Magnox stations remain operational, Oldbury and Wylfa, both of which have (steel lined) concrete pressure vessels.

During these reviews (LTSR and/or PSR), the safety of the Magnox reactors has been assessed against both deterministic and probabilistic criteria, and changes have been made to the design and operation which included the following:

- a secondary shutdown system in which boron beads were blown into the reactor following failure of the control rods to enter the core. This system provided protection against earthquake and additional diversity (applicable only to the early Magnox stations),
- a secondary guardline which provides a diverse means of detecting that a fault condition has occurred and initiating a reactor trip. The primary and secondary guardlines both use relays but they are of a different design and manufacture,
- a tertiary feedwater system which is diverse from the existing main and back-up feedwater systems and provides feed to the boilers in fault conditions, and
- modifications to mitigate the consequences of a hot gas release.

For the reactors with steel pressure vessels (the early Magnox stations), the secondary shutdown systems took the form of a boron ball injection system, whilst for the later reactors with concrete pressure vessels, design changes were implemented in the form of articulated control rods. These provide protection for fault sequences such as earthquake where the geometry of the core could be changed and provides a diverse means of shutting down the reactor.

Cooling of the core by natural circulation has now been demonstrated for all the remaining Magnox reactors due to the favourable geometry of the gas circuit. Natural circulation cooling capability for fault sequences involving a gradual depressurisation has also been demonstrated. This has led to the significant development of the natural circulation cooling safety cases for the reactors with concrete pressure vessels.

The Magnox PSAs were revised to take account of these modifications and revised capabilities, and are now of a standard which allows them to play a larger role in targeting potential weaknesses in the design or operation.

The current Magnox PSR PSAs consider all initiating events and limited hazards for the full power mode of operation; typical results indicate that an uncontrolled large release is most likely to result from failure to trip the reactor:

Fault Contribution to Large Release frequency	
Reactor Trip Faults	59.5%
Reactor Shutdown and Hold down Faults	14.4%
Post Trip Cooling Faults	26.1%

The dominance of the reactor trip faults is shown to be due to the common cause failure probability assumed for the main and diverse guardline control rod tripping contactors. Although the main and diverse contactors are of different design there physical proximity to each other dictates that a single CCF be applied to both.

Consideration of the post trip cooling faults indicates that the most likely contributors to an uncontrolled large release are:

Post Trip Cooling Fault Contributions to Large Release frequency	
Missile (Depressurisation) Faults	21.7%
Fire related Faults	18.4%
Depressurisation Faults	14.6%
Loss of Electrical Supplies Faults	11.6%
Loss of Grid Faults	10.8%
Extreme Wind Loading Faults	8.1%
Loss of Feedwater Faults	6.4%
Essential Systems Faults	4.8%
Seismic Faults	3.6%

Cooling of the Magnox reactor cores can be achieved by natural circulation which is reliant upon sufficient gas being available within the primary circuit to achieve effective heat transfer. Depressurisation of the primary circuit leads to a reduction in the amount of coolant available and negates the effectiveness of natural circulation to cool the core.

At NII's request, the Magnox licensees are reviewing their Operating Rules (equivalent to Technical Specifications) which govern the availability of safety related equipment to ensure that the increase in risk during periods of maintenance is kept as low as reasonably practicable. Another key area identified for improvement by the PSA involves the important recovery actions which could be undertaken. This has led to the development of new procedures and additional operator training.

8.2.3 Taiwan

The latest PSA update was completed in 2003 and the results are listed in appendix A. Core damage due to seismic and external fire is the major contributors to CDF for all operating NPPs. The results from Kuosheng also indicate that the events of lost of safety-related DC buses are most important initiators during power operation. After collecting plant specific operating data from 1994 to 2002, most initiating event frequencies and component failure probabilities are lower than the generic data after Bayesian update. The frequency of loss of off-site power is one of the interest exceptions. Due to the large power demands in north Taiwan, the electric power generated in south Taiwan has to be delivered north along the power grid across the high mountains. The existing plant operating data showed that the frequent significant earthquake impact directly on plant or on power grid would have high likelihood to cause the loss of off-site power event. The solution of the problem is to improve the strength of power grid against any external perturbation such as seismic, typhoon or significant imbalance between power generation and demands.

8.2.4 Switzerland

PSA-based modifications and backfits have often been introduced in the Swiss nuclear power plants and are listed below.

Beznau Plant

Beznau I and II are Westinghouse PWRs. They are in commercial operation since 1969 and 1971, respectively. The original design consisted of two trains of safety systems with relatively poor physical separation and seismic qualification. Backfits, which were performed based on PSA results, are given in the following:

- installation of new electrical transformers and improvement of the anchorage of existing transformers in the electric power system
- installation of a new instrument air compressor
- reinforcement of some electrical cabinet anchorage to the floor for seismic events
- reinforcement of a brick wall in the area of the main control room for seismic events
- reinforcement of cable trays for seismic events
- installation of a feed path from a third, existing battery, which is separated from the two existing paths to the plant DC buses
- several changes in the plant emergency operational procedures.

The CDF of the plant was reduced by about a factor of five by these cost effective measures.

Optimization of a large backfitting project by using PSA results:

During the late 1970's, the HSK required that the Beznau plant be upgraded to meet more recent safety standards. The aim of the backfit called NANO ("Nachrüsten Notstandsysteme") was to upgrade the safety systems of the plant with respect to redundancy, separation, qualification and protection against external events (bunkered decay heat removal system). In using the Beznau PSA model, the reductions to the core damage frequency of the following two configurations of NANO were analyzed:

a) A simple single train system, consisting of one train of steam generator (SG) feed and one of reactor cooling pump (RCP) seal injection, one emergency core cooling system (ECCS) low pressure injection pump, single train support systems and the rebuilding of the refueling water storage tank (RWST) so that it would be protected against external events.

b) A more costly two-trains system, consisting of two trains of SG feed and of additional component cooling water, one train of ECCS recirculation, one ECCS high head and two ECCS low pressure injection pumps, one charging pump, two trains of support systems and the rebuilding of the RWST so that it would be protected against external events.

As a result of this PSA investigation, the simple single train system was found more cost effective than the expensive two-trains system. The configuration of NANO, as finally realized, was a combination of these two systems and included the following modifications per unit:

Front line systems:

- adding one train of emergency SG feedwater and one of emergency RCP seal injection
- adding one train of ECCS recirculation
- adding two accumulators to the ECCS system

- replacing one ECCS safety injection pump by a new one in the NANO bunker
- rebuilding the RWST protected against external events
- replacing the pressurizer safety and relief valves by three new tandems of combined safety and relief valves
- seismic re-qualification of the primary circuit and of some other components and structures.

Support systems:

- adding one emergency diesel generator and one emergency cooling water pump, each with a cross-connection to the other unit
- adding a control system and a separate emergency control room for all NANO systems.

All systems added are located in a new and separate bunker protected against external events. As a result, the reduction to the core damage frequency obtained by the NANO upgrade is about a factor of 30.

Independently from PSA, a filtered containment venting system was installed.

The Beznau PSA was used to evaluate the optimal configuration for the feedwater upgrade project. This investigation resulted in the decision to install one additional emergency feedwater train. During the last few years, a new fourth battery train was implemented. Furthermore, passive recombiners have been installed in order to avoid containment failure due to hydrogen explosions during a severe accident.

Gösgen Plant

Gösgen nuclear power plant is a three-loop PWR built by Siemens-Kraftwerk Union AG (KWU). The design is four train safety and an additional two train special emergency systems with strict physical separation and seismic qualification. The plant began commercial operation in November 1979. Based on the PSA results, the utility has performed a number of changes and taken courses of action to address the principal contributors to risk. They include:

Based on full power PSA results:

- An on-site inspection carried out by HSK within the PSA review process revealed that the masonry walls in the electrical building were not included in the PSA model. An improved PSA model showed later that a lot of these walls were risk-significant. Therefore, HSK required the plant to backfit the walls.
- Addition of seismic restraints for electronic cabinets on double floors in the electrical and special emergency buildings (“Notstand” buildings).
- Modifications to reduce service water intake blockage vulnerability and new technical specifications to restrict “Notstand” (special emergency system) and 220-kV systems maintenance during periods of high debris content in river.
- Larger diameter emergency diesel generator heat exchanger tubes to reduce vulnerability to debris plugging.
- New accident management procedures and documentation for RCS injection via Notstand equipment, for steam generator feed via external sources and for active steam generator cooldown on loss of emergency (“Notstand”) buses.
- A change to keep containment sump lines isolated during normal operation except during controlled sump drain.

Based on low power and shutdown PSA results:

- By maintaining technical specifications of the plant it was possible to enter the outage state and go on RHR cooling even if only one RHR cooling train was available. There was an additional situation that was exacerbated by the technical specifications in which a two-train equipment outage may lead to an enforced plant shutdown and a need to go on RHR cooling when RHR and/or support systems are seriously degraded. Therefore, an additional train for spent fuel pool cooling that is capable of cooling the spent fuel pool when the core is unloaded into the pool during the refueling outage was implemented. Plant practice and technical specifications were correspondingly modified to ensure that there is no initial degradation of the RHR cooling function at the beginning of an outage involving cold shutdown.

- Technical specifications were further modified in 2001, in order to ensure that the single failure criterion is fulfilled during all outage configurations. These modifications reflect the practice introduced earlier as a result of the shutdown PSA.

Leibstadt Plant

Leibstadt nuclear power plant is a General Electric BWR/6 with a Mark III containment. The plant has an additional two-train special emergency heat removal system (SEHR). The plant began commercial operation in December 1984. Based on the PSA results the utility has implemented the following major plant and procedure modifications:

- Mitigation of the consequences of anticipated transient without scram (ATWS) requires that the plant operator reduce reactor pressure vessel water level to lower core power generation. The reduction of the RPV water level below Level 1 will initiate the logic sequence for initiation of ADS, which is designed to provide automatic actions in support of the low pressure ECCS following small to intermediate sized loss of coolant accidents. Automatic vessel depressurization is not desirable following this postulated ATWS. Reducing RPV water level is desirable following the postulated ATWS because the lower water level will reduce power generation. It is therefore necessary to inhibit opening of the ADS Safety Relief Valves during an ATWS event. The plant change incorporates modifications to the plant logic to automatically inhibit ADS when the ATWS control logic determines that an ATWS event is underway.

- Containment isolation failure is an important aspect of the level 2 PSA. Even though the isolation failure does not result in high radiological consequences due to the nature of the failure (a long narrow path for release), the utility implemented instructions in the emergency operating procedures (EOPs) to isolate two manual valves in the equipment drain lines (which are not supported by DC power), outside the containment, when the suppression pool reaches a certain temperature.

- For the depressurization of the reactor coolant system, accident management actions were implemented in the instructions. The instructions describe the use of an alternative water source (the lineup of reservoir water) and the manual opening of SRVs.

Mühleberg Plant

Mühleberg nuclear power plant is a BWR/4 Mark-I built by General Electric. It started commercial operation in November 1972. A major upgrading of plant redundancy and safety was done during the years 1985 -1989, when an additional and independent two train safety system was added, called SUSAN ("System zur unabhängigen und sicheren Nachwärmeabfuhr"). SUSAN was declared "ready for service" in September 1989 and consists of the following equipment:

- a bunkered, sabotage, airplane crash, earthquake and flooding resistant building containing:
    - an emergency control room which has a priority logic overriding any commands from the main control room
    - two specially separated 800 kVA diesel generators
    - associated cooling equipment, including independent river water intake

- filtered air ventilation equipment which can be operated to guarantee SUSAN-building habitability, even during hypothetical core melt accidents and after the noble gas releases.

In the reactor building, which acts, as in all Swiss nuclear power plants, as a secondary containment, the following equipment has been made part of the SUSAN-ECCS:

- two low pressure ECCS-pump trains delivering 150 t/h each at about 17 bars (ALPS)
- two high pressure steam turbine driven ECCS-pumps delivering 50 t/h each at primary system operating pressure (RCIC)
- two 100 % RHR-systems providing cooling to the pressure suppression chamber water (TCS)
- associated I&C (Instrumentation & Control) hardware
- for severe accident mitigation: containment pressure relief system and containment spray and flooding system.

In the containment, the most remarkable addition belonging to the SUSAN system are two electric motor driven pressure relieve valves (PRV), each of which is capable of discharging 50 t/h live steam into the pressure suppression chamber. This in addition to the standard ADS function, which was also made part of SUSAN. Last, but not least, a totally independent SCRAM function using SUSAN I&C has been added.

SUSAN is designed as an independent system, which is able to shut down the reactor and to assure RHR automatically, i.e. not requiring any operator interference. This effective safety system backfit has been planned and realized without making reference to any PSA analysis, which did not exist at that time. A level 1 and level 2 PSA for KKM, called MUSA (Mühleberg Safety Analysis) was started in the second half of 1988 and has been submitted to HSK in 1990. The bottom line of this study was that the plant, taking full credit of SUSAN, displays a low risk profile. Nevertheless, two modifications were made to the plant, which can be considered a direct consequence of the PSA results:

- a depressurization logic and hardware was added which is triggered by low RPV water level only. (The original automatic depressurization system, ADS, is activated by a low RPV level and high drywell pressure signal). This backfit was the result of an accident sequence identified by MUSA, which starts with an RPV isolation, followed by the failure of both high-pressure injection systems and an operator error by failing to manually depressurize the primary system. (Note that automatic depressurization would not have functioned because of lack of the high drywell pressure signal).
- analyses done for this sequence showed that the PRV's would depressurize the primary system after a 30-minute delay time, but that the low-pressure injection system would deliver too late to prevent massive fuel overheating and damage, though the RPV would most likely have remained intact. It was decided that this accident sequence is highly undesirable and that this fairly simple extension to the existing depressurization logic would eliminate it.
- During the analysis of ATWS success criteria to be used in the PSA, it was realized that the 120 sec. delay reset for automatic depressurization might interfere, in an undesirable way, with the very high capabilities of the plant to ride out an ATWS. Therefore, it was decided to add an "ATWS switch" which will, in this very rare case, eliminate any possibility to omit the repeated reset of the 120 sec. delay.

8.2.5 Sweden

This section gives a description of the Swedish PSA results that have been obtained and the insights that have been derived. E.g., weaknesses that have been identified and plant modifications or other changes are considered for improvement of the design or operation of the plant.

Insights from the domestic PSA:s and the plant improvements that have been made:

- The PSA-models have evolved and grown by time, and more and more information are put into them, that can be calculated. By the time lot of design weaknesses and other observations have revealed the need of plant modifications and renewals of structures, systems and components as well as of administrative routines.
- The PSA:s have been used to show, in many cases, an optimized design solution before a modification proposal is set.
- The PSA;s have strongly shown the need of consideration on dependences at design, daily operation and maintenance of plants

A tendency that can be seen in the Swedish PSA:s, is when the contribution from LOCA:s is decreased, the impact of electrical systems and dependencies pop-up and become more important.

8.2.6 Spain

For all NPPs, results indicate that the risk during non-power states is comparable to the risk during power operation.

For the level 1 internal events, the updated results of core damage frequencies are as follows:

Core Damage Frequency (reactor/year) for internal events

CN José Cabrera	2.16 E-5
CN Stª Mª de Garoña	1.89 E-6
CN Almaraz	5.12 E-6
CN Asco	2.92 E-5
CN Cofrentes	1.27 E-6
CN Vandellós II	3.51 E-5
CN Trillo	3.86 E-6

8.2.7 Slovenia

Results and insights based on the valid NEK PSA model “NEKC18IA” and 2004 seismic PSA are given.

“NEKC18IA”

Summary of Krško PSA Level 1 and Level 2 results

The contributions from various initiator categories to the total CDF are presented in Table 1.

Table 1: Profile of total “NEKC18” core damage frequency.

Initiator Category	*CDF [1/rcryr]*
Internal initiating events	3,00E-5
Seismic events	5,34E-5
Internal fires	1,25E-5
Internal floods	4,39E-6
Other external events	1,26E-5
Total	*1,13E-4*

Comparison of frequencies of macro-categories based on the sums of RC frequencies (PSA level 2 results) for the three groups of initiators (internal, seismic and internal fire events) is provided in Figure 2.

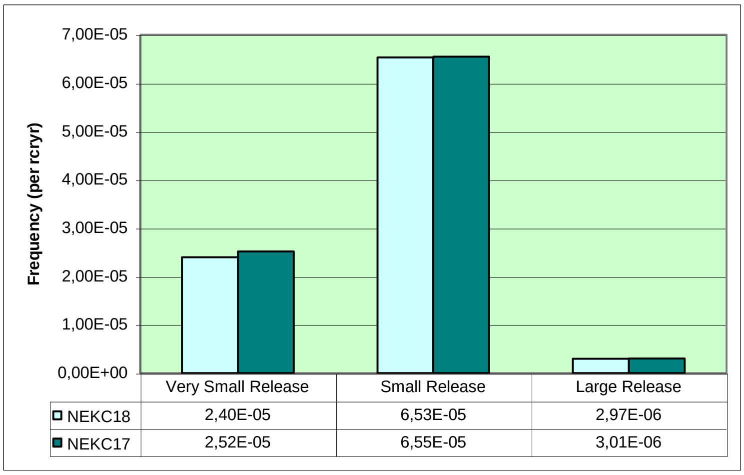


Figure 2: Macro-categories of releases Based on the Contributions from Internal, Seismic and Internal Fire Events for the Cases “NEKC17” and “NEKC18”

Important sequences

The event trees representing the plant response to Internal Initiating Events in the Baseline of the Krško NPP PSA Model “NEKC18IA” contain 176 event sequences that lead to core damage. The most important sequences are: Loss of Offsite Power (5,69E-06 /rcryr), Transient with MFW Available (3,49E-06 /rcryr), Station Blackout (3,28E-06 /rcryr), Small Loss of Coolant Accident (2,16E-06 /rcryr), Transient without MFW Available (2,11E-06 /rcryr). There are 10 sequences, which have frequency above the value of 1E-06 /rcryr. They contribute roughly 75% to the IIE CDF.

Important Internal Initiating Events

The IIE PSA in the Krško NPP Baseline PSA Model contains 16 internal initiating events’ categories. A group of the three most important single initiators is comprised of initiators’ categories Station Blackout (SBO), Transient with MFW Available (TRA) and Loss of Offsite Power (LSP). These three categories contribute cumulatively somewhat more than 60 % to the IIE CDF.

Component Importance

Important components are obtained by calculating the Risk Increase Factors (RIF) of Basic Events. The most important components are the pumps and valves of the Essential Service Water System (ESW) and Auxiliary Feedwater System (AFW).

Sensitivity studies

To provide additional perspective on the results, various sensitivity analyses were performed. The following cases were evaluated:

- Importance and Sensitivity Calculations for Selected Basic Event Groups (results from the analysis are: Risk Decrease Factor – RDF has the largest impact on Human-errors and Diesel Generator groups. Risk Increase Factor has the largest impact on Motor Operated Valves, Air Operated Valves and Human-Errors groups.);
- Unavailability of Equipment Due to Preventive On-line Maintenance;
- Impact of Absolute Cutoff (This sensitivity analysis was performed in order to present the impact of absolute cutoff used in quantification of IIE CDF on its value. The sensitivity analysis demonstrates that absolute cutoff of 1E-10/rcryr for the quantification of IIE CDF had been set appropriately);
- Impact of change in Reactor Containment Fan Coolers success criterion (Level 2);

2004 Seismic PSA

Results

A result of the 2004 seismic PSA study was a significant reduction in the seismic CDF by more than 50%. The CDF has decreased due to new equipment added to enhance safety, addition to the model of some systems previously assumed to be unavailable after a seismic event, and removal of some conservatism in the plant model and data.

Importance Analyses

Importance analyses were preformed in the 2004 seismic PSA study to identify the dominant contributors to seismic CDF. The importance was expressed as the change in CDF when the event was removed from the analysis. The most significant seismic initiating events are seismic station blackout (61.2% change in CDF), seismic loss of off-site power (13.5% change in CDF) and seismic ATWS (10.6% change in CDF). The most important seismic failure events are due to seismic failure of diesel generator control panel (24.6% change in CDF) and seismic failure of the condensate storage tank (11.3% change in CDF). Importance of the operator's actions (fail to switch valve alignment from the condensate storage tank to essential service water brings 5.8% change in CDF) as well as importance of non-seismic failures, where the main contributor is both diesel generators (diesel generator not recovered before core uncovery brings 26.3% change in CDF, diesel generator 1 fails to run 18.6% change in CDF, diesel generator 2 fails to run 18.5% change in CDF,…), were estimated.

Sensitivity Studies

Sensitivity studies indicating the value of further plant modifications were performed in the 2004 seismic PSA study. Modifications like additional third independent full size diesel generator, incorporation of existing small portable diesel generator (DG) to the power positive displacement pump and battery charger, implementation of backup to existing condensate storage tank (CST), addition of nitrogen tanks for operation of pressurizer power operated relief valves and implementation of backup to the existing essential service water (ESW) system, were evaluated. It was evaluated that especially the addition of third large 6.3kV DG (52%) or incorporation of the existing small portable diesel generator would significantly reduce the seismic risk.

Uncertainty Analysis

Uncertainty analyses in the 2004 seismic PSA study were preformed with the combination of uncertainty in the seismic hazard, the fragilities, random failure and human reliability. The predicted seismic CDF was based on the mean seismic curve and mean seismic fragility curves for systems, structures and components. The predicted seismic CDF increased by about 24% if also uncertainty in random failures and human error probability were included. Uncertainty in the seismic hazard and fragility was determined to have a bigger effect than uncertainty in random failure and human reliability.

Summary of main improvements impaired by risk analysis

Improvements based on risk analysis were:

- Internal Events:
    - Modification of air supply for Air Operated Valves 14500 and 14501;
    - Separation of Instrument Air Supply for Pressurizer Relief Valves;
- Seismic PSA study:
    - Improvement of support towers for CCW Surge Tanks;
    - Fixing of Incore Flux Monitoring movable support assembly;
    - Modification of Control Room ceiling to reach the specifications according to regulations for Safe Shutdown Earthquake 0,3g;
    - Improvement of support points and fixing places for different equipment;
    - Improvements in reducing possibility for equipment interactions as a consequence of a seismic event;
- Internal Fire:
    - Modification packages to install fire (smoke) detectors in following areas:
        - Radwaste Building;
        - Auxiliary Building Safety Room Pumps;
        - CC Building pump area, chiller area and HVAC area;
        - Fuel Handling Building;
        - ESW Pumphouse;
        - Main Control Room Panels;
        - IB AFW area and compressor room;
    - Installation of emergency lightning in some areas;
    - Improvement of the Krško NPP Fire Brigade efficiency to:
        - Train Fire Brigade members about the Krško NPP systems and operations;
        - Associate field operators to the Fire Brigade Team;
        - Supplement the Fire Brigade Rooms with Fire Announciator;
    - Implementation and sealing of fire barrier penetrations;
    - Improvement of fire doors between fire areas;
- Level 2:
    - RX Vessel Cavity:
      Level 2 PSA results showed important impact due to changing “dry cavity” into “wet cavity” on containment response and on core damage and fission products release out of containment. The Krško NPP performed the analysis and changed the design in accordance with its results.

- Accident management:
  By using PSA results, the dominant core damage sequences were identified. Response of containment and containment systems to each of these CD sequences was then evaluated. Actions for reducing the phenomenon and undesired consequences propagation were set up in Severe Accident Management Guidelines for the Krško NPP (SAMGs). This represents a direct PSA application.

8.2.8 Slovak Republic

The PSA results of Slovak NPPs have shown us that the safety goals of the regulatory authority are met. The living PSA programs of the plants demonstrate increasing safety of the plants after reconstruction and implementation of the safety measures. The last PSA results from 2006 are presented in the table:

Plant/Unit	PSA Type	CDF for full power operation	CDF for shutdown modes
V1/unit 1	level 1	2.09E-5/y	5.43E-5/y
V1/unit 2	level 1	2.28E-5/y	6.55E-5/y
V2/unit 3	level 1	2.36E-5/y	8.59E-6/y
Mochovce/unit1	level 1	3.67E-6/y	8.93E-6/y

The level 2 PSA results are performed for the Bohunice V1 and V2 NPP. The main results are described below.

Bohunice V1 NPP

Level 2 full power and shutdown PSA was performed for unit 1 of the Bohunice V1 NPP. For the *full power operation* it can be concluded that:

1. The results indicate that, given core damage, there is 25% probability that the confinement will successfully maintain its integrity and prevent an uncontrolled fission product release. After the implementation of the proposed modifications (recovery actions for SGTM and installation of hydrogen recombiners in the confinement this probability will be increased to 74%).
2. The most likely mode of release from the confinement is a confinement bypass after SGTM with conditional probability of 30%. Late confinement failure (after 6 h) at the vessel failure, with a conditional probability of 22%, is the next most likely mode of the fission product release. Finally, the confinement survives with the spray is expected to occur with a conditional probability of 5% per core damage event. The conditional probability for the confinement isolation failure probability without spray is 5%, for early confinement failure at the vessel failure is 4%, for other categories 1% or less.
3. The overall conditional confinement failure probability of 75% by the proposed modifications can be decreased to 26%. For a western plant this value is 16%.
4. The results of the level 2 PSA indicate that there are vulnerabilities in the area of the protection against hydrogen detonation. It requires immediate attention to improve the plant risk profile. In addition, attention must be paid to development of SAMGs in coincidence with the conclusions of this study.

For the shutdown *operating modes* it can be concluded that:

1. The shutdown risk is high for the open reactor vessel and open confinement. The reason is the high core damage frequency in the shutdown operating modes. After implementation of the recommended shutdown symptom-based emergency procedures (see level 1 shutdown PSA study of the plant) significant decrease of the shutdown risk is possible.

2. Installation of filtered venting system in the reactor hall with long term operation could significantly decrease the release magnitudes during the shutdown operating modes.

A number of features were identified through the course of the level 2 PSA which contribute to the performance of the confinement. These include the following:

1. The most important feature of the confinement with respect to the fission product retention is its ability to remain intact in case of the steam over-pressurisation. This construction allows natural deposition mechanisms to remove the airborne fission products from the confinement atmosphere, and provides adequate time for the additional accident mitigation activities to be implemented.
2. Installation of hydrogen recombiners is extremely important for the severe accident conditions. The confinement cannot withstand hydrogen detonation.
3. The inability to get the water into the reactor cavity prevents the external cooling of the intact reactor vessel.
4. The absence of any penetration in the lower vessel head coupled with the natural circulation in the primary system during a high pressure core melt is expected to induce creep rupture failure in the hot leg pipe prior to the vessel failure.
5. Depressurization of the primary system prior to the vessel failure, as a result of the creep rupture failure of a hot leg pipe, should preclude concerns about the high-pressure severe accident phenomena (i.e., ex-vessel steam explosion, direct confinement heating and vessel thrust forces).
6. Retention of the core debris in a dry cavity may induce MCCI melt through the cavity floor if the water cannot cool the core debris.
7. Injecting water through the failed reactor vessel, in an attempt to cool the core debris in the cavity, is advisable and it does not depend on the status of the confinement cooling. Injecting water into a cavity filled with the hot core debris results in the formation of the hot steam. If the confinement cooling is available this steam is condensed. If no confinement cooling is available steaming from the cavity can eventually over-pressurise the confinement but the COFs prevent the confinement failure. The radiological release consequences of inducing a COF opening are expected to be lower than those associated with MCCI failure of the cavity floor.
8. Steam inerting of the confinement during a severe accident cannot prevent hydrogen detonation in the BWST.
9. The insights gained through the analysis of the severe accident progression and the detailed study of the related phenomena has provided a detailed understanding of the plant behaviour under the severe accident conditions. The knowledge developed can form the basis for the future developments in the accident management.

Frequencies and conditional probabilities of large releases for the V1 plant for full power operation:

<u>Frequency of </u>early confinement failure and bypass and isolation failure: 1.22E-5/y

<u>Exceedence frequency for </u>1% release: 6.0E-7/y and 10% release: 9.0E-6/y

<u>Conditional probability of exceeding:</u>

1% release given core damage: 0,03

10% release, given early confinement failure and bypass and isolation failure: 0,43

The results presented above are not available in the level 2 PSA study of the Bohunice V2 NPP.

<u>Bohunice V2 plant</u>

- For power operational states the key confinement failure modes are attributed to hydrogen burn during in-vessel phase and cavity door failure due to loads at vessel failure. The high pressure Plant Damage States (PDSs) are dominant for early confinement failure.

- For shutdown states the dominant risk contributors are vessel open/confinement open states. This is attributed mainly to the high core damage frequency for the mid-outage states and disabled barriers during these states.
- A number of severe accident management (SAM) measures were investigated as sensitivity analysis and they all appeared to be beneficial plant improvement options. The SAM options studies included: RCS depressurisation, cavity flooding and hydrogen control. These measures are being considered for the V2 SAMG development.
- Implementation of RCS depressurisation (following the EOP FR.C-1 procedures) reduces the cavity door failure frequency but increases the frequency of low release end states through melt-through confinement failure.
- Implementation of cavity flooding with independent system reduces the vulnerability to cavity door failure, by reducing the number of sequences with vessel failure.
- Implementation of an effective system for hydrogen control would be beneficial in reducing contribution of very early confinement failure. This measure should be combined with one of the others providing protection against cavity overpressure.
- The radiological risk at shutdown operational states is significant and preventive EOPs are of high importance and beneficial.

8.2.9 Netherlands

Borssele

Level 1 results:

TCDF all Plant Operating States = 2.65 E-6/year

The contribution from:

Power POS:	81.4%
Midloop:	11.4%

The contribution from:

Internal Events:	20.2%
External Events:	67.6% (mainly external flooding and external gas cloud explosions/fires due to shipping accidents on adjacent river)
Area Events (internal fire and flooding):	12.3%

Power POS is dominated by External events (81%)

Cold shutdown POS is dominated by LOCAs (55%)

Midloop POS is dominated by Area Events (74%) and LOCAs (14.5%)

Level 1 Insights

The dominant contributors to the total core damage frequency are the flooding scenarios. This is the result of the relatively large failure rate of the surrounding dikes and the fact that with the current amount of diesel fuel the plant can only sustain 24 hrs, within which a refilling of the diesel tanks should take place. Because dike failure is likely to be accompanied by harsh weather conditions and together with the surroundings being flooded, this refilling is relative likely to fail. This results in a large contribution to the TCDF.

A cargo ship gas explosion failing the containment and the bunkered building makes up a significant portion of the risk to Borssele NPP. The gas explosion will cause the containment building to fail (collapse), debris penetrating the inner steel shell will fail the primary systems, resulting in no systems being available to mitigate the accident, and a non-isolable open containment building.

For the midloop POS spatially dependant events dominate the results due to fire scenarios failing the residual heat removal systems. The one alternative system available for residual heat removal, reserve-cooling system (TE), is a single train system requiring manual actuation.

The thermal-hydraulic runs yielded several insights. For the Power POS upon loss of all cooling, core uncovery comes between one-half and three hours after the initiating event with vessel breach at 5 – 16 hours. The containment does not over-pressurize, even during a LOCA, until after 5 – 6 days. Additionally, success of one TW pump (Bunkered primary reserve injection system; see figure 1.) is sufficient to delay the onset of core damage. In midloop, opening the reactor coolant system vents essentially makes the reactor coolant system behave as if the head is off, losing inventory faster. In the early phases of midloop, loss of all cooling leads to boiling at 20-25 minutes after the initiator and core uncovery occurs at 4 hours. In late phases (after refuelling), core uncovery extends to 30 hours. If the bunkered reserve injection system (TW) is successful in injecting, there is at least 15 hours for recovery actions to occur.

Level 2 results:

Time Phase	STC	Percent of total	Containment release mode
Early releases **(0 – 12 hours following reactor trip)**	1	0.06	Dry SGTR without isolation
	2	0.01	Dry SGTR with isolation
	3	0.90	Induced SGTR with secondary water
	4	0.08	Containment rupture
	5	0.44	Containment leak
Late releases **(12 – 72 hours following reactor trip)**	6	0.24	Interfacing systems LOCA
	7	0.01	SGTR without secondary water
	8	0.94	SGTR with secondary water
	9	0.05	Containment rupture
	10	0.18	Containment leak + isolation failure
Very late releases **(> 72 hours following reactor trip)**	11	0.11	ISLOCA + isolation failure
	12	0.01	SGTR with and without secondary water
	13	0.07	Containment rupture and leak
	14	0.07	Basemat penetration
	15	80.18	Filter vented release
No release	16	16.65	No containment failure

Early releases account for 1.5% of total, with induced failure of steam generator tubes contributing to 60% of these cases. Leakage of the containment occurs in 30% of these cases. Containment rupture in the early phase is dominated by external events, which fail containment directly and account for 5%

of the early releases. Finally, SGTR accidents without water in the secondary side, but which are isolated contribute for 3.9% of the early releases and those without isolation contribute 0.7% of the early releases.

Late containment failure is dominated by containment bypass failures, representing almost 30%. These cases are divided between interfacing systems LOCA sequences (17%) and LOCA sequences with a loss of containment isolation (12.6%). Steam generator tube rupture (SGTR) sequences account for 67% of the late containment failure.

HFR

Prior the modifications the core damage due to internal events was: 5 E-5/year

Due to internal fire and flooding:	1.9 E-5/year
Frequency of fuel damage but primary still intact:	6. E-5/year

From the 18 quantified initiating events 4 dominated the CDF (87%):

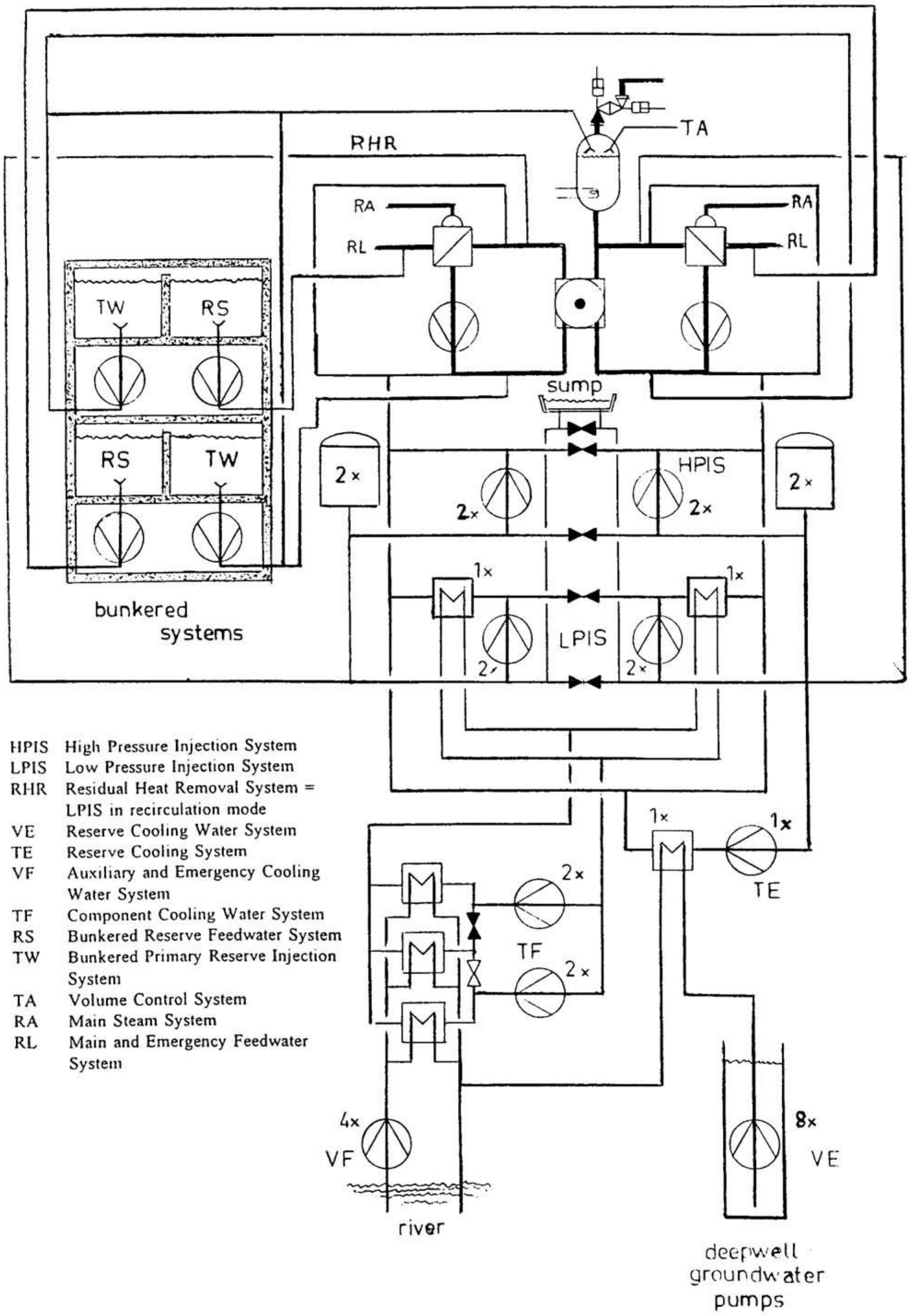
o Fire:	1.9 E-5/year (27%)
o Large LOCA outside pool on pressure side of pumps:	1.8 E-5/year (26%)
o Drop of heavy load above spent fuel pool, thereby damaging primary piping below pool:	.8E-5/year (26%)
o Loss of offsite power:	5.8 E-6/year (8%)

Local fuel damage mainly due to partial blockage of the core.

In case of a large break LOCA in the lowest part of the inlet piping, flow reversal due to the siphon effect, would cause the reactor core to be uncovered within 5 minutes.

After several modifications (e.g., installation of additional vacuum breakers on the primary system to avoid that the core would be emptied due to the siphon effect, as well as limitation of portal crane movement above the pool during power operation) the CDF changed from 6.9 E-5/year to 2.4 E-6/year:

Internal events:	1.2 E-6/year
Internal fire and flood:	1.2 E-6/year
Still 4 IEs contribute 86% to CDF of	2.4 E-6/year
o Fire:	1.2 E-6/year (49%)
o Medium LOCA outside pool in inlet:	3.1 E-7/year (13%)
o Medium LOCA outside pool in outlet:	3.1 E7/year (13%)
o Loss Of Offsite Power:	2.6 E-7/year



- (11%)

Figure 1. Safety Systems Borssele NPP

8.2.10 Mexico

The CNSNS developed a Probabilistic Safety Assessment (Level 1 and Level 2) in order to have an independent model to evaluate PSA applications as well as to compare the main results of the Individual Plant Examination (IPE) developed by the utility. The NSAC-159 methodology was selected by the utility to perform the back-end portion of the IPE, whereas the CNSNS used the NUREG-1150 methodology to perform level 2 PRA model. In order to calculate the source terms, CNSNS used the MELCOR code to simulate the evolution of selected severe accident sequences and a plant specific XSOR type of code, and the utility used the MAAP code for severe accidents simulations and the methodology presented in NUREG-1228 to obtain the source terms.

The IPE for Laguna Verde Nuclear Power Plant identified two vulnerabilities or weak points in the design and operation. One related to the high contribution of the station blackout scenarios (81%) and the other to the potential occurrence of the interface LOCA with a 10% contribution to the total CDF. There is a possibility of an interface LOCA in the Laguna Verde NPP if a failure in the check valve of the low pressure injection systems occurs in combination with an operational event that generates a signal to open the motor operated injection valves when the reactor is at high pressure. The opening of the injection valves results, due to a differential pressure permissive across the valve. The licensee submitted a plant modification package aimed to solve this vulnerability. The modification involves the change in the injection valves permissive from a differential pressure to a reactor low pressure. This modification reduces the possibility of occurrence of the interface LOCA, and thus reduces 8.4% the core damage frequency for Laguna Verde NPP.

The regulatory PSA level 1, estimates the point core damage frequency for Laguna Verde NPP unit 1 in 5.6x10-5 per year which is 10% less than the figure obtained in the IPE (6.18x10-5 per year). The accident sequences that most contribute to the total CDF are station blackout accidents in the same percentage reported in the IPE, transients without SCRAM (ATWS) contribute with 13%, and transient induced LOCA contribute another 4.6%.

The CNSNS study yield for the containment failure frequency 5.25E-5 compared with 2.59E-05 in the IPE. In both cases the dominant failure of the containment was by leak or rupture. For cases with containment without failure, the conditional probability was 0.07 in the regulatory study and 0.19 for the IPE. This difference, also present, in the containment failure frequency was the result of not taking into account the by-pass of the containment in the CNSNS study, and therefore resulting in a higher contribution to the failure containment by overpressure instead of by failure of containment isolation. The dominant containment failure time was at or after vessel breach with a conditional probability of 0.6. In the IPE for Laguna Verde the opening of the main steam isolation valves (MSIV´s) for venting the reactor vessel during primary containment flooding scenarios was taken into account and was identified as the most important contributor to containment by-pass. The CNSNS studies as well as other PSA studies do not consider this option.

The Large Early Release Frequency estimation for the CNSNS study and the IPE become: 1.02E-8 (less than 6 hrs and more than 10% of Cs-I) and 3.4E-7 respectively. Nevertheless the dominant radioactive release was in the intermediate period with a conditional probability of 0.7 (from 6 to 24 hrs). The largest source terms in both studies are associated with the Station Blackout scenarios. The dominant failure location is in the drywell.

8.2.11 Korea

The PSA have several purposes. The important purposes are to verify the safety of the NPP, to identify the vulnerabilities of the plants and to recommend the resolutions for the vulnerabilities. Since the first PSA was performed for Kori units 3&4 in 1992, twenty operating plants in Korea have completed PSA for the safety verification and improvement in operation or maintenance. Also, six plants under the construction or preparation are now performing the analyses.

The internal event analysis was performed to estimate the frequencies of the accident sequences that result in a severe core damage, to identify the dominant accident sequences contributing to the core damage, and to provide the valuable insights in performance improvement to the utility. The trend in the core damage frequency is decreasing as the plants are evolved.

Kori units 1&2 and Wolsong unit 1 were designed and constructed in '70 to early of '80. The PSA results for those NPPs show the comparable figures of worldwide accepted safety goals. This compels the utility to reinforce the safety by modification or addition of the safety systems and improvement in operation or maintenance. One example is additional installation of the Alternate Alternating Current (AAC) source for the electrical stability improvement. Kori units 3&4 and following Korean standard plants constructed from mid '80 to '90 show the enhanced safety characteristics to meet the recommended safety goals. Nowadays, Korea has the improved design plants such as OPR1000 (Optimized Power Reactor 1000) or APR1400 (Advanced Power Reactor 1400).

Some plants have performed their PSAs using the operating data with the consideration of generic data such as NUREG/CR-5750 in the initiating events and the domestic specific experience data in LOOP, etc. The other plants have used the generic data such as EPRI URD (Utility Requirement Documents) database. Also, the common cause factors are based on NUREG/CR-5497 and EPRI URD. The HRA is based on SHARP/THERP except the HCR (Human Cognitive Reliability) in a diagnostic stage of the analysis in Kori units 3&4 and Yonggwang units 1&2. The seismic event analysis was performed using the seismic PSA or seismic margin analysis.

The high reliability in high pressure injection system (HPIS) is embodied in the common configuration of the normal charging function. In view of the secondary system reliability, the changeover between the sources for auxiliary feedwater system showed high reliability. Also, on contrary to the design philosophy of the separation, the cross-tie or common piping and distribution system showed the high confidence in system functions.

The component cooling or service water system with a multiple train is needed for the maintenance flexibility as well as the reliability purposes. The other systems contributing to the plant safety are the AAC generator, the battery system with a large capacity for the satisfaction of the SBO (station blackout) rule and AMSAC (ATWS mitigation system actuation circuitry) or DPS (diverse protection system) for the ATWS (anticipated transient without scram) rule.

The characteristic on the general system arrangement is usually not to allow the shared system between the plants except the rad-waste treatment system. All Korean plants are located in the costal area to use sea water for cooling the plant components, and this causes the external hazards such as typhoon and foreign materials considered as the risk concerns. The divisional area concept is progressed to separate a compartment to the quadrant configuration. The compartment type of Kori units 1,2,3&4, Yonggwang units 1&2, Wolsong units 1&2 and Ulchin units 1&2 shows lower degree of safety to the external events. Some more enhanced configurations are reflected on the all Korean standard plants. The most evolved quadrant arrangement is employed in Shin-Kori units 3&4. The containment structure consists of the concrete reinforced with steel rods in all domestic plants except the Kori units 1&2. Kori units 1&2 have a containment structure surrounded by an environmental concrete shield with the steel liner.

The external events considered in PSA for Korean NPP are earthquakes, internal fires, floods, and other external accidents which are usually screened out in the qualitative stage of analyses. The quantified results for the external events are relatively high when compared with those of internal events in the older plants, but the values are diminished as the plants are optimized. Also, the results of external events cannot be considered with the same level of scrutiny due to the large inherent uncertainties in the external events analysis.

The goal of Level 2 PSA or containment performance analysis is to assess the containment performance for the mitigation of the severe accidents and consequent radiological source term characteristics. Currently, large early release frequency (LERF) is an immediate goal for the Level 2 PSA. It shows that LERF is in the range of 0.1 by virtue of the advanced design features such as the cavity configuration, hydrogen igniter and cavity flooding system, etc.

Shutdown PSA is performed for Yonggwang units 5&6 and Ulchin units 5&6 as a license requirement at the construction stage. The results show that the improvement for the pressurizer safety valve test in operation mode 2 and the operational alertness in mid-loop operation are needed.

The lessons learned from the domestic PSA can be summarized as follows. 1) The PSA results are enough for verification on the safety and identification on the plant level vulnerabilities. 2) As generally observed, the unexpected trip frequency in Korea is remarkably decreased, and the result is reflected in the living PSA model. 3) The methodology and technique on PSA are now evolved into the risk monitoring system focused on the maintenance and performance improvement. 4) For these goals on the PSA usage, database development for the domestic plants and improvement of the PSA quality are needed and must be commenced by industries as soon as possible.

8.2.12 Japan

Industries in Japan implemented AM countermeasures to all of conventional LWRs by the end of March in 2003 under the strong recommendation by NISA. In addition, Industries provided the PSA results to the conventional LWRs after the implementation of AM. NISA and JNES reviewed the AM implementations provided by Industries in a point of view on no-adverse effects and its effectiveness through PSA results.

Figure 1 shows core damage frequencies (CDFs) and its containment failure frequencies(CFFs) for conventional 52 NPPs after implementations of AM. The PSA results showed CDFs of 52 NPPs were less then 10-6(1/r.y) and CFFs were less than 10-7(1/r.y).

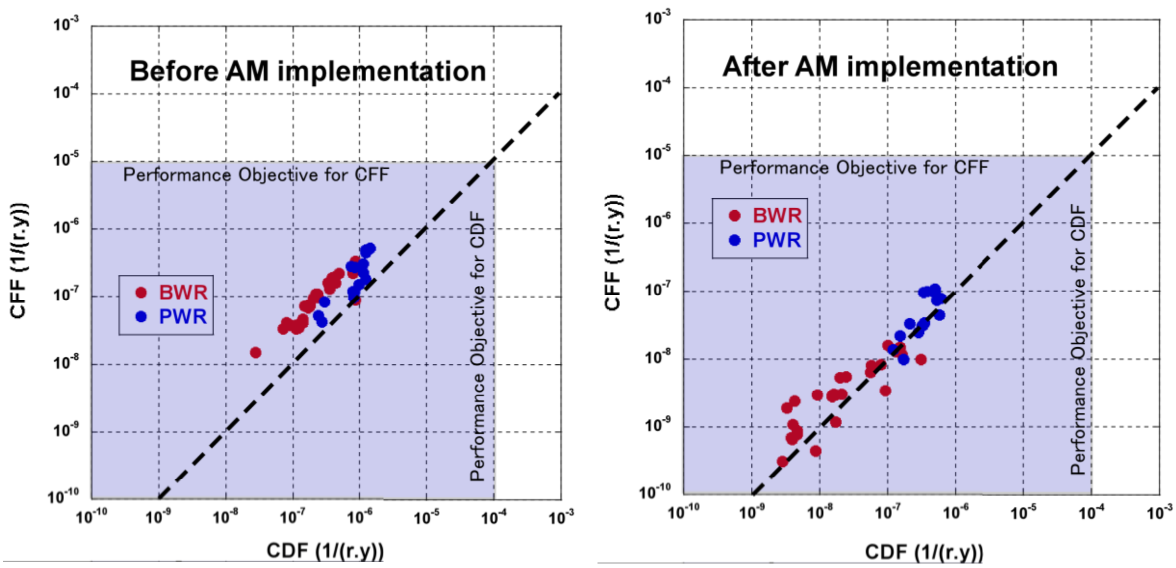


Figure 1. CDF & CFF for Conventional LWRs in Japan after AM Implementation

The latest PSA update was completed in 2003 and the results are listed in appendix A. Core damage due to seismic and external fire is the major contributors to CDF for all operating NPPs. The results from Kuosheng also indicate that the events of lost of safety-related DC buses are most important initiators during power operation. After collecting plant specific operating data from 1994 to 2002, most initiating event frequencies and component failure probabilities are lower than the generic data after Bayesian update. The frequency of loss of off-site power is one of the interest exceptions. Due to the large power demands in north Taiwan, the electric power generated in south Taiwan has to be delivered north along the power grid across the high mountains. The existing plant operating data showed that the frequent significant earthquake impact directly on plant or on power grid would have high likelihood to cause the loss of off-site power event. The solution of the problem is to improve the strength of power grid against any external perturbation such as seismic, typhoon or significant imbalance between power generation and demands.

8.2.13 Italy

Not applicable.

8.2.14 Hungary

Level 1 PSA for the Paks NPP

The existing unit specific level 1 PSA studies are updated annually. The risk figures are comparable for the different units. The latest analysis results (2005) for a reference unit are as follows:

Power operation

internal initiators: $9.6 \cdot 10^{-6}$ 1/year

fires: $2.6 \cdot 10^{-6}$ 1/year

internal floodings: $4.1 \cdot 10^{-6}$ 1/year

seismic events: $6.6 \cdot 10^{-5}$ 1/year

Shut down mode

internal events: $5.9 \cdot 10^{-6}$ 1/year

Some of the improvements that either were initiated by the PSA results ore were found effective in risk reduction are listed here:

- Relocation of emergency feed water system, at the recent location the system is now protected from hazard of high-energy line breaks and of fires and floods in the turbine hall;
- Protection of containment sump against clogging with redesigning of the sump strainers;
- Prevention of the refilling of the tanks of the low-pressure emergency core cooling system after they have been emptied;
- Elimination of the so-called artificial voltage cutting;
- Modification of the primary pressure relief system, introduction of “bleed and feed” possibility, realisation of a protection against cold overpressure;
- Modification of the reactor protection system with introduction of new protection functions and operating conditions, applying consistently specific design principles;
- Improvements in the emergency operating procedures (developing a full set of symptom oriented procedures);
- Reduction in probability of dropping a load during lifting and moving heavy equipment in the reactor hall by upgrading the 250te cranes (replacement of the lifting eye and the ropes with higher grade materials) and changing the load path;
- Upgrading the passive fire protection on different cable trays, (including the control room electrical cabinets). Installation of an automatic fire suppression system over the turbine oil and generator hydrogen fires. Relocation of air intake grills from the turbine hall.
- Increasing the seismic resistance of the plant (establishing the safe shutdown and heat removal technology, upgrading the seismic capacity of systems and structures which are essential to ensure seismic safety, installation of seismic instrumentation).

Level 2 PSA for the Paks NPP

The main objectives of the level 2 PSA study carried out for a reference unit were: (1) to provide a basis for the development of plant specific accident management strategies, (2) to provide a basis for the plant specific backfit analysis and evaluation of risk reduction options, and (3) to provide a basis for the resolution of specific regulatory concerns.

As the quantitative results, the annual frequencies of large radioactive releases for 13 different predefined release categories were calculated. The severity of the categories was correlated to the amount of the caesium released. Events of only three release categories may have severe consequences (releases higher than 1000 TBq Cs). The frequencies of the presumably most dangerous accidents (high energy reactor pressure vessel damage) are low, around 10^{-7} 1/year. The second (containment bypass due to primary-to-secondary leaks) and the third (early containment failure caused by hydrogen burn) release categories have together around $5 \cdot 10^{-6}$ 1/year frequency for the full power operation without any accident management assumed. For these two category events accident management and the corresponding hardware modifications are under preparation. According to the estimation the release frequencies of accidents in the shut down states and accidents of the spent fuel storage pool are relatively high.

The risk reduction capability of different accident management possibilities has been assessed. The accident management program is submitted to the regulator, the review process is ongoing. This program comprises hydrogen treatment by using recombiners, flooding of the reactor shaft for the external cooling of the reactor vessel or for protecting the basemat from melt through, filtered venting, prevention of the rector shaft door damage as mitigative measures. A number of other improvements, mostly preventive measures are suggested to decrease the frequencies of bypass sequences (i.e. blowdown of the secondary side of the SGs directly to the containment) and decrease the accident initiating frequencies in the shut down states and of the spent fuel pools.

8.2.15 Germany

Results of PSAs for all German NPPs show that the frequencies of core damage are well below the orientation value recommended by the IAEA for NPPs in operation.

Up to now, most PSAs for German NPPs have been performed voluntarily by the utilities or as research projects by GRS. However, several safety related modifications in systems design and operational procedures are based on PSA insights or are a result of recommendations of the German Reactor Safety Commission RSK. Insights and resulting modifications range from major safety issues, e.g. the importance of small leakages compared to large ones or the importance of steam generator tube rupture, to small but effective changes in the timing of test intervals or of operational procedures.

Examples of modifications are:

- Several modifications to control a steam generator tube rupture including I&C functions and automatization of 100 K/h cooldown to cope with a small LOCA (PWR):
- Introduction of emergency operator manual with AM procedures (PWR and BWR);
- Design of components to meet AM requirements, e.g. qualification of pressurizer valves to release wet steam and water (PWR);
- Improvements to prevent/limit internal floods (PWR and+ BWR);
- Additional shutdown line at the level of the feedwater line nozzles (BWR).

The most expensive modification was the installation of an additional decay heat removal system ("ZUNA") for the two units of BWR-72 (Gundremmingen NPP, units B and C). In most cases, safety improvements have been realized by inexpensive modifications. According to the requirements of the updated German PSA Guide many utilities are performing or have just performed a low power and shutdown states PSA. Particularly this PSA part has caused a lot of operational changes in the focus of the safety status in the different plant operation states.

Insights gained from PSA confirm the necessity to supplement the deterministic safety assessment by the probabilistic approach. This can be demonstrated by the design of the feedwater supply to the steam generators. The PSA has shown that the unavailability of the feedwater supply function (including the main feedwater supply, the emergency feedwater supply, and the start-up and shutdown system), in the original design of the German NPPs would dominate the core damage frequency, if only the deterministic requirements for this system function would be accomplished. Fortunately, the feedwater supply has been toughened up for most German PWRs by installing an additional independent emergency system ("Notstandssystem") as protection against external impacts. A vital part of the "Notstandssystem" is the highly redundant emergency feedwater supply system. The redundant strands of this system are consequently separated from each other, physically protected and equipped with their own diesel generators.

8.2.16 France

The results of the 1990 PSAs (level 1, internal events, all plant operating modes) were the following:

900 MWe plant: CMF = 5. 10-5 / reactor x year

1300 MWe plant: CMF = 1. 10-5 / reactor x year

The most outstanding result was the high contribution of shutdown modes (32% for the 900 MWe plant and 56% for the 1300 MWe plant). These studies led to many applications for safety improvement (see section 7)

These studies were updated by both IRSN and EDF. Moreover the scope was extended by the level 2 (IRSN and EDF) and by the Fire PSA (IRSN).

The updated studies (see section 5) take into account all the plant modifications in design and operation, as well as the evolution of knowledge and data (in particular success criteria were revised and new sequences were identified). For these reasons the results of the updated studies are not directly comparable to previous results.

For the recently updated EDF PSA (internal events, all plant operating modes),.the order of magnitude for CMF is less than 10-5/ry and for LERF is less than 10-6/ry.

Discussions are still in progress between IRSN and EDF for some sequences for which functional assumptions need some complementary analysis and justification.

8.2.17 Finland

Summary of Loviisa PSA programme

Since 1994 Fortum (former IVO) has submitted to STUK the updated risk analyses on harsh weather conditions, internal flooding, fire, shut down mode and internal initiators where the aforementioned plant changes are embedded in. The latest analysis results (2006) are as follows:

Power operation 3.9 x10^{-5}/a
- internal initiators, 8.4x10^{-6}/a
- fires, 1.6x10^{-5}/a
- internal floodings, 4.2x10^{-6}/a
- harsh weather conditions, 7.4x10^{-6}/a
- seismic events, 3.4x10^{-6}/a

Shut down mode 4.3 x10^{-5}/a
- internal events, 3.5x10^{-5}/a
- flooding, 4.8x10^{-7}/a
- harsh weather conditions, 7.4.x10^{-6}/a
- seismic events, 2.3x10^{-7}/a

Fortum submitted also the level 2 PSA to STUK which showed that the probability of large release (atmospheric release of Cesium-137 is more than 100 Tbq) is about 9.3x10^{-6}/a covering internal events, internal flooding and harsh weather conditions at power operation. The majority of the risk comes from leaks between primary and secondary circuits and other by-pass sequences of the containment.

Major risk informed plant and procedural changes

Internal Initiators

The original results of the Loviisa level 1 PSA (internal initiators) submitted to STUK in 1989 resulted in immediate measures at the plant, since one initiating event caused 73 % of the total core melt frequency (1.7E-03 1/a).

- In the original level 1PSA the dominating event was a loss of cooling of electrical and control instrumentation room. The ventilation system of this room had only one train equipped with cooling unit. The assumption that the control of whole plant is lost, if the temperature exceeds the design limit of control instrumentation led to the aforementioned high core damage frequency. A quick demonstration showed this assumption to be overly conservative, since the air-cooling is necessary only during the hottest summer days, which are infrequent in Finland. Most of the year, the cooling could be managed by blowing the air also by two normally standby fans without a cooling unit. A quick review of the accident sequence assured as well, that the auxiliary feedwater system could be manually operated even though the automatic control would be lost. These corrections updated the core melt probability of the respective initiating event to 3.3E-04 1/a, and the total core melt probability to 9E-04 1/a.

Instead of further analysis, immediate actions were tackled to redesign the air cooling system and to install an additional 100 % capacity diverse cooling unit. The redesigned system decreased the core damage frequency resulted from the loss of instrument room cooling to 1.2E-05 1/a and the total core damage estimate to 6.0E-04 1/a.

Improvements have been made in several other systems causing high probability core damage frequencies such as

- primary circulation pump seal system
- service water system
- minimum circulation of ECC system.

All the aforementioned systems suffered from design flaws which could be eliminated by cost-effective modifications.

- The redesigned back-rotation prevention system and a new stop signal activated by low flow in seal cooling system for primary circulation pumps (PCP) and improved operator instructions for avoiding seal LOCA decreased the frequency of the respective accident sequence from 2E-04 1/a to about 1.0E-05 1/a.

- The redundancy of the service water system was improved by changing base states of a few valves. This change eliminated the total loss of service water system in case of a pipe break and decreased the core damage frequency caused by the loss of service water from 1.3E-04 to 1.9E-05 1/a.
- An important design flaw was found in ECC system leading to high frequency accident sequence. If the closing valves in the minimum circulation lines fail to close on demand, the sump line valves and suction line valves may shift back and forth due to the suctions cycling between water tank and sump. The closing valves in the minimum circulation lines were replaced by more reliable type of valves in order to prevent the ECC water backflow to ECC tank. This change reduced the core damage risk from 5.4E-05/a to 1.4E-05/a in LOCA cases.
- Back up battery supply for PCP seal cooling outlet valves reduced the seal LOCA contribution to the core melt in case of the loss of offsite power.
- Automatic actuation of an alternative cooling path for the seals via the makeup and boron system
- the modification reduced the risk from harsh weather conditions and flooding no less than 63% and 80%, respectively
- the modification reduced the risk from fires only 3%

Several improvements have been made in emergency operating procedures such as refilling of the ECCS tank in case of multiple steam generator tube ruptures, primary circuit depressurisation and ATWS management.

Related to the steam generator tube and collector rupture the isolation of the steam generator can be made both at primary and secondary side. The isolation made at primary side interrupts the leakage with certainty but the reliability of the main isolation valves is questioned, due to sparse data.

In order to reduce the risks resulted from the tube and collector ruptures in steam generator the following back fittings have been implemented:

- The reliability of pressurizer sprays are improved by installing new pipelines from ECC system to pressurizer sprays to back-up the normal pressurizer
- sprays from main coolant pumps.
- New protection signal activated by high water level in the steam generator (steam generator tube rupture) will close the main steam line and the main feedwater line and to stop the respective main cooling pump.
- Additional ECC water tank has been build up to maintain the volume of primary circuit in case of a rupture of steam generator tube.
- New protection system to control the level of radioactive substances in the secondary circuit has been assembled. This system is to alarm in case of tube ruptures in steam generator.

The aforementioned changes lowered the risks of steam generator tube ruptures from 1.6E-04/a to 1.4E-06/a.

- To improve the reliability of ECC system, minimum flow lines downstream the ECC pumps to the ECC injection water tank have been replaced by new lines with heat exchangers leading from the pumps forcing side directly to the suction side. The failure of former minimum flow line valves could lead to refilling of the ECC injection water tank, alternating of the line-up of the ECCS suction between the tank and the sump, and possible additional valve failures.

Fires

Fire safety improvements implemented during fire PSA project:

- fire insulation and sprinkler protection of service water system control and electrical cables
- fire protection of pressure measurement transmitter of service water system
- fire insulation of control and electrical cables of primary circulation pump sealing system
- fire insulation of control cables of electrical building ventilation and cooling system
- fire safety improvement of safety related pressure air pipe
- sprinkler protection of hydraulic oil stations of turbine by - pass valves
- double piping of high pressure hydraulic oil pipes to prevent spreading of high pressure oil leaks and jets to the surroundings

Internal floods

Flood improvements implemented during internal flood PSA project:

- construction of flood wall in cable tunnels between turbine building and reactor building to prevent flood spreading from turbine building into reactor building where flooding can damage primary circulation pump seal cooling system and emergency cooling pumps
- prevention of flooding and floor overloading in cable spreading rooms below electrical rooms and main control room
    - improving capacity of floor drainage
    - removing of cooling water pipeline
    - installation of remote controlled motor valves to isolate sprinkler system in case of false actuation
    - change actuation mode of sprinklers system from automatic to manual
- – prevention of flooding on feed water tank floor level
    - replacing of feed water pipes with pipes of better material
    - installation of jet shelters and whip restrainers
    - coating and sealing of floor level to be water tight
    - installation of new drainage of high capacity
    - relocation of pressure transmitters into higher location above postulated flood level

Harsh weather conditions

Sea vegetation can cause a blockage of chain basket filters in seawater channel.

- To reduce the risk of filter breaks due to high pressure difference over filters and to prevent the consequent access of algae to the main circulating and service water system an automatic power and flow reduction system has been installed
- In addition, a line for seawater intake from the outlet side will be taken into operation in 2007 to ensure seawater supply to the service water system.

Blockage of air in-take of diesel generator by snow or freezing rain during a storm can result in a loss of emergency diesel system.

- In case of blockage of the normal air intake, combustion air can be taken from the DG rooms.

<u>Summary of Olkiluoto PSA programme</u>

Since 1994 TVO has submitted to STUK the updated risk analyses on harsh weather conditions, internal flooding, fire, shut down mode and internal initiators where the aforementioned plant changes are embedded in. Since 1995 some major plant changes have been made in order to compensate the power upgrade (TVO is applying for Operating Licence for upgraded power of 115%):

- two diverse safety relief valves have been installed to upgrade the reactor overpressure capacity and to enhance the system reliability as well
- the hydraulic protection and control system of turbine has been replaced by a system based on digital and analog electronics
- Inertia of main coolant pumps has been increased and the control system has been replaced by digital and analog electronics

In the newest version TVO has refined the PSA model and reduced some overly conservative assumptions used in PSA. The latest analysis results are as follows:

TVO submitted to STUK also the level 2PSA which showed that the average probability of large release (atmospheric release of Cesium-137 is more than 100 Tbq) is about $4x10^{-6}$/a. The majority of the risk comes from early high pressure transients and the remainder mainly from low pressure transients and the shut down mode initiators.

Power operation

- internal initiators, $7.9x10^{-6}$/a
- fires, $3.5x10^{-7}$/a
- internal floodings, $1.2x10^{-7}$/a
- harsh weather conditions, $1.2x10^{-6}$/a
- seismic events, $5.0x10^{-6}$/a

Shut down mode

- internal events , $1.7x10^{-7}$/a
- fires, $8.4x10^{-9}$/a$x10^{-9}$/a

Major risk informed plant and procedural changes

Internal Initiators

The original results of the OL level 1 PSA (internal initiators) submitted to STUK in 1989 resulted in some plant changes:

- TVO has improved the water level measurement system to prevent the water from boiling in the reference piping and to ease the surveillance test of the system, because for example the function of auxiliary feed water system is controlled by water level in reactor vessel.

- Mussels capture strainers were installed into the sea water cooling channels in order to prevent mussels of blocking the intermediate cooling and dieselgenerator cooling heat exchangers (weak link to risk assessment)

- In 1994 STUK required that the lower air lock will be kept closed during the refuelling outages when the maintenance of the main coolant pumps is underway, because the maintenance work can results in large bottom LOCA in the reactor tank. If large bottom LOCA takes place and the lower air lock remains unlocked, the coolant escapes out of the containment and prevents adequate core cooling function which leads to core uncovery and core damage within few hours.

- the connections of the plant to the outside grid are upgraded by installing a new additional start transformer and improving the plant connections to the hydro power plant

New EOPs have been made as follows:

- refilling of the EFW tank and condenser
- cross-connection of the diesel generators of neighbouring plant units
- manual depressurization of the reactor tank from the relay room.

Harsh weather conditions

In the spring 1995 TVO PSA was revised due to two weather related phenomena which took place at TVO plant. In February 1995 snow storm blocked the air intake filter of air suction channel to diesel generators which stopped two diesels of running in surveillance test.

- To upgrade the reliability of DG system, dampers opening automatically on pressure difference were installed to enable the taking of the combustion air directly from DG rooms

In January 1995 sub-cooled seawater blocked coarse bar screen in the inlet channel of service water system which is vital to emergency core cooling systems

- To reduce the risk from the crystal ice, a system circulating warm water to the intake of sea water channel has been installed. The system is to prevent crystal ice formation in the coarse bar screen and its blocking

Modelling of these two CCF type of phenomena contributed to TVO PSA core damage frequency an increment no less than 1.9x10-5/a. The total core damage frequency including all identified initiating events and changes made due to the regulatory review was 3.34x10-5/a. The defence against the aforementioned type of external initiators has been introduced with respective plant changes which lowered the core damage frequency back to the almost preceding level.

Seismic

Seismic risk analysis resulted in some plant changes. The major contributions to seismic risk came from loose anchoring of diesel generator battery system and of some electronics cabinets.

To reduce the risk, the battery system will be supported by surrounding frame which prevents the batteries falling down from their foundation. The electronics cabinets will be adequately anchored to solid structures

After the implementation of these plant changes the contribution of seismic events to the core damage probability is about 4x10-6/a.

8.2.18 Czech Republic

<u>Summary of Dukovany site</u>

The basic living PSA models and related PSA applications tools are at Dukovany site updated regularly since 1996. The latest analysis results (end of 2005) are as follows :

Level 1 PSA - for a list of analyzed initiating events /fires, floods and heavy load drops included/ and all operating states CDF is 4,5x10-5/y. * The CDF for unit operation at power is 7x10-6/y.

Main contributors /85 % CDF/ of Dukovany risk level are :

- loss of natural circulation,
- LOCAs initiators,
- heavy load drops,
- cold overpressurization,
- and main steam collector breaks.

- Within the loss of coolant accidents the dominant contributors are small, medium and large LOCAs which contribute more than 20% together.

Plant operating states with the highest contribution to the CDF are :

- POS 1 - Power and low power operation / 100% - 2% of nominal power/
    - contributes 25% of the CDF
- POS 8 – RCS Drainage before refueling
    - Contributes 32% of the CDF

Level 2 – for unit at power operation an estimation of LERF is 1,1x10-6/y *

* *CDF at power is* $7x10^{-6}/y$

Three levels of containment failure are distinguished in Level 2 PSA – a rupture, a leak and no failure. They can be early, i.e. before or within 2 hours after vessel bottom head failure (about 8 to 20 hours after accident initiation) or late, i.e. after this time. Activity release is also traced. Large Early Release Fraction (LERF) means the release of iodine or other elements (except noble gases) exceeding 10% of initial inventory early. On the other end of the release scale is the “very low” release with less than 0.1% of cesium inventory.

A relatively large fraction of early containment rupture, 13.3 % of CDF is indicated, it is almost entirely due to hydrogen large deflagration or DDT (11.6 %). The rest is due to initial isolation failure, 1.1 % and cavity or cavity door rupture due to pressure or thermal effects, 0.6 %. The early leak represents 6.4 %, divided between small containment bypass due to one SG tube rupture, 3.3 %, and cavity door leak after loss of sealing due to thermal effects, 3.1 % of CDF. LERF follows these failures (early rupture and part of early leak) with 15.5 % of CDF or $0.1x10^{-5}$ / year. Late containment rupture is very rare, but late containment leak is more frequent, 6.7 % with prevailing cavity door loss of seals late, basemat melt through by debris is only slightly above 1 %. There is a high probability, 71.6 %, of intact containment, but the very low activity release does not coincide with it, it is only 51 %. This is due to relatively high natural containment leak. Conservatively, no credit is given to retention factors on the release path and auxiliary building, thus this high natural gas leak leads to cesium release up to 1 % of inventory in case of intact containment and sprays failure. [24,25]

The results taking into account plant modification like plugging the reactor cavity drainage. Also, some SAMG interventions from the prepared guidelines were selected, which have high chance for success, like primary system depressurization or manual spray start. On the contrary, those that seem not to be efficient with current plant hardware, like influencing hydrogen risk, or those improbable like isolating containment bypass not isolated before core damage, have been omitted.

<u>Summary of Temelin site</u>

Level 1 - at power results

The Level 1 - internal events model has been updated during 2001-2002. The main final results shown below indicate that the updated total CDF from internal initiators decreased substantially compared to original 1996 PSA value.

- The point estimate core damage frequency, for the updated PSA for internal initiating events is 1.49E-5/year year.
- LOCAs contribute 4.5E-6/year (31%), primary to secondary leakage events 3.6E-6/year (24%) and transients 6.7E-6/year (45%).
- Within the loss of coolant accidents the dominant contributors are small and very small LOCAs which contribute 22.1% and 4.7% respectively. It should be noted that the 22.1% identified as the contribution from small LOCAs is made up of the sequences initiated by a small LOCA and sequences which are initiated by a very small LOCA but transfer to the small LOCA tree as the result of subsequent failures.
- In the primary to secondary leakage category, the dominant contributor (approximately 86% of the primary to secondary leakage sequences) is from sequences initiated by medium leakage, either from multiple tube failures or leakage through the SG header cover.
- The highest transient initiator, contributing 39% of the transient total is the Loss of offsite power. The next highest is transients with Loss of feedwater (31% of transient contribution) and the third contributor is the Main steam line break event (30%). The remaining transients contribute less than 1% between them to the transient initiated CDF.
- As far as the difference between the earlier PSA performed when the plant was still under construction and the current results crediting the information on the currently operating Unit, it can be seen that there is a significant reduction in the contribution to CDF from both primary to secondary leakage (a reduction of 6.24E-5) and from LOCAs (a reduction of 1.05E-5). There is a small reduction in the contribution to the core damage frequency from ATWS (a reduction of 2.68E-6). This result was expected, as there has been little change to the design of the main plant systems that provide the safety functions for the transients and LOCAs.

Level 1 - Low power and shutdown results

For the purpose of performing the safety assessment of shutdown phases of operation at Temelin, the six plant operating modes were further subdivided into plant operational states (POSs), which are characterized by a particular subset of plant activities and reactor states. New Plant Operational States are defined for each unique combination plant system operating configurations. Some examples are as follows: the RCS integrity (open/closed), the reactor vessel head (on/off), TQ-RHR configuration (normal configuration/mid-loop operation), the RCS water level (full/vessel flange/mid-loop/refueling,), decay heat load (early/late in outage). There were 23 unique POSes identified for Temelin NPP Shutdown risk analysis.

The CDF for low power and shutdown plant operating states is 9.3E-6/yr. This compares with for the at power internal initiating events core damage frequency of 1.49E-5 per year.

The dominant contributor is Loss of Offsite Power at 8.1E-6/yr. This initiator contributes around 87%. No other initiator contributes more than 5% to the CDF.

Plant operating states with the highest contribution to the annual CDF comes from the draining of the reactor vessel cavity and refueling passage (POS 13) at 4.1E-6/yr (44%). This is closely followed by mid-loop operation (POS 7) at 3.9E-6/yr (42%). The third highest contributor is the reactor vessel head removal (POS 9) at 8.7E-7/yr. No other POS contributes above 5% to the CDF.

Level 2 PSA Analysis

The most important mode resulting from the containment analysis is No Failure. This mode represents two events that could prevent containment failure: cooling debris in-vessel and cooling debris ex-vessel in long term. Thorough analysis of these phenomena showed that there is a good chance to prevent containment failure if sufficient amount of cooling water is available in long term. Frequency of No Failures is 3.7E-06 (24.2 % of CDF).

Late containment failure frequency is 6.8E-06 which is 45.4 % of CDF. This is almost ten times higher than Early Failure frequency, which conclusion is similar to western PWRs. Dominant mechanism of Late CMTM Failures is late basemat melt through.

Generally, Early Containment Failure frequency makes only 8.1E-07 (5.4 % of CDF) being dominated by the Loss of CMTM isolation (1.6 % of CDF).

The frequency of Large Early Releases (LERF) was found to be 4,0E-6/year. A comprehensive sensitivity analysis has been made to demonstrate the impact of Severe Accident Measures and plant specific SAMGs developed for Temelin.

Insights from the PSAs

A lot of safety improvements have been made in Dukovany NPP since 1991 with aim to decrease units risk level. PSA insights have helped significantly in this still ongoing systematic process, which helps in Dukovany NPP to achieve a comparable risk level of WWER unit with "western" design (CDF for FP operation decreased more than by factor of 15 within last years).

Relocation of emergency feedwater collector and feeding heads, and implementation of new EOPs, including all new human post accident interventions, previously identified by PSA, are the plant modifications with the most significant influence on unit risk level. Implementation of additional PORV to be used for F&B and cold overpressure protection, improvements of ECCS, I&C, electric power systems, new SAMG etc. represent some other important safety measures PSA insights have been used for in decision making process.

At Temelin NPP a comprehensive safety improvement program has been started before 1989 by the identification of potential design vulnerabilities list and it has been substantially extended following 1990 -1992 through various safety audits conducted either by nuclear safety consultant companies, by the IAEA, GRS, WENRA, etc. or in the frame of bilateral relationship.

As most of the important design changes has been decided to implement prior PSA development these design changes were not PSA based upon. The PSA was used in an „ex-post" manner to evaluate selected, already implemented or decided to be implement safety measures. This was the case of IAEA safety issues e.g.„S06 - ECCS water storage tank and suction line integrity" where a pipe-in pipe concept has been adopted and implemented for common suction line of ECCS from the containment sump. The PSA provided quantitative evidence that the CDF from suction line break scenarios were ranging in order 1E-8/year to 1E-9/year (prior suction line casing installation). Similar for „S08 - Power operated valves on the ECCS injection line" the PSA confirmed the design solution being adopted. Also some other design changes were justified by the PSA, like addition of two additional diesel generators into the design, common for both Units - which decreased LOSP contribution substantially to 3% of total CDF compared to around 20% in the 3 DGs standard Russian design.

Recently, the risk contribution of the new control valve introduced into the LHI/RHR pumps was evaluated.

The Level 2 analysis has been used at both sites for plant SAMG development and based upon the results of the Level 2 PSA the utility decided to implement SA measures to decrease the frequency of the containment early failure.

8.2.19 Canada

REGULATOR

The PRAs play an increasingly important role in CNSC activities, as the following examples indicate:

- Based on the Pickering A Risk Assessment (PARA) insights, the CNSC put a number of conditions on the restart of the four units at Pickering A. More specifically, the CNSC required that:

  - the Severe Core Damage Frequency (SCDF) be significantly reduced such that the OPG internal SCDF target to be met, and
  - the event sequences that do not meet the single failure criterion to be removed as much as possible.

- Using Bruce B Risk Assessment (BBRA) results, OPG requested the CNSC to drop an action item.
- OPG used the results of Darlington A Risk Assessment (DARA) to support a request for functional changes.
- Used BAPRA to assess the validity of the assumptions made in nuclear accidents and malfunctions section of the Environmental Assessment, prepared in support to the restart Bruce A Units 3 and 4.

The CNSC review of the PSA Level 1 as a design assist tool for the Advanced Candu Reactor (ACR), identified a series of model improvements, and potential improvements of the design.

INDUSTRY

The completed PSA for the multi-unit plants indicated that the dominant contributors to severe core damage risk are the initiators that can potentially affect multiple systems, particularly secondary side steam line breaks in the powerhouse and losses of service water. Improvements to powerhouse venting systems have been introduced to reduce the contribution to severe core damage frequency.

Offsite risks appear to be very low due to the large containment volume and redundancy in containment mitigating systems afforded by the shared containment structure. Consequential containment failure is found to be unlikely.

As mentioned in the previous sections, AECL developed a design-assist PSA for ACR-700 that provided the following insights:

Internal Events at Full Power

Thirty-five internal initiating events, which collectively represent events postulated to occur at full reactor power and could lead to significant consequences if not mitigated, were assessed in terms of their risk to core damage.

The assessment shows that:

- The summed mean SCDF is 3.4E-7 occurrences per year, which is well within the design target. There are no cross links that disable the plant heat sinks. The top seven dominant initiating events that contribute to SCDF are the total loss of service water, main steam line break in the reactor building, Heat Transport System (HTS) heat exchanger leaks within the pressurizing pump capacity, large Loss of Coolant Accident (LOCA), pressure tube and calandria tube rupture, total loss of instrument air; and feeder stagnation break.

- Design vulnerabilities were identified and resolved with the designers.

Internal Events at Shutdown State

Based on the ACR outage plan, there are three distinct states that the reactor will be in during a planned maintenance outage. Initiating events were analyzed for each state since the available heat sinks and mitigating strategies vary among the states. The three states are:

- Reactor in Guaranteed Shutdown State (GSS) with the HTS full and pressurized to 2 MPa and the reactor outlet header temperature at 60°C. This state is required for defuelling and refuelling operations (shutdown state M4A).
- Reactor in GSS with the HTS full and depressurized to atmospheric pressure and the reactor outlet header temperature at 54°C (shutdown state M4B).
- Reactor in GSS with the HTS drained to low level and open to containment and reactor outlet header temperature at 54°C. In this state, maintenance activities are undertaken, including steam generator and fuel channel inspections (shutdown state M6).

The assessment shows that the estimated mean SCDF is well below the target of 1.0E-6 occurrences per year. The result indicates that the ACR design has sufficient redundancy with respect to heat sinks while in a planned maintenance outage. ACR design improvements, particularly the division concept for the long-term cooling system and the passive make-up capability from the reserve water system directly to the heat transport system and moderator, contribute to this result.

The top six dominant initiating events that contribute to SCDF are the total loss of service water in M4A, heat transport leak in state M6, loss of long-term cooling in state M4A, total loss of service water in state M4B, long-term cooling leak in state M4A, and heat transport leak in state M4A.

Internal Flood

A limited assessment of the ACR-700 in response to several internal flood initiating events was conducted. The results showed that the contribution to core damage from these events was negligible.

Also, a Level 1 PSA-based seismic margin analysis (PB-SMA) was performed using the USNRC seismic margin approach methodology. All potential seismic failure modes and component weak links/functionality were considered. Non-seismic failures, human errors, and their conditional probabilities were also considered in the analysis. Estimates were made of seismic capacities using ACR seismic design criteria and qualification criteria, including recent PSA and SMA experiences for other advanced reactor designs. With these estimates and ACR seismic event trees and fault trees, a seismic margin measured in terms of HCLPF (High Confidence of Low Probability of Failure) was shown to meet 0.5 g peak ground acceleration for both severe core damage and limited core damage. This compares well with the design basis earthquake of 0.3 g.

8.2.20 Belgium

For all NPPs, results indicate that the risk during non-power states is considerable compared to the risk during power operation.

Plant specific modifications (both hardware and procedural changes) have been proposed and implemented in the framework of the periodic safety reviews of the NPPs or in the framework of major modifications to the installation.

Based on the results for mid-loop operation, all plants have now taken the decision to open the man-whole on the pressuriser to avoid pressurisation scenarios at midloop operation with the steam generator nozzle dams installed.

Some quantitative information on the results is given in the following tables.

NPP	Contribution to CDF from power states	Contribution to CDF from non power and shutdown states
Doel 1 and 2	61%	39%
Tihange 1	46%	54%
Doel 3	49%	51%
Tihange 2	To be re-evaluated due to modified operating practices in shutdown	To be re-evaluated due to modified operating practices in shutdown
Doel 4	64%	36%
Tihange 3	To be re-evaluated due to modified operating practices in shutdown	To be re-evaluated due to modified operating practices in shutdown

The initiating events with highest CDF contribution are:

NPP	for power states	for non power and shutdown states
Doel 1 & 2	Loss of CC-cooling (43%) SBLOCA (33%)	Loss of RHRS (79%)
Tihange 1	SBLOCA (23%) Loss of internal electrical power (18%) Loss of offsite power (16%)	Loss of RHRS (66%)
Doel 3	SBLOCA (20%) Loss of offsite power (17%) ATWS (12%) MBLOCA (12%) Induced LOCA (12%) SLB inducing SGTR (11%)	Loss of RHRS (62%)
Tihange 2	Partial or total loss of component cooling-service water system (29%) Loss of offsite power (23%) SBLOCA (14%)	To be re-evaluated due to modified operating practices

NPP	for power states	for non power and shutdown states
Doel 4	Loss of feedwater (15%) Loss of offsite power (15%) SBLOCA (15%)	Loss of RHRS (81%)
Tihange 3	SBLOCA (27%) MBLOCA (20%) SLB inducing SGTR (20%)	To be re-evaluated due to modified operating practices

For the level 2 PSA results (performed for Doel 1 and 2 and Tihange 1), the dominant failure modes of the containment are:

- Core-concrete interactions leading to basemat melt-through
- Slow overpressurisation after vessel failure
- Containment by-pass (basically originating directly from initiating events)

9 FUTURE DEVELOPMENTS AND RESEARCH

9.1 Summary

Nearly all the countries indicate that they intend to up-date their studies (living PSA). Another very general is to extend the scope of the existing PSA studies to level 2, external hazards or Shutdown Situations.

It appears clearly that the future “standard PSA” will be a living PSA including both level 1 and level 2, both full power and shutdown situations, and both internal and external initiating events.

Future PSA applications:

Several countries describe their activities aiming to improve Risk-informed regulation and Risk-informed decision making (USA, Canada, The Netherlands).

Other countries indicate more specific applications:

- Optimization of testing and maintenance (Hungary, Czech Republic, Taïwan),
- Precursor analysis (Germany, Czech Republic),
- Risk Monitors (Slovakia, Czech Republic).

In fact, many other PSA applications are carried out (not reported in this section).A more complete view on the different PSA applications is given by the tables in Appendix A of the countries answers.

Research activities:

An interesting point is that an important number of research activities are in progress, relating to many different PSA aspects. Some very classical topics are indicated by many replies, for example:

- HRA (USA, UK, Switzerland, Korea, Japan, Hungary, France, Czech Republic)
- Digital I&C (USA, Korea, Japan)
- Fire (USA, Mexico, Japan, Finland, Canada, Sweden)
- Earthquakes (Japan, Hungary)
- External Hazards (Mexico, Japan, Finland, Canada, Belgium)
- Level 2 PSA and severe accidents (UK; Slovakia, Korea, Japan, Hungary, France, Canada, Belgium, Sweden)
- Data and CCF (UK, Switzerland, Sweden, Japan, Hungary, Canada)
- Uncertainties (Korea, Canada)

Also, work is carried out in several other countries like Finland in all these areas. Moreover, it is likely that for these classical topics, some work is also carried out in the other countries, even if not explicitly indicated. From this list it appears that HRA, Fire and other external hazards, and Level 2 PSA are the main fields of research.

Other development topics appear in country replies less frequently. Some examples are as follows:

- Ageing (Italy, France, Czech Republic, Canada)
- Level 3 (Japan)
- Dynamic PSA (Switzerland)
- Reliability of passive systems (Japan, Italy)
- PSA for Non-Reactor Facilities (Italy) and more specifically PSA for Spent Fuel Pools (Slovakia, France)
- Advanced Methods (USA, Korea)

Furthermore, there seems to be research for a better presentation and communication of PSA contents and results carried out in USA, Korea and Spain.

In summary, it can be noted that although PSA methods and applications have made real progress during these last years. This amount of research activity indicates that PSA results are considered as sufficiently useful to justify this amount of work.

9.2 Country replies (in reverse alphabetical order)

9.2.1 USA

In order to support and integrate its ongoing efforts to risk-inform its regulatory processes, the NRC has created and is maintaining a Risk-Informed Regulation Implementation Plan (RIRIP). The RIRIP describes the NRC's strategy to risk-inform NRC regulatory activities in all arenas. The plan, which is updated semi-annually, provides background information on the NRC's approach to risk-informed regulation, as well as descriptions of ongoing implementation activities.

For example, one key implementation activity described in the RIRIP is a program to create a risk-informed environment. The objective of this program, started in 2001, is to create an environment in which risk-informed methods are integrated into staff activities, and staff plans and actions are naturally based on the principles of risk-informed regulation. The program has four phases: (1) evaluate the current environment, (2) design an improved risk-informed environment, (3) implement changes to achieve the target environment, and (4) assess the effectiveness of environmental changes. As this approach suggests, the basic strategy for the program is to first understand the current environment and then address the weaknesses and build on the strengths. To date, Phases 1 and 2 have been completed.

Another key activity described in the RIRIP is the development and implementation of a plan to develop a regulatory structure for new plant licensing. The objective of this activity is to provide an approach for the staff to enhance the effectiveness and efficiency of new plant licensing in the longer term. It is to be technology-neutral to accommodate different reactor technologies, risk-informed to identify the more likely safety issues and gauge their significance, and performance-based to provide flexibility, and will include defense-in-depth to address uncertainties.

The April, 2006 version of the RIRIP is provided as an attachment to SECY-06-0089. In general, information on the RIRIP (and on the NRC's use of risk in regulation) can be obtained from NRC's website:

http://www.nrc.gov/what-we-do/regulatory/rulemaking/risk-informed.html

Regarding future industry work relevant to the use and development of PSA, the Electric Power Research Institute (EPRI) is performing a broad spectrum of activities. These activities include the development of analytical methods, guidance; the support of PSA standards development; the support of risk-informed programs (e.g., fire protection, special treatment, and technical specifications); the support of industry efforts relevant to the development of a risk-informed licensing framework for new plants; the support of the development of PSA-related education and training and of a number of user groups; and the performance of a number of activities aimed at security- and emergency-planning related decision making. The EPRI portfolio of activities for 2007 can be found at the following website:

http://www.epri.com/portfolio/product.aspx?id=2180

The remainder of this section addresses some noteworthy examples of ongoing activities.

PSA Models

As discussed in Section 4.US, the NRC and industry are making a significant effort to develop PSA guidance documents (including consensus standards and regulatory guides) as well as supporting technical reports. This effort is in support of the NRC's phased approach to achieving appropriate quality for risk-informed regulatory decision making. It is expected that the effort will, among other things, result in improved and more complete PSA models. In particular, when the work is completed, it is expected that the industry will have full-scope (i.e., internal and external event) PSAs that are fully quantified (including a full uncertainty analysis) and are reviewed and approved by NRC.

One current example involves fire PSA. As discussed in Section 7.US, EPRI and NRC RES have jointly developed an improved fire PSA methodology that builds on lessons from the IPEEE program, and on the results of subsequent fire-risk related research efforts. Also, as discussed in Section 4.US, the American Nuclear Society has the lead in developing an industry consensus standard for fire PSA. Both the improved methodology and the standard are expected to be used by licensees developing updated fire PSA models in support of risk-informed fire protection programs as described under 10 CFR 48(c).

In addition to PSA-quality and standards related activities, work is being pursued on a number of topics identified from operational experience. Example activities involve the analysis of events involving the loss of the electrical grid and of the development of updated methods to assess seismic hazards (particularly those associated with higher frequency ground motions).

PSA Data

Both NRC and industry continue to collect and analyze data needed to support the development and quantification of PSA models. As discussed in Section 6.US, NRC is currently developing a revised set of generic distributions for SPAR model parameters based on recent U.S. operational data collected from a variety of sources, including the Institute for Nuclear Power Operations' (INPO) Equipment Performance Information Exchange (EPIX) system, the NRC's Initiating Events Database, and the NRC's Reactor Oversight Program.

A number of new data development activities currently underway involve HRA and fire PSA. Regarding HRA, NRC has initiated the Human Event Repository and Analysis (HERA) project, which will develop a database for HRA-relevant information from a variety of sources, including nuclear power plant operational events and nuclear power plant simulator experiments. The HERA project is summarized in NUREG/CR-6903. NRC is also supporting the OECD Halden Reactor Project's efforts to develop simulator-based information supportive of HRA modeling and quantification. Regarding fire PSA, NRC has initiated the Cable Response to Open Live Fire (CAROLFIRE) project, which will develop experimental data regarding the thermal response and functional failure of electrical cables exposed to fires.

Modeling of Physical Processes

NRC has recently initiated a major study aimed at updating the current state of knowledge (e.g., as represented by NUREG-1150) regarding the potential consequences of a U.S. reactor accident. This study will perform a realistic evaluation of severe accident progression, radiological releases and offsite consequences, focusing on a spectrum of risk significant scenarios (i.e., truncation of low probability scenarios). The study will use current, detailed integral modeling of plant systems, radionuclide transport and deposition, and release pathways. The principal phenomenological codes will be MELCOR and MACCS. The study will use updated, site-specific emergency preparedness modeling assumptions, and will use state-of-the-art HRA methods to support the assessment of the effectiveness of various mitigation strategies for the delay or prevention of core damage (which will further reduce potential offsite consequences).

NRC is also undertaking a study of success criteria used in its SPAR models. The principal phenomenological code used in this assessment is TRACE, a best-estimate thermal-hydraulic code being developed by NRC. TRACE is based on the older RELAP and TRAC codes, but incorporates improved models within a modern software architecture.

PSA Methods

Human Reliability Analysis (HRA)

Over the last several years, NRC's work in the area of HRA methods development has focused on the development and testing of A Technique for Human Event Analysis (ATHEANA). ATHEANA is an HRA method aimed at addressing the issue of scenario-specific context and a particularly challenging topic in HRA: the treatment of errors of commission. ATHEANA's underlying premise is that significant human errors occur as a result of a combination of influences associated with plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel. This premise requires the identification of these combinations of influences, called the "error-forcing contexts," and the assessment of their influence. ATHEANA has been used in the PTS PSA studies (see Section 7.US) and is expected to be used in the upcoming assessment of reactor accident consequences (see Section 9.US.3 above). Additional application areas (including HRA for fire PSA) and extensions to treat time as a dependent variable of the analysis are under consideration.

Regarding the HRA calculator mentioned in Section 6.US, EPRI is continuing to perform work to enhance the calculator and to provide training and user support.

Fire PSA

As discussed in Section 9.US.1 above, EPRI and NRC RES have jointly developed an improved fire PSA methodology. One of the major improvements in the methodology, which is documented in NUREG/CR-6850 / EPRI 1011989, involves the treatment of fire-induced circuit failures. The improved approach is expected to lead to improved treatments of fire-induced spurious actuations and, therefore, improved assessments of fire risk. One area not addressed by NUREG/CR-6850 / EPRI 1011989 is the performance of a detailed HRA for fire events. It is recognized that additional work is needed in this area to develop a sound technical basis for acceptable approaches before guidance can be written.

Digital Instrumentation and Control Systems

It is well-recognized that U.S. licensees are currently replacing their original analog control, instrumentation, and protection systems with digital systems, and that there are no widely accepted methods for including software failures of real-time digital systems into current generation PSAs. NRC has initiated a project aimed at developing methods of modeling digital systems that can be integrated into current PSAs.

This project has three parts. The first part is based on traditional approaches (e.g., fault tree and Markov methods). The second part will use dynamic reliability methods such as Dynamic Flowgraph Methodology to model digital systems. Both the traditional and dynamic methods will be exercised using case studies based on a digital feedwater control system and a reactor protection system. The third part will involve the development of regulatory guidance aimed at supporting risk-informed reviews of digital systems.

Advanced PSA Methods

Recognizing the complexity of current PSA models, EPRI is investigating a number of methods that may be useful in the review and verification of these models. The particular methods for which proof-of-principle studies are being done are Binary Decision Diagrams (BDDs) for model quantification and declarative modeling for simplified model construction and enhanced model review.

Treatment of Uncertainty

As part of its phased approach to PSA quality, the NRC is developing guidance for the treatment of uncertainties and the use of alternate methods in the risk-informed decision making. The guidance will address the integrated risk-informed decision making process and different approaches appropriate for the treatment of different types of uncertainty (e.g., parameter, model, and completeness uncertainties). Both traditional PSA techniques (e.g., regarding the propagation of uncertainties) and supplemental techniques (e.g., sensitivity studies, qualitative analyses, bounding analyses, screening methods) will be addressed. EPRI has developed guidelines for the treatment of uncertainty in risk-informed applications, which includes guidance on the identification os key uncertainties, i.e., those that can have an influence on a decision. Related work identified in EPRI's 2007 plan involves research "relative to risk acceptance criteria and their role combined with defense-in-depth to account for uncertainty."

Research and Development Planning

As part of its continuing efforts to address current limitations in PSA methods, tools, and data, NRC has started to develop a formal plan for future PSA research and development (R&D) topic areas. The intended uses of this plan are to (a) support high-level, resource allocation decisions and (b) provide a starting point for the planning of detailed activities addressing the topic areas identified by the plan. It is expected that the resources required to develop and maintain a formal plan will be balanced by a number of benefits. These benefits include the increased assurance that future PSA R&D topic areas are tightly coupled to the regulatory needs of the agency, and the availability of documentation enabling internal and external stakeholders to determine where and why NRC is focusing its PSA R&D resources. The documentation will also facilitate updates to the RIRIPas the agency's knowledge base and needs change.

PSA Results Communication

The communication of risk results (including uncertainties) to decision makers and other stakeholders remains a challenge. The staff has developed a set of guidelines (NUREG/BR-0308) focusing on risk communication to external stakeholders and a companion set of guidelines (NUREG/BR-0318) for risk communication within the agency.

9.2.2 United Kingdom

In the UK, a Health and Safety Commission Co-ordinated Programme of Nuclear Safety Research has addressed generic nuclear safety issues identified by NII. Over many years, research in various areas connected with PSA has been carried out by both licensees and the NII. In recent years the issues researched have tended to range wider than the technique of probabilistic safety analysis and look at wider aspects of risk analysis. Risk criteria and the arrangements in place for assessing compliance with risk criteria have been included. (See table below for research conducted.) The research has addressed issues which have arisen as a result of safety case submissions, state-of-the-art practices in risk assessment and its applications, and operational matters. There have been elements of information gathering and data acquisition and also methodological developments.

Validation of PSA	Fault tree analysis consistency
	PSA data validation
	Accident sequence precursor analysis
PSA Methods	Comparison of PSA techniques
	Sensitivity studies
	Worker risk
	Capability of methods for specified applications
	Common cause failure across systems
	Significance to the risk of non-compliance with site procedure
	Reliability of repair
	Review of international standards for PSA
PSA Applications	Reliability/ conditioned centred maintenance
	Extension of the scope of PSA to include all hazards
	Feasibility of Event Based Seismic Risk Criteria
	Comparison of deterministic and probabilistic based Operating Rules
	ALARP - non-risk based factors
	Time at risk - acceptance criteria
	New approaches to decision making in conditions of uncertainty
	Seismic PSA - application to gas cooled reactors
	Fire PSA
	Review of risk management arrangements
	ALARP decisions database development and maintenance
Derivation of Data for PSA	Zero failure data
	Effects of ageing
	Data for standby systems
	Methods of combining generic and specific data
	Relationship between testing and reliability data
	Loss of grid frequency
	Update of accident costs
Human Action Representation	Quantification of human actions over long timescales
	Representation of human error within PSA

Although there is now a diminished need for further research in basic PSA techniques, there is an increased interest in improving the existing PSAs so that they better support safety decisions at nuclear installations. Therefore, new research activities are focused to support future PSA scope enhancements, improved PSA realism and wider PSA application.

The analysis methodologies and codes used for PSA are generally well understood and accepted worldwide. However, although a large number of issues have been addressed in recent years, there is a need to continue improving PSA methods with the aim of having better and more complete PSAs that can more effectively support safety related decisions at the nuclear installations.

Both the UK regulators and licensees are involved in international activities on PSA sponsored by the IAEA, EU, OECD/NEA, etc. In particular, the OECD/NEA Committee on the Safety of Nuclear

Installations has a Working Group, WGRISK, which provides information directly relevant to this section of the NRI. IAEA work on PSA and PSA applications is also relevant.

PSA related research currently underway in the UK, and in collaboration with others, is described in detail below:

International common cause failure data exchange project (ICDE): The ICDE is an international collaborative exercise aimed at gathering and sharing data on common cause failures. Participants include USA, Canada, France, Switzerland, Germany, Finland and Sweden. The UK was invited to participate, through NII, and participation in the pilot scheme was endorsed by a technical review meeting on CCF.

During 1998/99 processes for the export and import of data were set up and data for a limited number of sample systems were extracted from existing databases and exported and sent to ICDE.

During 1999/00 the initial export of data for sample systems began and import of data for diesel generators was undertaken. Useful information has been gained on the causes of CCF.

By the end of 2000, the ICDE had produced reports analysing data on centrifugal pumps, diesel generators and motor-operated valves.

During 2002/04, saw data collection on reactor protection and shutdown systems, on switchgear and circuit breakers, and on batteries. Also a project which compared the data quantitatively with CCF probability factors used in UK reactor PSAs for diesels.
In 2005/06 data collection on control rods, pumps, valves and level monitors is ongoing. The UK is represented in this work by Magnox Generation and the NII.

Assessment and Calibration of the Unified Partial Beta factor Method used to evaluate Common Cause Failure probabilities for the PSA: In the UK common cause failure probabilities (CCF) for PSA are calculated using a method based on the beta factor approach. In this model the probability of the common failure of two or more redundant components or system trains is calculated by multiplying, respectively, failure probabilities of individual components by relevant beta factors. The beta factors are assessed using the Unified Partial Beta Factor Method (UPM). This is generally accepted as a valid and useful approach. The UPM is based on structured expert judgment for a broad and complete range of important influence and conditioning factors regarding CCF events. Bearing in mind the significance from the risk point of view of the common cause failures, and the important role that risk assessment plays in the Stations' Safety Cases and more and more in the Stations' operational decision making processes, it is essential to have confidence in the predictions of the CCF method used. In this regard, current research is aimed at determining how results obtained using the UPM method compare against other widely used data-based CCF approaches, and in understanding how the UPM predictions compare against specific information obtained from the Stations' operating experience. With increased maturity in the Industry's understanding of the common cause failure issues, it is an appropriate time to assess the predictions of UPM.

To address the above, current efforts are focused on using ICDE data to support CCF probability quantification and to compare the results against the results obtained using UPM.

Level 2 PSA for Gas Cooled Reactors - Methodology and Procedure: The risk associated with a potential severe accident depends on two factors; the amount of damaged fuel/the release of fission products in the reactor building, and the opening of direct or indirect pathways for the release of radionuclides to the environment. An important aspect of the risk reduction process is accident management. State-of-the-art practices for conducting Level 2 PSA include a quantitative assessment of plant response to accident sequences that would result in extensive damage to the reactor core and release of a large fraction of the core's inventory of radionuclides. The current PSAs for Gas Cooled Reactors calculate the frequencies of various radiological dose bands. However, these PSAs have not been extended to analyse the fraction of the frequency within DB5 (> 1000 mSv) that is represented by fault sequences that would produce an offsite release of sufficient magnitude to cause significant short-term effects on human health.

The current research involves an assessment of fault sequences involving extensive damage to the core to provide information essential to the process of identifying and implementing appropriate severe accidents management measures and to facilitate a demonstration that the risk is reduced so far as is reasonably practicable. The expected outcome of the research work is the identification of all information, data and analysis work necessary to perform a more detailed Level 2 PSA for the AGRs, the identification of work done so far and the information already existent that is relevant and can be used to develop Level 2 PSAs for the AGRs, the preparation of a procedure to perform Level 2 PSA for AGRs, and preparation the evaluation of this procedure in a trial application. This research is ongoing and is lead by British Energy.

Evaluation of procedure and assessment of potential outputs: Following the development of a procedure for Level 2 PSA for AGRs (see above) there will be a need to evaluate this procedure before fully applying it to all AGRs. The following research activities aim at ensuring that a viable and practicable procedure is obtained:

- Evaluation of the Level 2 PSA procedure developed by applying it to a selection of dominant sequences chosen from the PSA for one of the AGRs
- Compilation of lessons learned both from the methodological point of view as well as insights regarding the potential to identify risk reduction measures for AGRs.
- Introduction of enhancements in the proposed Level 2 PSA procedure
- Establishment of a programme to develop Level 2 PSAs for the operating Gas Cooled Reactors

This research to be lead by British Energy.

Nuclear Action Reliability Assessment (NARA): In the UK, as elsewhere, probabilistic safety assessments (PSAs) are carried out to assure the safety of nuclear power plants. For the past decade, the principal tool used in the UK to quantify the reliabilities of human interactions has been the Human Error Assessment and Reduction Technique (HEART). Whilst this technique has served well, it was developed many years ago. In the intervening time, although it has had some minor modifications, it has remained principally the same technique, based on the same original data. Meanwhile since 1992, a human error probability (HEP) database called CORE-DATA (Computerised Operator Reliability and Error Database) has been under development. Additionally, an internal industry review of the application of HEART in actual PSAs, revealed some shortcomings of the technique, in particular that HEART did not always ‘fit’ very well with the nuclear power plant tasks being assessed. It was therefore felt, by users of the technique that a new tool could be developed. It was considered that this tool should be established along the same lines as HEART, but based on more recent and relevant data, whilst being more tailored to the needs of UK nuclear power plant PSAs and HRAs. This lead to a project called NARA (Nuclear Action Reliability Assessment) to develop a nuclear power plant specific HRA approach. The NARA development project is now nearing completion. Within the last year it has been the subject of a NII sponsored peer review which raised various issues for further consideration. These issues have now been addressed. Currently workshops are being set up to disseminate the NARA methodology to potential users.

9.2.3 Taiwan

The ongoing project of operating NPPs is the update of the living PSA models of the three operating NPPs in response to the comments of peer review. The project will be completed in 2007 with plant specific operating data updated to 2006. The TIRM-2 and PRiSE will also be revised to incorporate the updated PSA.

The development of Lungman PSA is another ongoing project which is scheduled to be completed at the end of 2007, near the startup test of this new ABWR.

The pilot study of RI-ISI plan had been conducted on the RHR system of the Kuosheng NPP. An integrated full scope analysis for all safety significant systems of Kuosheng will start at 2008. The project is aimed at producing a revised RI-ISI and RI-IST program plan to be submitted to TAEC in the process of periodic review of the plant license for the next 10 years.

In the development of Maintenance Rule implementation plan, PSA is used to categorize those in-scope SSCs according to their safety significances. The maintenance effectiveness of these SSCs will be monitored against appropriate performance criteria. For high safety significant SSCs, they will be monitored at the train level through routine trending on their reliabilities and availabilities. For low safety significant standby SSCs, their reliabilities will be monitored. The other in-scope SSCs will be monitored against plant-level criteria that are characterized by some operation-associated performance indexes. PRA will also be used to evaluate the maintenance configuration risk during online maintenance. The three operating NPPs will implement the Maintenance Rule at the beginning of 2007.

9.2.4 Switzerland

In order to increase the range of application of the PSA, HSK focuses on the harmonization of the PSAs in order to make the PSA more comparable. This is the main focus of the development of the PSA in the next years. Furthermore, the level 2 PSA shall be extended to low-power and shutdown operations in the next years. Level-2 results for various plant operational modes can be compared more easily than level 1 PSA results.

Switzerland supports research and development in the following fields:

- *Data Collection*: HSK is an active member of various international programmes for data collection such as ICDE (International Common Cause Data Exchange) the OECD-FIRE (OECD Fire Incident Records Exchange) and the OPDE (OECD Piping failure Data Exchange).
- *Severe Accidents*: HSK supports a research project conducted at the Royal Institute of Technology (KTH) on severe accident phenomena and severe accident risk in a LWR. The focus of this project is on Melt-Structure-Water Interactions (MSWI) that may occur during a late phase of in-vessel core melt progression and ex-vessel phenomena. The main intention for this research is to create a basis to assess ex-vessel debris coolability and steam explosion energetics, as chief threats to containment integrity in a BWR plant, which employs ex-vessel cavity flooding in severe accident management.

  In addition HSK supports the international OECD project on Melt Coolability and Concrete Interaction (MCCI). This project provides experimental data on the coolability of molten debris that has spread into the reactor cavity and on two-dimensional, long-term interaction of the molten mass with the concrete structure of the containment.
- *ADAM System*: A much faster than real-time accident diagnostics and prognostics system has been developed by Energy Research, Inc. (ERI) for HSK and has been implemented at the HSK emergency response centre for all Swiss nuclear power plants. Aside from applications to accident diagnostics and prognosis, ADAM is also used for training and as a tool for severe accident analysis and application to PSA level 1/2 studies (e.g., review of success criteria, containment loads, accident source terms, etc.). ADAM uses a highly versatile graphical user interface, and allows to efficiently analyze potential scenarios of interest.
- Human Reliability Analysis (HRA): HSK funds a research project on HRA methodology at the Paul Scherrer Institute (PSI). The work focuses on the further development of a method for quantifying decision-related errors, in particular for errors of commission. The method is based on ranking the error opportunities in terms of a set of situational factors that have been

identified in analyses of operational events that included EOCs. Following up on applications of this method at PSI, the method is being revised and user guidance is being prepared in order to carry out external applications and review. In previous work, PSI developed the CESA method for EOC identification and performed a pilot application; CESA will now be used to identify potential EOC opportunities in a second application study. The objectives of this work are, first, to continue to obtain insights on plant-specific risks associated with EOCs, and, second, to enhance the CESA identification process with further analysis aids.

- Dynamic PSA: A second area of work in PSI's HRA research project addresses the development and application of dynamic scenario analysis tools to support HRA. The purpose of such tools is to provide capabilities to simulate the nuclear power plant's physical response as well as operator actions in an integrated simulation. The past analyses performed for EOC identification at PSI show that a simulation tool to address the interactions of the plant evolution and operator responses in accident scenario could be very helpful. It would extend the analysts' ability to consider a broader range of scenarios, potential actions and errors, in conjunction with the factors and cues that may increase the likelihood of errors or conversely support error correction and recovery. PSI is cooperating with the University of Maryland to develop a tool based on the ADS (Accident Dynamic Simulator) framework and software. The current work at PSI addresses scenarios for a Swiss nuclear power plant.

9.2.5 Sweden

Issues addressed here are the description of the Swedish PSA work being carried out to increase the scope or otherwise improve the PSA:s that have been carried out, or to provide better support for them.

This section addresses:

- The domestic PSA:s are nowadays fulfilling the requirements in the regulation SKIFS 2004:1. All plant modes are analyzed and also the event area analysis and external events analysis are performed or will soon bee completed as part of all operational modes. The studies are performed for level-1 and level-2.
- The studies are very detailed and large.
- The data collection regarding the initiating event frequencies, component failure probabilities, common cause failure probabilities, human error probabilities, are natural parts of the overall PSA work.

Development and research matters regarding the development of domestic PSA:s are mainly initiated via the Nordic PSA Group.

PSA research

In Sweden and Finland the Nordic licensees have established a special working group, called Nordic PSA group (NPSAG), in which PSA related researching is discussed, initiated, followed-up.

The regulatory body SKI in Sweden and STUK in Finland are also members of that NPSAG Group, as adjourning members.

Matters that concern general reactor safety issues and touch PSA questions are items on the agenda for the NPSAG.

The topics that are on the NPSAG agenda covers all the tradional PSA areas, that must be of good quality in a PSA documentation or –model in level-1, level 2 and in area event analyse for all operational modes.

Sweden also participates in the OECD/ICDE, OECD/FIRE and in the OECD/OPDE projects.

This section provides a structured input of the actual research and development in the area of methods and procedures for risk assessment and application, which includes development of PSA level 1 and 2 and the use of these at the nuclear power plants.

Although PSA:s of level 1 and 2 are produced regularly, and the results are used in certain applications, there is still a need for improvements in order to achieve a broader acceptance and use.

Topics that are actual and suggested to be discussed at present in the NPSAG, are:

- Sequence modelling, including deterministic basis
    - Development of estimation methods for reactivity
    - End states in PSA:s
- Area events / external events
    - Fire frequency estimation
    - External events analyses
    - Plant impact at loss of room cooling/-heating
    - Information from the OECD/FIRE project
- CCF and dependencies
    - OECD/ICDE project
    - CCF data on Control Rod Drive Assembly
    - CCF - European Working Group on CCF
    - Education package about CCF:s and dependencies
- Data for PSA, including internal IE
- Development of a database, for estimation of pipe failure frequencies (R-Book)
- Level 2 PSA
    - SARNET - Severe Accident Research Network
- Issues related to PSA quality and interpretation of PSA results SARNET - Severe Accident Research Network
    - Common method description for PSA
    - Validity of safety goals

- Shutdown PSA
- Level 2 PSA
- PSA applications
- HRA
- xx
- QA

- PSA applications, risk informed applications regarding
  - Development of Technical Specification demand, by risk informed technique
  - NPSAG/NKS - Risk-based assessment of technical specifications
  - SAFIR / Risk-informed piping and equipment testing (RI-ISI)
- QA

Internally at SKI, there will be a certain research and development concentration during 2007-2008, on better understanding of the aspects related to the levels of defence-in-depth (DiD) principles from both a deterministic and a probabilistic point of view. Also, how to be able to better treat these aspects and new findings with the traditional PSA technique today. One problem today is that the PSA results do not clearly enough give risk measures and values strictly about failures and degradations challenging the different levels of the DiD, as they are defined in the SKIFS 2004:1regulation and in INSAG-10.

There is a need to restructure and complement existing PSA:s on such a way that comparisons of the levels of the DiD and the deterministic interpretations are enabled. Such a comparison makes it also necessary to extend the present even-tree and fault-tree models, with new information and trees.

This research project is also presented at the IAEA TM ”Effective Combination of Deterministic Analysis and PSA in Plant Safety Management” in Barcelona the 4-8 September 2006.

9.2.6 Spain

In order to conclude the Edition 2 of the Integrated Program, a final part is included describing "Future Forecasts" on the use of PSA and the promotion of the technological progress that the same ones entail.

The first and main point of this IP part introduces the concept of "Living PSA" and the activities of permanent updating and constant applications that can be visualized in the future to fit and use the PSA systematically. As can be seen in the status of plant specific PSA, Spanish plants are already more or less following this concept, keeping resources to maintain and update their PSA and to use them continuously to help decisions about safety and operation planning and analysis. In five plants (Cofrentes, Garoña, Ascó, Vandellós -2 and Almaraz), risk monitors are already available and integrated in daily operations.

CSN involvement in this process and activities to implement the models of the seven Spanish PSA in the CSN computers, for their use in CSN internal PSA applications and for the CSN review of applications proposed by the utilities, will be completed at the end of this year. This web-based PSA information is being used by the CSN inspectors.

To provide regulatory coverage for the process of performing and evaluating PSA applications the CSN is developing an Instruction regarding PSA consistent with the current Regulatory Framework. The Instruction will collaborate to establish the basis for what will be the new regulatory system in the future.

The Instruction will include aspects related to PSA availability and PSA applications requirements, safety guides, exemptions, penalties, etc.

Finally, the last point of the IP is related to continue fomenting the technological development that the assimilation of the PSA technology has meant in the country and the extension of the use of these techniques to other fields where risk is induced by ionizing radiations.

9.2.7 Slovenia

PSA model is a useful tool especially when it represents the plant as accurately as possible. That is why the PSA model is a developing tool dependent upon plant specific changes and also the methodology development.

At the Krško NPP

New updates of the Krško NPP PSA model are expected due to:

- the new Human Reliability Analysis (HRA), which would consider new methodologies and also human-error data refreshment;
- inclusion of new seismic study results after the implementation of the related modifications;
- (possible) new PSA study for External Flooding events;
- data update;

No progress regarding the impact of ageing in the PSA model has been done yet. Its inclusion is possible in the future.

At the SNSA

The regulation that would explicitly address PSA is still under preparation (the first draft has been prepared). It will involve the WENRA requirements and selected parts from US NRC Regulatory Guides.

The SNSA is constructing an internal information system (IS VVA) based on the PSA models, which will be used in the risk-informed decision making process (modification assessment, plant operation safety, …), in inspection planning, in regulatory activities planning, in importance indication of inspection findings,…

The SNSA has also developed a set of Safety Indicators which includes several Risk Indicators. Risk Indicators are safety indicators which are calculated with the help of the PSA model (e.g. Plant risk due to unplanned unavailability of NEK-STS equipment). Risk Indicators will keep developing on the basis of experience.

9.2.8 Slovak Republic

The plants have well established living PSA programs which are being continued and the PSA studies are being periodically updated.

In the near future the level 2 PSA study will be updated for the V2 NPP and a level 2 PSA project will be started for the Mochovce NPP. Both plants will have updated the risk monitors.

Detailed PSA will be performed for the units of V1 NPP after termination of their operation. The risk assessment will be concentrated on the spent fuel pools where the spent fuels will be storage.

9.2.9 Netherlands

As described in chapter 2 the development taking place is in the field of a transition towards Risk Informed Regulation. There a no research programmes foreseen for the near future other than those meant for improvements of the current PSAs. As described in the last paragraph of chapter 4, the

Borssele PSA is being updated with a new HRA methodology, a new fire PSA (NUREG/CR-6850) and increased mission times (72 hours).

9.2.10 Mexico

Recently the CNSNS has initiated a program to expand the use of risk-information into the regulatory framework. The efforts are addressed to emphasize the need to extend the present scope of the Laguna Verde Nuclear Power Plant IPE to cover accidents initiated by fire, external events and the low power and shutdown operating modes.

Based on the CNSNS experience during the review process of the IPE, it became clear the usefulness of developing in advance a set of guidelines to establish the level of detail and technical quality for those initiating events and operational modes did not take into account on the IPE scope. The development of such guidelines allows for the developers and reviewers, to agree in advance on the main objectives of the intended applications, and therefore provides an efficient way for the reviewing and approval process. Previously the utility has devoted some unfinished efforts for the development of a LVNPP Fire-PSA, according the regulatory authority produced a set of guidelines for the reviewing process. The objective of the review process is to assure that the fire related plant vulnerabilities are identified and corrective measures are proposed and implemented. The guidelines were developed bearing in mind the public available state-of-the-art Fire-PSA methodologies and were updated at the light of the NUREG/CR-6850 recently release.

Currently the CNSNS is involved in the development of a PSA level 1, (internal events) for low power and shutdown conditions with the objective to identify dominant risk contributors in such conditions.

As a result of the CNSNS partake on the Safety Margin Action Plan (SMAP) managed by the OECD/NEA, efforts will be addressed to better the level of detail of the existing PSA Models in order to analyze and assess the impact of plant modifications on plant safety margins.

9.2.11 Korea

Development of PSA Modelling Methodology and Related S/W

PSAs are widely used in many areas, so we need a lot of analysts. But, performing the PSA need several skilled experts for following purposes:

The amount of models and information is too large. It is difficult to trace a PSA

The different method is used for each scope of PSA. For example, the internal and the fire PSA use the different kind of information and method.

Only part of the PSA quantification is automated. We need a lot of manual work to quantify a PSA.

It is not easy to reproduce the result of a PSA even if a whole model and data is given. To make the PSA actively used, it is necessary to support non-specialists in PSA to perform the quantification or the sensitivity analysis of a PSA.

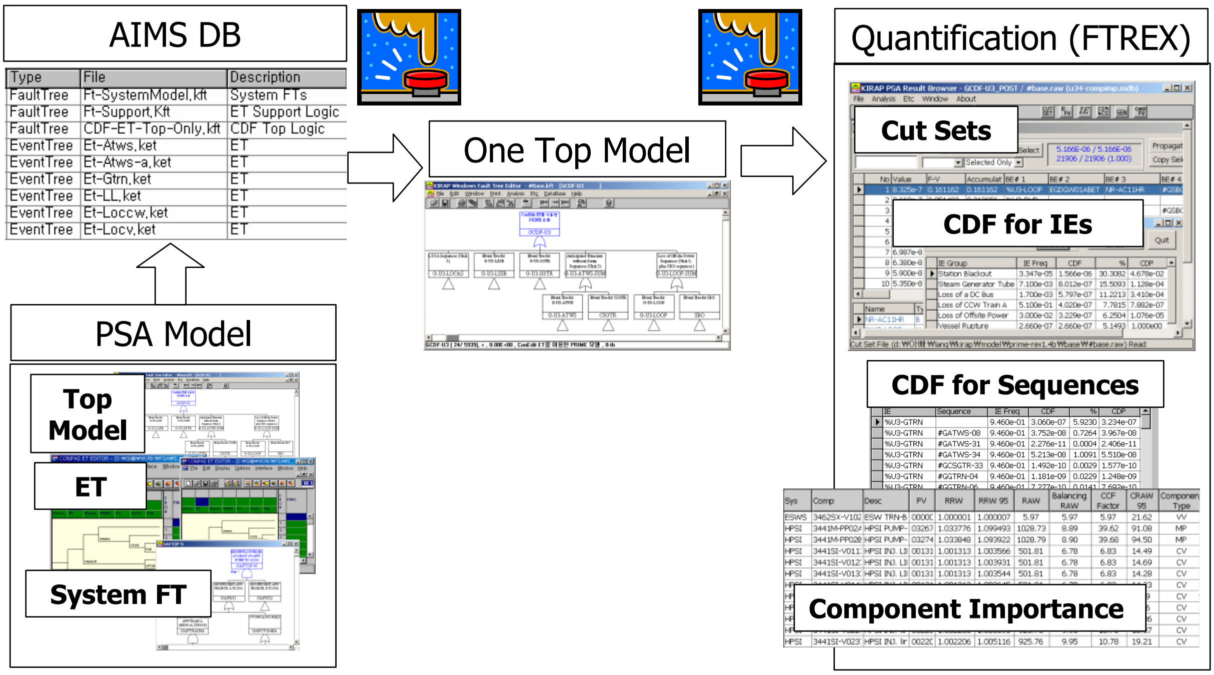
KAERI is developing the software called AIMS-PSA (Advanced Information Management System for PSA). The target of AIMS-PSA is:

- integration of full scope PSA
- easy and fast quantification
- traceability and
- reproducibility.

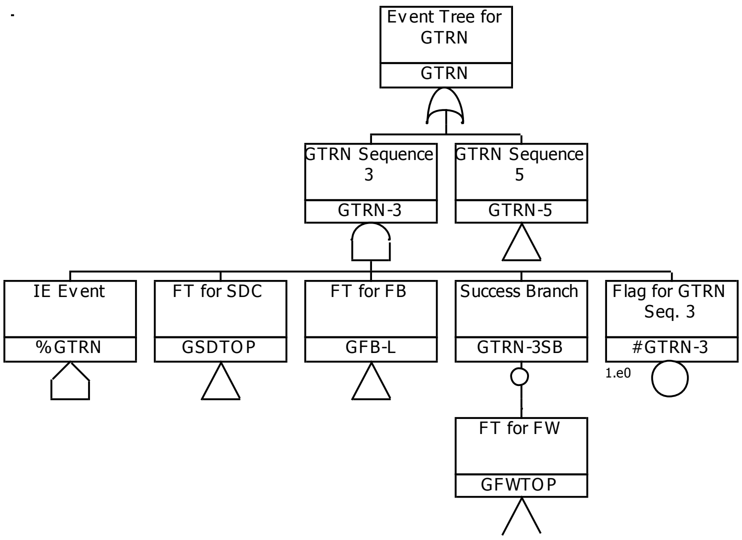
The detailed features of AIMS-PSA are given below.

Integration of Event Trees and Fault Trees

The following figure illustrates how we manage the PSA model using AIMS-PSA. Event trees and fault trees are stored in the AIMS DB.



In AIMS-PSA, the logic of each sequence of an event tree is converted into a fault tree. The fault tree for a sequence consists of an initiating event, failure branches, success branches, and a dummy event to represent a sequence number.



AIMS-PSA generates the one top fault tree model for the core damage frequency (CDF) from the event trees and the fault trees.

The one top model can be used for both a traditional PSA and a risk monitor. The cut sets generated from the one top fault tree contains the sequence information. The idea to use a dummy event representing a sequence number has been used to review the sequence information of the cut sets generated from a risk monitor in USA. The difference is that AIMS-PSA can delete the duplicated nonsense cut set between sequences with the help of the cut set generator, so that we have proper cut sets for each sequence from the one top model.

From the generated minimal cut sets for the one top model, we can get the total CDF, CDF for each initiating event, and CDF for each sequence. We don't need to repeat the calculation of minimal cut sets for every sequence. Only one time calculation of minimal cut sets is enough to do the quantification of a PSA. It takes about 10 seconds to generate minimal cut sets for the PRIME Level-1 PSA model for the UCN 3&4 units. The model has about 2800 gate events and 2500 basic events, and has also a lot of circular logics.

Integration of Level-1 & 2 PSA

The Level-1 PSA model is extended to include the containment performance model for the Level-2 PSA. The end state of each event tree is not the core damage but the plant damage state. The interface between Level-1 PSA and Level-2 PSA is the plant damage states (PDS). Level-2 PSA software (CONPAS) produces a table which has the large early release frequency (LERF) information for each plant damage state. Then, AIMS-PSA combines the event trees for PDS and system fault trees with the LERF/PDS information, and generates the one top model for the LERF.

If we add another table for the large late release frequency (LLRF) for each PDS, we can also generate the one top model for the LLRF. Once the cut sets are generated for the one top LERF model, the total LERF and LERF for each event sequence are calculated. The information is transferred to the Level-2 PSA software.

Integration of Internal & External PSA

Quantification for a typical fire event consists of 1) modifying the fault tree affected by the fire event, 2) calculating the conditional core damage probability (CCDP), 3) calculating the fire propagation and suppression factors, and 4) calculating the CDF for the fire event.

Because the analysis is not automated, the quantification for fire zones requires a huge amount of manual works. We are planning to develop a software to perform the quantification for fire PSA if we provide a information such as the components affected and propagation factors for each fire event.

Exact Value of a Fault Tree

The calculation of the exact probability of a fault tree has been of great concern in the PSAs. The BDD method gives the exact top event probability of a fault tree if it can solve the fault tree. At this moment, it is not likely to solve the large fault tree models for PSAs using the BDD algorithm.

FTREX is based on the coherent BDD algorithm. It can not give the exact value for the minimal cut sets directly because it has the different structure with the BDD method. We developed a method called the coherent BDD upper bound (CBUB). The following table shows the effectiveness of the CBUB method. It gives the very close value to the exact top event value.

Fault Tree	Truncation limit	# of Cut Sets	Top Event Probability		
			Rare Event Approximation	CBUB	Exact value
FT5	1.0E-08	713	5.134E-05	1.742E-05	1.692E-05
	1.0E-09	3,638	5.982E-05	2.236E-05	
	1.0E-10	23,605	6.549E-05	2.599E-05	
	1.0E-11	139,204	6.874E-05	2.735E-05	
	1.0E-12	794,260	7.061E-05	2.829E-05	
FT8	1.0E-07	35	4.450E-05	3.525E-05	3.517E-05
	1.0E-08	230	4.998E-05	3.694E-05	
	1.0E-09	1,806	5.432E-05	3.778E-05	
	1.0E-10	11,299	5.692E-05	3.830E-05	
	1.0E-11	70,316	5.856E-05	3.855E-05	
FT9	1.0E-06	89	8.790E-04	4.108E-04	4.053E-04
	1.0E-07	509	1.017E-03	4.680E-04	4.565E-04
	1.0E-08	2,135	1.062E-03	4.855E-04	
	1.0E-09	8,850	1.082E-03	4.952E-04	
	1.0E-10	33,546	1.090E-03	4.991E-04	

Introduction of the Condition Gate

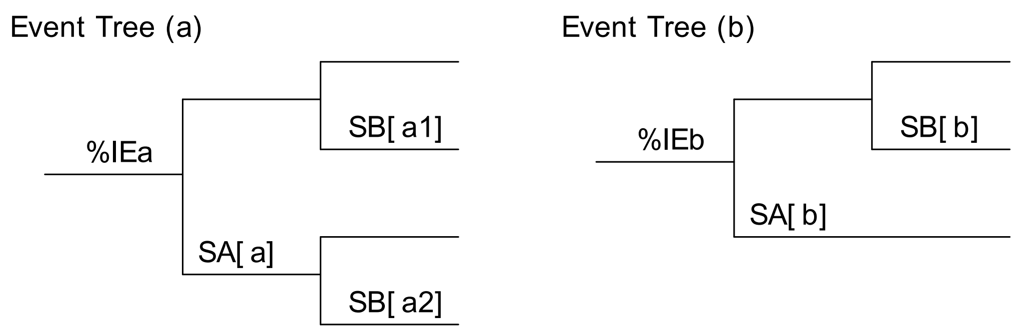
One system fault tree can be used in several places with different conditions in a PSA. Up to now we handle such situation by developing the separate fault trees for each condition and/or using the flag concept. Suppose we develop the separated new fault trees for each condition. This method increases the number of fault trees as the number of conditions increases.

Another approach is to use the flag events in the fault trees. It is the simple way to handle such kind of situation. We can handle most cases via this approach in the one top PSA model which is typically used in a risk monitor. But, there are some cases that we can not model the changed conditions correctly by just using the simple flag setting in the one top PSA model.

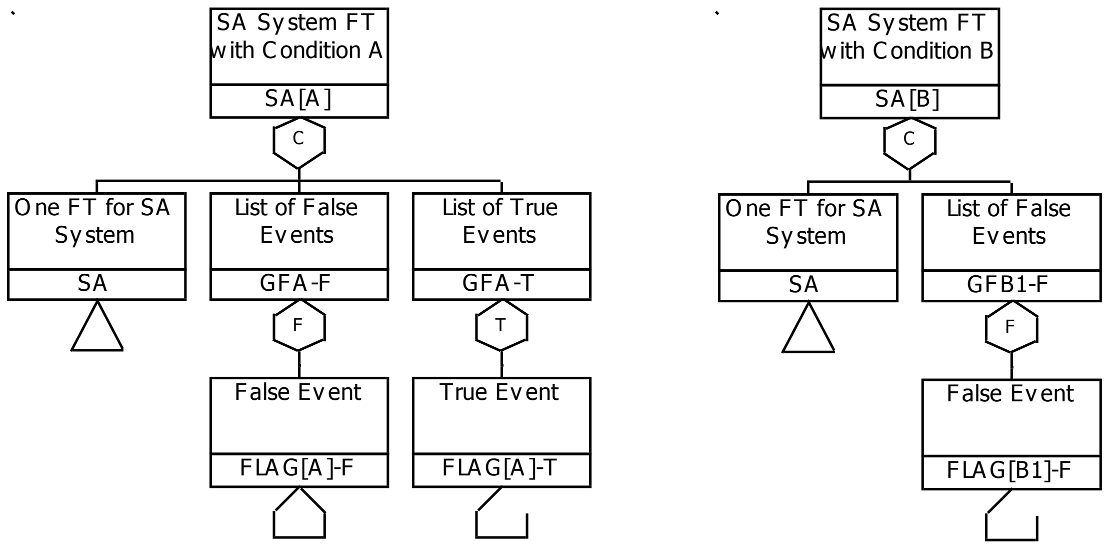
We introduce new type of a gate, the Condition Gate, to use the conventional flag setting method in a one top PSA model. For example, a system SA is modeled in 2 event trees. The fault tree model is modified by using flag for each event tree as below;

SA[a] = SA(FLAG[A]-F = False, FLAG[A]-T = True)

SA[b] = SA(FLAG[B1]-F=False)



The following figures illustrate how we use the condition gates to handle the flag events.



The gate types C, F and T are described in the following table.

Type	Function	Description
C	Condition Gate	Type C can have (1) only one normal gate as a child (2) several Type T Gates as children (3) several Type F Gates as children
T	True Event List	Includes the List of Events set to be True
F	False Event List	Includes the List of Events set to be False

AIMS-PSA takes the fault tree with condition gates. It processes the condition gates, generates a fault tree without the condition gates, and passes the fault tree to the cut set generator. The use of condition gates enables us to build the one top model using the existing event trees and fault trees without excessive effort. It also saves the effort to manage the PSA model.

Component Importance and Uncertainty

We have to calculate the importance of components for many risk informed applications. AIMS-PSA provides the 3 kinds of importance measures (Fussell-Vesely, Risk Reduction Worth, Risk Achievement Worth) as well as the uncertainty bound of importance for grouped events. Because it is an issue how to calculate the risk achievement worth when the common cause failures (CCF) exist, AIMS-PSA calculates the 3 kinds of RAW measures.

Type of RAW	Assumption
Basic RAW (Too conservative)	Pi = 1 for every Event (including CCF events) related to a Component
Balancing RAW	RAW = 1 + [(1-P)/P] * FV, (P = □ Pi) Calculate the RAW based on FV importance
CCF Factor Adjusting RAW (realistic)	Pi(Independent Event) = 1 Pi(CCF Event) = CCF Factor When a component fails, assume that a redundant component fails with a probability of CCF factor.

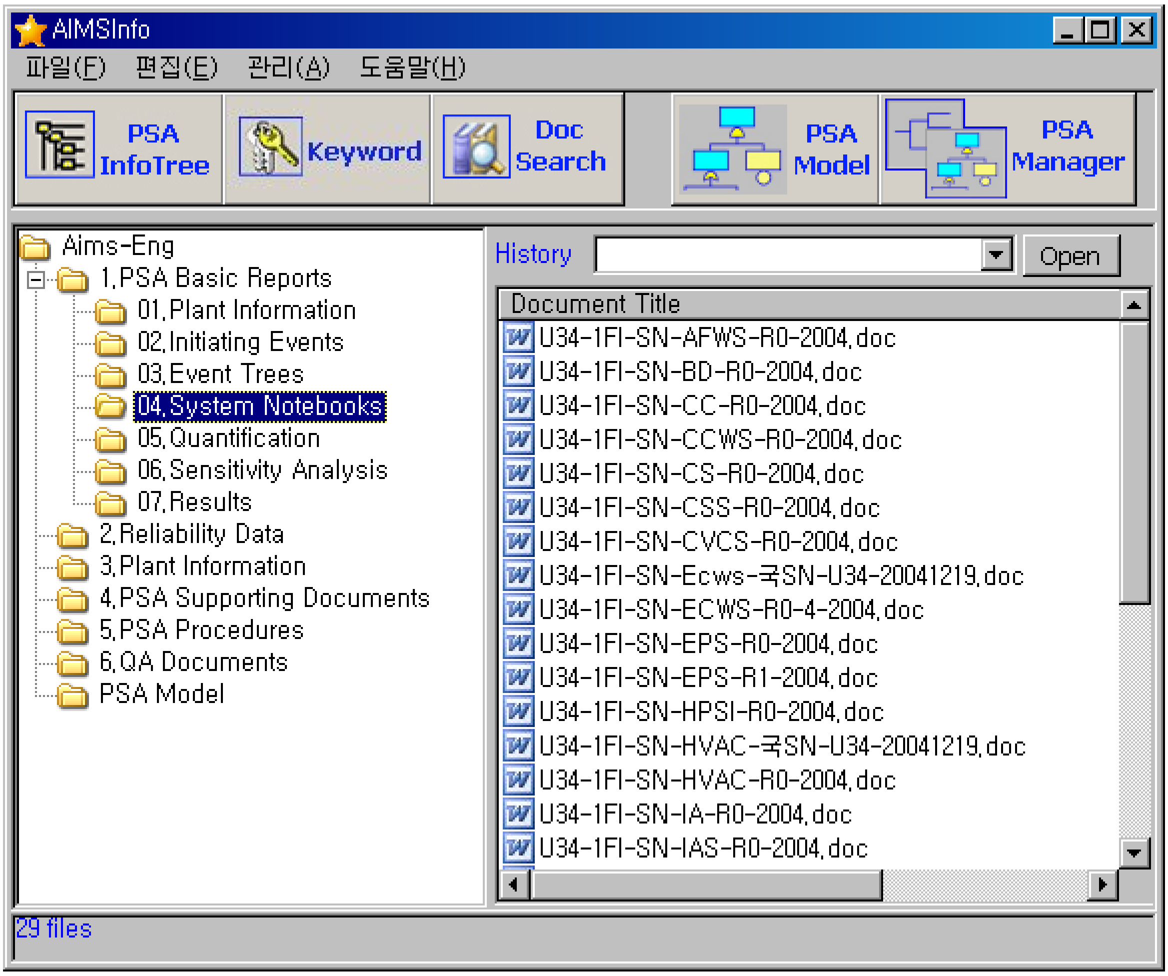
The following table shows the results of the component importance and uncertainty.

Comp	FV	RRW		RAW(CCF=1)		Balancing RAW		CCF Factor RAW	
		RRW	95%	RAW	95%	RAW	95%	RAW	95%
HPSI PUMP-1	0.0327	1.034	1.099	1028.7	2487.2	8.9	25.5	39.6	91.1
HPSI PUMP-2	0.0327	1.034	1.094	1028.8	2492.4	8.9	26.9	39.7	94.5
HPSI Pump Disch. CV SI-404	0.0038	1.004	1.010	507.1	1233.9	17.6	62.8	18.0	41.9
HPSI Pump Disch. CV SI-405	0.0038	1.004	1.011	507.1	1235.1	17.6	59.9	18.1	42.4
Sump Iso. MOV SI-675	0.0006	1.001	1.001	13.6	33.7	1.3	1.8	1.6	2.3
Sump Iso. MOV SI-676	0.0009	1.001	1.002	14.0	34.2	1.5	2.1	2.0	3.5

PSA Information System AIMS-INFO

PSA Information System AIMS-INFO is developed. All the information such as documents and drawings is stored hierarchically in the AIMS DB.

The AIMS-INFO provides a hierarchy tree viewer for PSA information such as a table of contents for the whole PSA. A user can find a document from the information tree by handling (expanding or collapsing) the tree control of the window. The following figure shows the information tree on the left side. We can open and view a document displayed on the right side.



Improvement of Level 2 PSA

One aspect of R&D related to Level 2 PSA has been focused on qualification of the existing Level 2 PSA model (under developed for operating license) and improvement of its implementation methodology for risk-informed application (RIA). The ASME PRA Standard for RIA has been utilized as a key reference for the forgoing purpose. As a result, there have been remarkable improvements for a few issues as follows:

- Methodology development for formal integration of the decoupled Level 1 and 2 PSA Model into a single operational PSA model and its practical implementation (made under the Level 1&2 coupled PSA code package 'KIRAP-FTREX-CONPAS').
- Methodology development and for a rule-based transformation of a full Level 2 PSA model to a simplified LERF model and its practical implementation.
- Assessment of the plant-specific impact of different pressurization rates (i.e., quasi-static and dynamic loads) in the estimation of containment failure mode probabilities
- Assessment of uncertainty bound due to different binning of the Level 1 accident sequences into the Level 2 plant damage states (PDSs) (currently underway).

Another aspect of the Level 2 PSA R&D has been closely related to uncertainty analysis, including the following items:

- Qualification of the various sources of uncertainty addressed in the Level 2 PSA and development of a formal guidance for assessing them
- Development of a methodology for formally integrating both Level 1 and 2 uncertainties

- Development of the application-specific procedures for eliciting judgments from experts in assessing the Level 2 uncertainty issues

PSA for Digital Computer Systems

The PSA methodology development for digital computer system becomes an urgent issue in Korean because digital technologies have been adopted for safety-critical functions in recent nuclear power plants. Even though they consist of many redundant channels and utilize various monitoring mechanisms for the fault tolerance, the high complexity of internal hardware structure, the complicated/flexible functional assignment, and the use of software increase the necessity of a careful investigation on the digital system's risk assessment. The important issues being addressed in KAERI for a realistic risk evaluation for digital safety-critical systems are:

– Modeling the multi-tasking of digital systems,

– Estimating software failure probability in consideration with the effect of V&V,

– Estimating the coverage of fault-tolerant features such as watchdog timers,

– Modeling the CCF for many trains (more than 8 redundancies),

– Modeling the effect of network failure when the network is used for safety function,

– Digital system induced initiating events including human errors.

Human Factors and HRA

In KAERI, OPERA (Operator PErformance and Reliability Analysis) database has been developed. The main role of OPERA database is to provide plant-specific and domain-specific human response times to HRA. And also it can be used as technical bases for human performance researches. To this end, over 130 audio-visual records for the re-training sessions of licensed main control room operators have been collected by using a full scope simulator of KSNP. Major emergency tasks and their response times were analyzed by goal-means task analysis and time-line analysis respectively. Some data of the result have already been used for a HRA to assess the diagnosis error probabilities on post-initiating human failure events.

The MDTA (MisDiagnosis Tree Analysis)-based method was developed to systematically assess the potential for diagnosis failures in emergency situations and their impacts on the plant safety. The MDTA framework provides an appropriate taxonomy of misdiagnosis causes and guidance on the incorporation of those into the estimation of the diagnosis failure probability (DFP) for a given event. The results of the MDTA include possible misdiagnosis events with their diagnosis failure probabilities (DFPs) and misdiagnosis paths with the probable misdiagnosis causes. After conducting the MDTA, one analyses the impacts of the misdiagnosis for the unscreened-out misdiagnosis events. The method also proposes some guidance on the identification of the unsafe actions that might occur from the misdiagnoses, and on a rough quantification scheme for their assessment and modelling into a PSA framework. The developed method has been applied to the small LOCA event, resulting in the diagnosis failure probability of 6.47E-3 and in the risk impact of 5.4 % increase in total CDF.

9.2.12 Japan

Reliability Analysis for Digital Safety Protection System

In Japan a few of NPPs under commercial operation or construction , such as advanced BWR (ABWR) and APWR, have introduced digital control systems to the safety system. Utilities and JNES have made level 1 PSA for ABWR, including reliability analysis of digital safety system. In the PSA of JNES both hardware and software failures of the digital safety system were taken into account mainly based on IAEA-IWG-NPPCI-94/8, IAEA-TECDOC-581 and so on.

Central Research Institute of Electric Power Industry (CRIEPI) started the collection of failure data and population data about digital control units for the following components: Computing unit (Digital Trip Module, Trip Logic Unit, Safety Logic Unit), Interface, Input/Output devices, Logic card, Load Driver, Power unit, Manual switch, Flat display switch, Optical cable and Optical connector (Some of failures are coped with every function). Software failures are classified to V&V (Validation and Verification) error and Configuration error. CRIEPI compiled first report on failure data, population, definitions for boundaries and failure mode about digital control units in March, 2004. Human Reliability Analysis

JNES and CRIEPI have programs on various aspects such as human reliability analysis, man-machine interface research, operational management, training, utilization of artificial intelligence for operational aid and collection and analysis of human reliability data. Utilities are collecting and analyzing human behavior data at their training centers.

JNES is pursuing to establish a HRA project to make HRA database, which can be used in PSA. Current HRA methodology used in PSA in Japan is mainly THERP. The roles of the project are (1) to confirm the applicability of THERP to PSA including HEPs (human error probability) obtained under Japanese circumstances, and (2) to make human failure event analysis using emerging PSA methodology.

Reliability Analysis for Passive Safety Features

In future large-scale FBR systems, it is examined to adopt passive safety features in addition to active ones to enhance the reactor safety. In order to understand the safety level of such systems, JAEA implemented a sensitivity analysis on plant response under the unprotected-loss-of-flow (ULOF) event, which is a typical initiator of the core disruptive accident, in the model plant equipped with the passive safety features such as the curie point electromagnet type of the self-actuated shutdown system and the gas expansion modules at the reactor core. Based on the ULOF analysis result, the failure probability of the passive features was preliminarily estimated by considering uncertainty factors of various design parameters such as actuation temperature, effective reactivity insertion, etc.

Component Reliability Database

Component reliability data for commercial light water reactor plants are collected by the utilities and centralized at CRIEPI and JNES, and those are statistically analyzed by these organizations. A set of component reliability data for PSA developed by CRIEPI, which is the first one reflecting operational experience of Japanese NPPs, was reviewed by the voluntary committee in NSRA consisting of representative PSA-specialists from governmental organizations and industry groups, and issued after some modifications in March 1997. CRIEPI revised this set of data expanding to 1997 for 49 LWRs, which was issued in February 2001.

CRIEPI established NUCIA to publish troubles and subtle events occurring in Domestic NPPs on October 2003. NUCIA is open not only to the utilities but also to the general public on Website, so as to prevent troubles in NPPs from occurring, to upgrade operation and maintenance (O&M) and to improve the transparency of administration of NPP. In NUCIA, to assist reliability assessment at domestic NPPs, CRIEPI developed a "Nuclear Component Reliability Data System" that collects data on failures and troubles of major components and component specification data over a long period, and processes the data to calculate reliability data such as component failure rate. Using this system, CRIEPI has organized a domestic database. With the use of this system, one can analyze, for example, failure rates and numbers of occurrences of failures by component and failure rates by mode, to comprehend the reliabilities of nuclear components by statistical processes. Following the establishment of JANTI, the administration of NUCIA is placed under the authority of JANTI.

In order to expand the statistical population of the component reliability database and statistical analysis system (CORDS) for FBR, JNC continues to make an effort to collect the operational data and failure data primarily related to FBR-specific components from the experimental fast reactor "JOYO" and the prototype FBR "MONJU" in Japan.

Level 2 PSA

In a program of "Development of Level 2 PSA Methodology", JAERI developed the THALES/ART code and its advanced code THALES-2 for analyzing progression of a core melt accident and fission product release and transport behavior. Improvements of aerosol transport and iodine chemistry models of THALES-2 are on going based on experimental data such as the WIND experiments of JAERI.

In the utilities the MAAP code has been extensively applied to examine effects of various accident management countermeasures on mitigation of accident progressions for implementing of accident management measures.

In JNES the MELCOR code has been extensively applied to analysis for prevention and mitigation of various severe accident progressions under AM conditions for 4 types of PWRs (2-loop, 3-loop, 4-loop with a large dry containment and 4-loop ice-condenser type) and 4 types of BWRs (BWR-3 Mark-I, BWR-4 Mark-I, BWR-5 Mark-II and ABWR). A program on source term analysis for the typical BWR plants has been finished to September 2003 but another program for the typical PWR plants has been conducted in 2003. These programs have obtained source term profiles of all accident sequences that lead to containment failure including various large early release sequences. In these programs, residual risk profiles will be provided for level 3 PSA. Also, source term analyses for shutdown conditions including a mid-loop operation condition has been conducting for a 4-loop PWR plant with a large dry containment.

In addition to level 2 PSA for internal events at the full power operation, programs regarding with level 2 seismic PSA for 2 types of BWRs (BWR-4 Mark-I, BWR-5 Mark-II) and a type of PWR (4-loop with a large dry containment) have been obtained with tentative conditional containment failure frequencies with using level 1 seismic PSA results.

Level 3 PSA

JAERI has developed the OSCAAR computer code package, which consists of interlinked computer codes to predict (a) transport of radio nuclide through the environment to man, (b) subsequent dose distributions, and (c) health effects in the population. Level 3 PSA for a generic LWR is in progress for providing inputs to discussions on various safety related issues such as the safety goals and the effectiveness of emergency measures.

NUPEC has investigated models of MACCS to estimate the effectiveness of the AM on the off-site radiological consequence and has developed database in accordance with Japanese environmental characteristics. The MACCS-2 code has applied to estimate radiation dose profiles and residual risk profiles to accumulate technical information for the discussions on safety goals. Based on the source term of internal events at full power operation obtained in Level 2 PSAs for the typical PWR and BWR plants, Level 3 PSAs have been implemented and the average individual risks which satisfy the safety goals have been obtained. Preliminary risk evaluations have been started to the seismic conditions.

Seismic Risk Analysis

JAERI and JNC have established whole sets of methodologies for seismic risk analysis of LWR and FBR, respectively. JAERI published a report on its seismic PSA for a generic BWR in 1999. Recent activities at JAERI were directed to application of the methodology to issues in seismic design and seismic risk management, including the studies on (a) the use of seismic hazard analysis for determining scenario earthquakes for seismic design, (b) the use of seismic PSA for NPPs sited on Quaternary Deposits, and (c) risk management for seismic risk at existing plants.

NUPEC started the development of comprehensive methodologies for seismic risk analysis in 1994. The preliminary seismic PSA analysis of a Japanese typical BWR has been performed since 1997. Seismic hazard curves for typical NPP sites were evaluated by the use of empirical attenuation equations and faulting models. Seismic sources and ground motion propagations for each site were modeled by reflecting experts' opinion. Japanese specific seismic fragility data have been analytically pursued on the basis of both the structural analysis and Japanese seismic proving test data. Fragility data, especially uncertainties of their capacity of active components and electrical components, were re-evaluated with experts' opinion.

In 2001, NSC started the work to deliberate on the revision of the current seismic design evaluation criteria that had been used since 1981. In this work seismic safety evaluation using seismic PSA, design ground motion due to unidentified seismic sources, etc. have been listed as one of important issues for the deliberation. Based on these discussions, NUPEC started in 2002 fragility tests (shaking table tests) for active components such as electrical and control equipment, pumps, control rod driving system and their critical elements, which are dominantly contributing to core damage frequency in preliminary seismic PSA of typical BWR and PWR. These fragility tests have been performed by the use of the Tadotsu large shaking table and also smaller size shaking test facilities in Japan. The target of these tests is to find functional failure limits and failure modes of these components. At the same time, activity of seismic PSA has been intensified, where detail system models of seismic PSA have been developed for typical BWRs and PWRs and fragility evaluation has been done with revised seismic hazard curves and component/structure capacity data of domestic NPPs.

NUPEC's activities are succeeded by JNES. JNES has upgraded seismic PSA methodology (such as seismic hazard evaluation based on faulting model), developed fragility data and so on. At JNES a study on the design ground motion based on the probabilistic approach has been also performed. Especially this approach is important for unidentified near-field earthquakes. Faulting model was applied to various kinds of potential buried faults, and relations between response spectra and exceedance probability of ground motions from these buried faults (unidentified near-field earthquakes) were obtained under a standard soil condition and seismic circumstance in Japanese island. Currently the application of the seismic PSA technologies is going to widen to the reactor shutdown state.

Fire Risk Analysis

Since 1998 NUPEC has made fire severity factors to be applied in fire PSAs for Japanese NPPs, using fire simulation codes and fire experiments. NUPEC has prepared fire severity factor for every categorized fire source, taking into account specific circumstances of fire source components deployed. Using these fire severity factors JNES has made fire PSAs for typical BWR and PWR during rated power operation and shutdown operation.

PSA for Other External Event

JAERI conducted a preliminary study on PSA methodology for external events other than seismic and fire events in 1994 to 1998. This study aims at proposing a screening methodology to identify external events for which detailed examinations of hazard and/or plant fragility are necessary. It has proposed a screening methodology for volcanic activities.

9.2.13 Italy

R&D activities in nuclear safety research with respect to PSA aspects have concerned mainly the following subjects.

- development of improved and new methods and models for passive system reliability [1,2, 3, 4,5];
- modelling of ageing, in reliability and probabilistic safety assessment studies, APSA (ageing PSA), [6]
- application of PSA approach to Non Reactor Nuclear Facilities, with reference to, e.g., fusion plants and accelerator driven systems for waste transmutation purpose.

9.2.14 Hungary

The PSA related R&D activity in Hungary can be considered as applied research, i.e. an activity which directly supports an ongoing PSA application. The current interests are as follows.

Human Factor Analyses

Much attention has been paid at human reliability analyses (HRA) since the beginning of PSA activities in Hungary. Efforts are made to developed HRA methods that can better represent human behaviour and the effect underlying situational characteristics for various types of safety related human interactions, including maintenance and operation as well as responses to plant transients. These methods try to integrate field experience, insights from event reports, results of simulator observations, and expert opinion into a common framework to help HRA modelling and quantification. Also, VEIKI develops data collection and analysis systems in support of identifying strengths and weaknesses in human performance and providing input for use in HRA.

System Reliability Analyses

A new set of Nuclear Safety Codes were issued in May 2005. The fulfillment of the requirements included in the Codes have to be demonstrated during the updating of the current Final Safety Analyses Report [FSAR]. To prepare this FSAR-updating a multiyear project has been initiated for complex reliability assessment of systems discussed within the FSAR. This assessment has 5 main objectives:

- to quantify the reliability/availability of system safety functions,
- to evaluate the protection against common mode failures on functional level,
- to demonstrate the fulfillment of the single failure criteria on functional level,
- to assess the protection against human failures,
- to estimate the protection against internal hazards such as fires, floods and flying objects.

The FSAR has been reviewed and the scope of safety related systems to be analyzed have been outlined. It covers the main systems and their supporting auxiliary systems, too. The electrical power supply system is modeled as contributors to the safety functions. Further study needed to integrate the results of these detailed system reliability studies into the event logic models of the current PSAs.

Reliability Data Base Updating

A three-year project was initiated in 2004 to update the component reliability data base of the Paks NPP PSA studies. This data base updating project includes both the collection of raw statistical data available at the site and their combination with appropriate generic failure parameters. The Bayesian approach was selected to perform this combination.

The review of the initiating event statistics, as well as of the mechanical component failure data has been performed. Currently the statistical information of the electric and C/I component failures are under evaluation, as well as the Bayesian updating of all component data is being performed.

The project is also aiming at the definition of further requirements on failure data collection to be performed through the newly developed Integrated Technical Data System (IMR) being implemented at the Paks NPP recently.

Modeling of the Symptom-Based Emergency Operating Procedures

New symptom-based emergency operating procedures have been introduced at Paks NPP, consequently the earlier (based on event-oriented EOPs) PSA models have to be modified. This modification has to cover the revision of all event sequences where operator interactions are involved. As a result booth the logic structure of the failure event model and the human error probabilities are to be modified.

The modelling of the new symptom-based EOPs within the internal event PSAs is ongoing, while its consideration in the seismic (full power, low power and shutdown, level 2) PSAs requires further efforts in the near future.

Extension of the Scope of the Current PSAs

The main effort to extend the scope of PSAs is devoted to perform seismic studies for low power and shutdown states, as well as on level 2.

The level 1 shutdown seismic PSA is going to be based on the full power seismic PSA, i.e. the available input hazard curves, failure logic models, as well as equipment fragility curves and data will be reviewed to prepare a consistent set of input information for quantification of the core damage frequency included by the seismic effects.

The level 2 seismic PSA is to be concentrated on full power operational mode in the first phase with a potential extension to shutdown states. The study will be based on the internal event level 2PSA, i.e. first the available plant damage states will be reviewed and extended considering the seismic effects, then the containment event trees will be supervised and after necessary modifications quantified.

Risk-Informed Maintenance and Inspection

Currently preliminary studies are being performed to prepare the introduction of a wide-scope maintenance efficiency monitoring system at Paks NPP, as well as to investigate the potential applicability of risk-informed inspections.

The planned maintenance efficiency monitoring is to comprise booth deterministic and probabilistic approaches. The latter one will be based on the quantification and evaluation of such probabilistic safety indicators of systems and equipment which are related to the maintenance performance. The necessity of this activity is prescribed by a specific guide issued by the Nuclear Safety Directorate of the Hungarian Atomic Energy Authority, its importance is highlighted by the planned technical life extension of the Paks NPP, too.

Meanwhile a feasibility study is being performed to evaluate the practical conditions and scope of risk-informed inspection of equipment. This study is based on the NEA-JRC RISMET project aiming at identifying the impact of various RI-ISI methodologies applied to the same technology on the reactor safety.

9.2.15 Germany

In the draft version of new sub-legal nuclear safety regulations currently under preparation, it is required that the PSA to be performed in the frame of the Safety Reviews (SR) at a time interval of ten years for each reactor unit, will be updated in shorter time intervals under certain circumstances (e.g., new PSA relevant results from operation or safety research). This is also important for the application of plant specific PSAs for the assessment of operational events ("precursor studies"), which have been performed by GRS for many years on behalf of the federal nuclear authority.

9.2.16 France

Level 1 PSAs development and updating

As indicated in section 5, EDF and IRSN are both working on the updating of the level 1 PSA relating to 900 and 1300 MW plant series.

Moreover EDF updates the level 1 PSA relating to the 1450 MW series and to the EPR project.

Level 2 PSAs development and updating

The updating of level 2 PSA for the French 900 MWe PWR is on-going in IRSN and in EDF.

In IRSN a version of the study was performed in 2003 for power states of reactor.

This version is being updated on the following points:

- plant modifications (recombiners, new severe accident guides …),
- severe accident studies with last version of severe accident codes,
- improvement of uncertainties evaluation for physical phenomena,
- evaluation of core reflooding possibility during the degradation process,
- introduction of shut-down states of reactor,
- interface between level 1/ level 2 PSA,
- assessment of radiological consequences for each release category (with standard meteorological data).

The study is based on ASTEC (severe accident codes), CATHARE 2 - simulator SIPA 2 (thermal-hydraulics), MC3D (steam explosion), CAST3M (mechanical behaviour of containment). When some physical phenomena have been judged inadequately modelized in available codes, some specific simplified parametric models have been developed, especially in the field of advanced core degradation. Particular efforts are made for uncertainties assessment. Recent experimental results, in particular for fission product behaviour (PHEBUS PF program), have been also taken into account. Specific studies of the survivability of equipments under severe accident conditions, including small scale experiments, have also been performed.

In 2005, IRSN has begun a level 2 PSA for French 1300 MWe plant and supporting studies are on-going. This study should be available for the third Periodic Safety Review of these plants (2009) and should be supported by the last experimental results and ASTEC V1 severe accident code.

In EDF a level 1+ PSA (preliminary assessment of containment failure) was developed for the 1450 MW series.

The EPR PSA includes a level 1+ PSA and a level 2 will be developed in a further step.

Fuel Pool PSA

PSA were performed at EDF to assess the risk of core uncovery in the fuel pool due to the loss of the Fuel Pool Cooling System or due to uncontrolled level drop in the pool. Such PSA were performed for the third PSR of the 900 MWe PWR units and was presented to the Standing Advisory Committee for Nuclear Reactors in 2005 and for the EPR Preliminary Safety Assessment Report (expected in April 2006).

Fire PSA

In IRSN the Fire PSA for the 900 MW series is updated.

The IRSN Fire PSA takes into account the results of fire tests carried out for studying the behaviour of CCI and electrical cables under thermal load, combustion of electrical cabinets and fire propagation from a compartment to the adjacent ones. The damage time for safety equipment is assessed by use of FLAMME-S computer code qualified by fire test results.

In 2005, IRSN and EDF have begun to prepare specifications of a Fire PSA for French 1300 MWe plant. This study should be available for the third Periodic Safety Review of these plants (2009).

Ageing PSA

Investigations are in progress in IRSN for introducing ageing effects in PSA models. These investigations need a detailed review of data. A workshop was organised (in cooperation with JRC-Petten) in October 2005.

PSA for new designs

The CEA is involved in the GenIV Forum, mainly in the development of Gas Fast cooled Reactor (GFR) and Sodium Fast cooled Reactor (SFR).

Since January 2006, preliminary feasibility studies are on-going on several possible GFR designs. To help the choice of a reference design at the end of 2007, simplified Level 1 PSA are under development for each of the studied designs, with a specific attention on the optimization of the decay heat removal systems. The used methodology and the program of work for GFR has been presented at the PSA’05 Conference (10-15 September, San-Francisco, California).

Methodological development are currently done on the choice of reliability data for innovative designs, and the influence of the functional reliability of passive systems on the PSA modelling. Part of these works are done in co-operations with JAEA and MIT.

PSA data

EDF set up a specific organization on site and at corporate level in order to update PSA data (reliability data, system unavailability, duration of standard states) at regular intervals. The aim is to support not only living-PSA programs but also to support maintenance and safety management activities.

In 2005, in the framework of the preparation of the third Periodic Safety Review of the 900 MW plant series, discussion with the Safety Authority have been carried out on the set of data for critical system failures which was re-assessed for the purpose of the 900 MW PSA updating.

PSA Methodology

The main results of EDF works on PSA methodology have been presented by EDF experts at the PSA’05 Conference (10-15 September, San-Francisco, California).

The subjects were:

- Level 2 Probabilistic Safety Assessment
- Use of PSA for Beyond Design Basis Accidents

- Importance Factors
- Common Cause Failure Parameters
- Organisational Factors' Impact on Safety – Pilot Study starting from PSA

IRSN methodology developments were presented during several international workshops and meetings:

- Fire PSA (CSNI Fire PSA workshop – June 2005)
- Level 2 PSA (CSNI Severe Accidents and Level 2 PSA workshop – March 2004; CSNI Uncertainties workshop – November 2005; JRC/AEN workshop on emergency and risk zoning – April 2005; SARNET cooperation meetings; PSAM 8 – May 2006;)
- Ageing PSA (IRSN/JRC Workshop – October 2005; PSAM 8 – May 2006)

PSA comparisons

A comparison is conducted between the French 900 MWe series PWR PSA, the Belgian Tihange-1 PWR PSA and the South Africa Koeberg PWR PSA, which have a comparable design. This work is a cooperation between IRSN (France), AVN (Belgium) and NNR (South Africa).

The main technical objective of the comparison was to understand the important differences between the PSA results, and especially to identify if the differences are due to design differences or to differences in PSA methods and data.

Several important insights were drawn from this exercise concerning plant safety, as well as PSA methodology and model improvements. This exercise could be considered as a particularly detailed external review, contributing to PSA quality and completeness.

The main results are presented to the PSAM 8 Meeting (May 2006)

9.2.17 Finland

Analysis of oil spills

The number of marine oil transportation has been rapidly increasing from Russia to Europe. An oil tanker accident in the Finnish Gulf may threaten the safety of Loviisa NPP given that big amount of oil is drifting from the transportation route to the coast of Finland. The oil spills from tanker accidents can range from thousands to hundred thousands oil tons. The large amount of oil getting into the inlet channel of service water system, may seriously increase the accident rate of the plant. The oil spills contribute to the risk most during the annual refueling period when the residual heat removal is in total based on the function of service water system. During the power operation the risk from oil spills is pretty small due to diverse means to remove the residual heat.

The further research of the behavior and drifting of oil in the sea water is worth in order to ensure the frequency of initiating event in PSA

Probabilistic Fire Simulation

A new probabilistic fire simulation method (PFS-TMMC computer code) has been developed in the SAFIR nuclear safety research programme 2003-2006. This method is capable to compute the probability of damage of a component given pilot fire in the proximity of the target component. The method analyses the growth of pilot fire and the possible spreading of it to the target component and the probability that the target component will be damaged in a given time period. The fire alarm, actions of fire brigade and operation of possible extinguishing systems are integrated in the method as random variables. Pilot application on the fire spreading in a cable tunnel between two redundant cable trays is completed as well as the fire spreading between redundant instrumentation cabinets in a large instrumentation room. The integration of the PFS-TMMC program into the PSA models will be implemented in the new nuclear safety research programme 2007-2010.

PSA Info System

A special PSA Info system has been developed in order to use the insights of PSA for training the inspectors, to upgrade their risk perception and to demonstrate the importance of most significant accident sequences. PSA Info system provides a tool to train the inspectors to understand and use the PSA insights while planning the regulatory inspection programs and conducting the inspections at site.

9.2.18 Canada

CNSC is a member of COOPRA and it has a leading role in the activities of the special interest group on Risk-Informed Decision-Making.

In 2004, the USNRC and the CNSC signed the COOPRA five-years agreement (renewable) regarding the participation in the area of Probabilistic Risk Assessment Research [6]. The collaboration includes the following areas of research:

(NRC) – (a) Methods development (fire risk, equipment aging, human reliability, digital systems reliability and risk), (b) Analysis of operating events, (c) Development of PC-based PRA software (SAPHIRE), (d) Regulatory applications of PRA;

(CNSC) – (a) Independent assessment of plant design and reliability, (b) Identification and clarification of safety issues and reduction of uncertainties in plant behavior under operational and postulated accident conditions, (c) Development of regulatory documents on the use of PSA in the regulatory process, and (d) a set of performance indicators, and (e) development and implementation of a risk-informed management process.

CNSC participates in the International Common-Cause data Exchange (ICDE) project. In this respect, CNSC initiated a research contract with an external contractor for collecting data on centrifugal pumps, MOVs, and safety/relief valves.

CNSC is also participating in the WGRISK-ICDE sub-task on quantification of the Common-Cause Failures using the ICDE data.

- In 2005, CNSC staff initiated a research project aimed to incorporating Ageing Effects into PSA Applications. This three phase project is scheduled to be completed over the next three years. The main objectives are to (a) identify aging sensitive CANDU specific equipment, (b) evaluate the impact of incorporated aging effects on plant-specific PSA, (c) assess the need for addressing aging PSA in the regulatory documents and develop tools to account the aging PSA results in RIDM, and (d) share the results of the research project to the international nuclear community through the Ageing PSA network. This is a large project that will require the use of the CNSC expertise in aging, and collaboration with Canadian academia, and other international organisations.

The introduction of Regulatory Standard S-294 will add requirements to address risk from external events and fire (although non-PSA methods are permissible). It will be necessary to ensure that PSA methods are in accordance with best industry practice.

There are on-going developments to address the PRA aspects required for the Reliability Program Implementation in all Canadian nuclear power facilities arising from Regulatory Standard S-98. Among which are (a) the use of time-based versus demand-based data, (b) methodology for determining mission testing requirements, (c) defining reliability performance measures and criteria, and (d) the use of expert panels. These are being studied through an industry Risk and Reliability Working Group under the auspices of COG.

Areas for further review and development may include:

- Process and tools for data collection
- Level 2 methods
- Treatment of uncertainty
- Efforts through industry groups to increase the degree of standardization of PRAs for Candu reactors
- Operational risk management practices and tools.

OPG and BP are also interested in increasing the use of PSA for optimizing plant operations in terms of testing and maintenance, inspection requirements and outage planning. OPG is playing a leading role in the development of risk-informed asset management tools for the North American industry.

9.2.19 Czech Republic

PSA Applications

Development of On-line Safety Monitor which will allow to:

- see immediate risk situation of unit operation to “everybody” at the plant
- make simple ”what-if“ evaluation of planned manipulations
- optimize maintenance activities to reduce risk

Justification of requests to regulatory body to relax system/train AOTs which would optionally allow to:

- optimize maintenance activities
- perform maintenance of safety systems on-line, under at power conditions, thus significantly shorten outage duration while maintaining acceptable operational risk
- Continuation of pilot activities on use and implementation of RI ISI methodology, which would allow to use this approach in real operational practice
- Development and implementation of system on PSA based event evaluation

Living PSA

- Development of integrated Level 1/2 PSA models for all operating states
- Development of guidelines how to treat ageing in PSAs and how to incorporate ageing effects into PSA models
- Analysis of reliability impact on use of expert systems supporting human interventions within mitigation of accidents situations

9.2.20 Belgium

In the framework of the ongoing periodic safety reviews of all plants, discussions took place between TE, Electrabel and AVN to define the future updates of the PSAs for the different plants. For all tasks being part of a PSA level 1 (initiating events, plant operating states, event trees, fault trees, data, human reliability analysis, quantification and interpretation of results) and PSA Level 2 (interface, accident progression event tree, quantification, evaluation of results) an evaluation has been made to investigate whether updates are needed related to plant modifications, corrections to the existing models, changes in methodology, extension of scope and in view of future PSA applications. In these discussions, lessons learned from PSA comparison with other countries (in particular France) are also considered for implementation.

The objective of any of the PSA updates is to verify again the robustness of the plant in its current state:

- taking into account all changes to systems, procedures, and considering an extended operating experience;
- taking into account more refined working hypotheses were necessary (correcting errors, filling gaps, more balanced modelling);
- reconsidering the PSA methodologies to be applied in view of the current state-of-the-art;
- to provide the basis for – existing or anticipated – PSA applications;
- to extend the scope of the PSA (Fire & Flooding PSA);
- to update PSA Level 2 models (including Source Term & LPSD states).

Moreover, improvements in maintainable PSA documentation and ready-to-use computer models are expected.

10 REFERENCES

10.1 USA

American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2002, April 2002, Addendum A, ASME RA-Sa-2003, December 2003, and Addendum B, ASME RA-Sb-2005, December 2005.

Atwood, C.L., et al, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR-6823, Sandia National Laboratories, 2003.

Brown, T.D., et al, “Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant,” NUREG/CR-5305, Sandia National Laboratories, 1992.

Chu, T.L., and W.T. Pratt, “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1,” NUREG/CR-6144, Brookhaven National Laboratory, 1995.

Electric Power Research Institute, “2007 Portfolio: AP41.09, Safety Risk Technology and Application,” 2006.

Electric Power Research Institute and U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,” NUREG/CR-6850 / EPRI 1011989, 2005.

Gaertner, J., D. True, and I. Wall, “Safety benefits of risk assessment at U.S. nuclear power plants,” Nuclear News, pp. 27-36, 2003.

Mosleh, A., D.M. Rasmuson, and F.M. Marshall, “Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,” NUREG/CR-5485, Idaho National Engineering and Environmental Laboratory, 1998.

National Fire Protection Association,“Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” NFPA 805, 2001.

Nuclear Energy Institute, “Guidance for Post-Fire Safe-Shutdown Circuit Analysis,” NEI-00-01 Rev. 1, 2005,

Nuclear Energy Institute, ”10 CFR 50.69 SSC Categorization Guideline,” NEI 00-04 Rev. 0, 2005.

Nuclear Energy Institute, Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program Under 10 CFR 50.48(c),” NEI-04-02 Rev. 1, 2005.

Payne Jr., A.C., et al, “Analysis of the LaSalle Unit 2 Nuclear Power Plant: Risk Methods Integration and Evaluation Program (RMIEP),” NUREG/CR-4832, Sandia National Laboratories, 1992.

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

U.S. Nuclear Regulatory Commission, “Safety Goals for the Operation of Nuclear Power Plants; Policy Statement; Correction and Republication,”Federal Register, Vol. 51, p. 30028 (51 FR 30028), August 21, 1986.

U.S. Nuclear Regulatory Commission, “Individual Plant Examination (IPE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f),” Generic Letter 88-20, 1988.

U.S. Nuclear Regulatory Commission, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants,” NUREG-1150, 1990.

U.S. Nuclear Regulatory Commission, “Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f),” Generic Letter 88-20, Supplement 4, 1991.

U. S. Nuclear Regulatory Commission, “Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement,” Federal Register, 60, p. 42622 (60 FR 42622), August 16, 1995.

U.S. Nuclear Regulatory Commission, “Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance,” NUREG-1560, 1997.

U.S. Nuclear Regulatory Commission, “An Approach for Plant-Specific, Risk-Informed Decision-making: In-service Testing,” Regulatory Guide 1.175, 1998.

U.S. Nuclear Regulatory Commission, “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance,” Regulatory Guide 1.176, 1998.

U.S. Nuclear Regulatory Commission, “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications,” Regulatory Guide 1.177, 1998.

U.S. Nuclear Regulatory Commission, “Options for Risk-Informing Revisions to 10 CFR Part 50 - Domestic Licensing of Production and Utilization Facilities,” SECY-98-300, 1998.

U.S. Nuclear Regulatory Commission, “Reactor Oversight Program,” NUREG-1649, Rev. 3, 2000.

U.S. Nuclear Regulatory Commission, “Consolidated Line Item Improvement Process For Adopting Standard Technical Specifications Changes for Power Reactors,” RIS 2000-06, 2000.

U.S. Nuclear Regulatory Commission, “NRC Incident Investigation Program,” Management Directive 8.3, 2001.

U.S. Nuclear Regulatory Commission, “Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria),” SECY-01-0133, 2001.

U.S. Nuclear Regulatory Commission, “Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program,” NUREG-1742, 2002.

U. S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174 Rev. 1, 2002.

U. S. Nuclear Regulatory Commission, “Update to SECY-01-0133, ‘Fourth Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50 (Option 3) and Recommendations on Risk-Informed Changes to 10 CFR 50.46 (ECCS Acceptance Criteria)’,” SECY-02-0057, 2002.

U.S. Nuclear Regulatory Commission, “An Approach for Plant-Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping,” Regulatory Guide 1.178 Rev. 1, 2003.

U. S. Nuclear Regulatory Commission, “Staff Requirements - COMNJD-03-0002 - Stabilizing the PRA Quality Expectations and Requirements,” Staff Requirements Memorandum COMNJD-03-0002, 2003.

U. S. Nuclear Regulatory Commission, “Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission,” NUREG/BR-0058, Rev. 4, 2004.

U. S. Nuclear Regulatory Commission, “Effective Risk Communication: The Nuclear Regulatory Commission’s Guidelines for External Risk Communication,” NUREG/BR-0308, 2004.

U. S. Nuclear Regulatory Commission, “Effective Risk Communication - Guidelines for Internal Risk Communication,” NUREG/BR-0318, 2004.

U. S. Nuclear Regulatory Commission, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Regulatory Guide 1.200 for trial use, 2004.

U. S. Nuclear Regulatory Commission, “Issues Related to Proposed Rulemaking to Risk-Inform Requirements Related to Large Break Loss-Of-Coolant Accident (LOCA) Break Size and Plans for Rulemaking on LOCA with Coincident Loss-Of-Offsite Power,” SECY-04-0037, 2004.

U. S. Nuclear Regulatory Commission, “Plan for the Implementation of the Commission’s Phased Approach to PRA Quality,” SECY-04-0118, 2004.

U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis (HRA),” NUREG-1792, 2005.

U. S. Nuclear Regulatory Commission, “Technical Basis for Revision of the Pressurized Thermal Shock (PTS) Screening Limit in the PTS Rule (10CFR50.61): Summary Report,” NUREG-1806, 2005.

U. S. Nuclear Regulatory Commission, “Status of the Accident Sequence Precursor (ASP) Program and the Development of Standardized Plant Analysis Risk (SPAR) Models,” SECY-05-0192, 2005.

U. S. Nuclear Regulatory Commission, “Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance” Regulatory Guide 1.201, Rev. 1, 2006.

U.S. Nuclear Regulatory Commission, “Human Event Repository and Analysis (HERA) System, Overview,” NUREG/CR-6903, 2006.

U.S. Nuclear Regulatory Commission, “Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants,” Regulatory Guide 1.205, 2006.

U.S. Nuclear Regulatory Commission, “Changes to the Safety System Unavailability Performance Indicators,” RIS 2006-07, 2006.

U.S. Nuclear Regulatory Commission, “Update of the Risk-Informed Regulation Implementation Plan,” SECY-06-0089, 2006.

Whitehead, D.W., “Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1,” NUREG/CR-6143, Sandia National Laboratories, 1995.

10.2 United Kingdom

[1] ‘The Tolerability of Risk From Nuclear Power Plants’; HSE Books 1992, IBSN 0 11 882043 5

[2] ‘Safety Assessment Principles for Nuclear Plants’; HSE Books 1992, IBSN 0 11 886368 1

[3] ‘Reducing Risks, Protecting People; HSE’s Decision Making Process’; HSE Books 2001, IBSN 0 7176 2151 0

[4] ‘Hinkley Point C Inquiry’ report Transcript of Proceedings, 1989 JL Harpham Ltd, 55 Queen Street, Sheffield S1 2DX

[5] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), IAEA Safety Series No 50-P-4, Vienna

[6] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), IAEA Safety Series No 50-P-8, Vienna

[7] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA Safety Series No 50-P-12, Vienna.

10.3 Taiwan

1. AEC, "Probabilistic Risk Assessment for Kuosheng Nuclear Power Station," Atomic Energy Council, 1985, Taipei, Taiwan, R.O.C.
2. AEC, "Probabilistic Risk Assessment for Maanshan Nuclear Power Station," Atomic Energy Council, 1987, Taipei, Taiwan, R.O.C.
3. AEC, "Probabilistic Risk Assessment for Chinshan Nuclear Power Station," Atomic Energy Council, 1991, Taipei, Taiwan, R.O.C.
4. Institute of Nuclear Energy Research, “At-Power Living Probabilistic Risk Assessment for Chinshan Nuclear Power Station,” INER-0060, Institute of Nuclear Energy Research, December 1995.
5. Institute of Nuclear Energy Research, “At-Power Living Probabilistic Risk Assessment for Kuoshan Nuclear Power Station,” INER-0061, Institute of Nuclear Energy Research, December 1995.
6. Institute of Nuclear Energy Research, “At-Power Living Probabilistic Risk Assessment for Maanshan Nuclear Power Station,” INER-0062, Institute of Nuclear Energy Research, December 1995.
7. Institute of Nuclear Energy Research, “Shutdown Living Probabilistic Risk Assessment for Chinshan Nuclear Power Station,” INER-0063, Institute of Nuclear Energy Research, June 1998.
8. Institute of Nuclear Energy Research, “Shutdown Living Probabilistic Risk Assessment for Kuoshan Nuclear Power Station,” INER-0064, Institute of Nuclear Energy Research, June 1998.
9. Institute of Nuclear Energy Research, “Shutdown Living Probabilistic Risk Assessment for Maanshan Nuclear Power Station,” INER-0065, Institute of Nuclear Energy Research, June 1998.
10. Tsu-Mu Kao, C.M. Peng, T.J. Lin, C.H. Wu, C.C. Chao, P.L. Hsu, G.D. LI, and C.C Yao, “The Buildup and Application Examples of the Taipower Integrated Risk Monitor (TIRM) During Shutdown Period for Nuclear Power Plants in Taiwan,” Monthly Journal of Taipower’s Engineering (in Chinese), 628, 24-42, Taiwan, December, 2000.
11. Tsu-Mu Kao and Chun-Chang Chao, “The Second Generation of Taiwan’s NPP Risk Monitor, TIRM-2”, The 14th Pacific Basin Nuclear Conference, Honolulu, Hawaii, USA, March 21-25, 2004.
12. Chun-Chang Chao and Jyh-Der Lin, “Streamlining the Evaluation Process of Inspection Findings,” The 20th Sino-Japanese Seminar on Nuclear Safety, Hiroshima, Japan, Nov. 15-16, 2005.
13. James C. Lin, Ching N. Guey, Tsong-Lun Chu and George Apostolakis, “Final Report: Peer Review for Chinshan, Kuosheng, and Maanshan At-Power and Shutdown Living PRAs”, PLG-1432, ABSG Consulting Inc., August 2002.
14. Nuclear Energy Institute, “Probabilistic Risk Assessment Peer Review Process Guidance,” NEI-00-02, Revision A3, March 20, 2000.
15. American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2002, April 5, 2002, and “Addenda to ASME RA-S-2002,” ASME RA-Sa-2003, December 5, 2003.
16. “PRA Procedure Guide, A Guide to the Performance of Probabilistic Risk Assessment for

Nuclear Power Plants," NUREG/CR-2300, USNRC, January 1983.
17. W.T. Pratt, et al, "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," NUREG/CR-6595, Brookhaven National Laboratory, January 1999.
18. Idaho National Engineering and Environmental Laboratory, "Common-Cause Failure Parameter Estimation," NUREG/CR-5497, October 1998.
19. USNRC, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 – 1995," NUREG/CR-5750, U.S. Nuclear Regulatory Commission, Feb. 1999.
20. Idaho National Engineering Laboratory, "Generic Component Failure Data for Light Water and Liquid Sodium Reactor PRAs," EGG-SSRE-8875, February 1990.

10.4 Switzerland

1. Federal Ordinance 0n Nuclear Energy (KEV, SR 732.11)

10.5 Sweden

References – section 2

1. Description of the regulatory framework in Sweden, the PSA environment, *The Nuclear Activities Act (1984:3)*, DOCSOPEN #10491 v1

References – section 3

1. *An Approach for using probabilistic risk assessment in risk-informed decisions in plant-specific changes to the licensing basis*, U.S. Nuclear Regulatory Commission, November 2002, Regulatory Guide 1.174, Revision 1

2. *Probabilistic Safety Assessment - INSAG-6*, IAEA, 1992, Safety Series No. 75-INSAG-6, ISBN 92-0-102492-4.

3. *The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety*, IAEA, 1992, Safety Series No. 106, ISBN 92-0-101492-9.

4. *The Safety of Nuclear Power Plants – INSAG-5*, IAEA, 1992, Safety Series No. 75-INSAG-5, ISBN 92-0-100192-4.

5. *A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards – INSAG-8*, IAEA, 1995, INSAG Series No. 8, ISBN 92-0-102395-2.

6. *Safety Assessment and Verification for Nuclear Power Plants – A Safety Guide*, IAEA, 2001, Safety Standards series, No. NS-G-1.2, ISBN 92-0-101601-8].

References – section 4

1. SKI Report 2002:27, Guidance to External events Analysis].
2. In 2003, SKI produced a report dealing with best estimate of fire frequencies for Swedish NPP:s [in SKI Rapport 2003:25, Branddataprojektet].
3. In 2003 SKI produced the Reviewing handbook of PSA:s. [in Swedish, SKI Rapport 2003:48, Tillsynshandbok PSA].

Widely used international PSA standards and public reports are as follows:

1. ASME; *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications;* ASME RA-S 2002; 2002
2. EUR; *European Utility Requirements for LWR Nuclear Power Plants;* Volume 2. Generic Island Requirements. Chapter 12. PSA Methodology. Rev 2; 2001
3. IAEA; *A Framework for a Quality Assurance Programme for PSA;* IAEA TECDOC-1101; 1999
4. IAEA; *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3);* IAEA Safety Series No 50-P-12; 1996
5. IAEA; *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2);* IAEA Safety Series No 50-P-8; 1995
6. IAEA; *Advances is reliability analysis and probabilistic safety assessment for nuclear power reactors;* IAEA TECDOC-737; 1994
7. IAEA; *PSA for the shutdown mode for nuclear power plants;* IAEA TECDOC-751; 1994
8. IAEA; *Defining Initiating Events for the Purposes of Probabilistic Safety Assessment;* IAEA TECDOC-719; 1993
9. IAEA; *The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety;* IAEA Safety Series No 106; 1992
10. IAEA; *Probabilistic Safety Assessment ;* IAEA Safety Series No 75-INSAG-6; 1992
11. IAEA; *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1);* IAEA Safety Series No 50-P-4; 1992
12. IAEA; *Application of Probabilistic Safety Assessment to Research Reactors;* IAEA TECDOC-517; 1989
13. IAEA; *Probabilistic Safety Assessment for Research Reactors;* IAEA TECDOC-400; 1987
14. STUK; *Probabilistic Safety Analyses (PSA);* YVL-guide 2.8; 2003
15. USNRC; *Individual Plant Examination: Submittal Guidance;* NUREG-1335; 1989
16. USNRC; *Probabilistic Safety Assessment Procedures Guide;* NUREG/CR-2815; 1985
17. USNRC; *PRA Procedures Guide;* NUREG/CR-2300; 1983

Widely used international PSA standards referred to at reviewing of PSA:s, are as follows:

1. EPRI/HSK; A *Probabilistic Safety Assessment Review Guidance for Swiss Nuclear Power Plants*; ERI/HSK 92-1115, HSK-AN-2517; 1992
2. IAEA; *Review of Probabilistic Safety Assessments by Regulatory Bodies*; IAEA Safety Report No. 25; 2002
3. IAEA; *Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2*; IAEA TECDOC-1229; 2001
4. IAEA; *Regulatory Review of Probabilistic Safety Assessment (PSA) level 1*; IAEA TECDOC-1135; 2000
5. IAEA; *IPERS Guidelines for the International Peer Review Service*; IAEA TECDOC-832; 1995
6. NEA CNRA; *Review Procedures and Criteria for Different Regulator Applications of PSA*; 1997 CNRA Special Issue Report; 1998
7. NEI; *Probabilistic Risk Assessment Peer Review Process Guidance*; NEI 00-02; 2000
8. USNRC; *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*; NUREG-800;

Widely used international PSA standards referred to at PSA applications, are as follows:

1. EPRI; *PSA Applications Guide;* TR-105396; 1995
2. IAEA; *Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants;* IAEA TECDOC-1200; 2001
3. IAEA; *Living Probablistic Safety Assessment (LPSA);* IAEA TECDOC-1106; 1999
4. IAEA; *Use of PSA Level 2 analysis for improving containment performance;* IAEA TECDOC-1002; 1998

5. IAEA; *Application and development of probabilistic safety assessment for nuclear power plant operation;* IAEA TECDOC-873; 1996
6. IAEA; *Modelling and data prerequisites for specific applications of PSA in the management of nuclear plant safety;* IAEA TECDOC-740; 1994
7. IAEA; *Use of Probabilistic Safety Assessment for nuclear installations with large inventory of radioactive material;* IAEA TECDOC-711; 1993
8. IAEA; *Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants;* IAEA TECDOC-729; 1993
9. IAEA; *Use of Plant Specific PSA to Evaluate Incidents at Nuclear Power Plants;* IAEA TECDOC-611; 1991
10. IAEA; *Defence in Depth in Nuclear Safety*; IAEA INSAG-10, 1996.
11. IAEA; Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1; IAEA INSAG-12, 1999.
12. NEA CNRA; *Living PSA Development and Application in Member Countries;* Summary of TÜV Workshops held from 1988 to 1994; 1996
13. USNRC; An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis; Regulatory Guide 1.174; 1998
14. USNRC; *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions: Inservice Testing;* Regulatory Guide 1.175; 1998
15. USNRC; *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions: Graded Quality Assurance;* Regulatory Guide 1.176; 1998
16. USNRC; *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions: Technical Specifications;* Regulatory Guide 1.177; 1998
17. USNRC; An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions: Inservice Inspection of Piping; Regulatory guide 1.178; 1998
18. USNRC; *Assessing And Managing Risk Before Maintenance Activities At Nuclear Power Plants;* Regulatory guide 1.182, 2000
19. USNRC; *Issues and Recommendations for Advancement of PRA Technology in Risk-Informed Decision Making;* NUREG/CR 6813
20. USNRC; An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results of Risk Informed activities; Regulatory Guide RG 1.200; 200 4
21. USNRC; *Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities;* Draft Standard Review Plan Chapter 19.1
22. ASME; *Risk-Informed Requirements for Class 1, 2 and 3 Piping, Method A, Section XI, Division 1*; America Society of Mechanical Engineers, Boiler and Pressure Vessel Code, Code Case N-577; September 2, 1997.
23. ASME; *Risk-Informed Requirements for Class 1, 2 and 3 Piping, Method B, Section XI, Division 1*; America Society of Mechanical Engineers, Boiler and Pressure Vessel Code, Code Case N-578; September 2, 1997.
24. Westinghouse;. *Westinghouse Owners Group Application of Risk-Informed Methods to Piping Inservice Inspection Topical Report*; WCAP-14572, Revision 1-NP-A
25. EPRI; *Revised Risk-Informed Inservice Inspection Evaluation Procedure*; EPRI TR-112657, WO 3230; Final report April 1999.
26. EUR; *Report on risk-informed in-service inspection and in-service testing;* EUR 191153

Widely used PSA standards or other public reports, referred to at analysis of CCF:s in PSA:s are as follows:

1. Bento, J-P, Hellström, P; *Redundancy Protection Guidance;* NAFCS PR-12, to be published as SKI Report; 2003
2. IAEA; *Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment;* IAEA TECDOC-648; 1992
3. Johansson, G. et.al.; *Summary Report of the Nordic Working Group on Common Cause failure Analysis;* NAFCS PR-09, to be published as SKI Report; 2003

4. Knochenhauer, M, Mankamo, T; Dependency Analysis Guidance; NAFCS PR-13, to be published as SKI Report; 2003
5. USNRC; Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment; NUREG/CR-5485

Widely used PSA standards or other public reports, referred to at analysis of data in PSA:s are as follows:

1. Angner, A., Pörn, K.; *X-Boken - Inledande Händelser vid nordiska kärnkraftverk - Yttre Händelser;* PC Rapport 96-2; 1996
2. IAEA; *Generic Component Reliability Data for Research Reactor PSA;* IAEA TECDOC-930; 1997
3. IAEA; *Manual on Reliability Data Collection for Research Reactors PSAs;* IAEA TECDOC-636; 1992
4. IAEA; *Survey of ranges of Component reliability data for use in probabilistic safety assessment;* IAEA TECDOC-508; 1989
5. IAEA; *Component Reliability Data for Use in Probabilistic Safety Assessment;* IAEA TECDOC-478; 1988
6. SKI; *I-boken, Inledande händelser vid nordiska kärnkraftverk, version 2;* SKI Rapport 94:12; 1994
7. TUD-kansliet, m.fl.; *T-boken, Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer, version 4;* ISBN 91-7186-303-6; 1995

Widely used PSA standards or other public reports, referred to at analysis of external events in PSA:s are as follows:

1. ANS; *External Events PRA Methodology Standard;* ANS-58.21 [3.6-2] Draft,; 2002
2. IAEA; *Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants;* IAEA Safety Report No. 10; 1998
3. IAEA; *Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants;* IAEA Safety Series No 50-P-7; 1998
4. IAEA; *Probabilistic Safety Assessment for Seismic Events;* IAEA TECDOC-724; 1993
5. IAEA; *External events;* IAEA Safety Guide 50-SG-S9
6. Knochenhauer, M., Louko, P; *Guidance for External Events Analysis;* SKI Report 02:27; 2002
7. USNRC; *Procedural and Submittal Guidance for the Individual Plant Examination of* USNRC*; External Events (IPEEE) for Severe Accident Vulnerabilities, Final Report;* NUREG-1407; 1991
8. USNRC; *Procedures for the external event core damage frequency analyses for NUREG-1150.;* NUREG/CR-4840; 1990
9. USNRC; *External event analysis methods for NUREG-1150. ;* NUREG/CP-0104

Widely used PSA standards or other public reports, referred to at analysis of human errors in PSA:s are as follow:;

1. IAEA; *Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants;* IAEA Safety Series No 50-P-10; 1995
2. USNRC; *Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications;* NUREG/CR-1278; 1983

Widely used PSA standards or other public reports, referred to at analysis of uncertainties in PSA:s are as follows:

1. USNRC; *Approaches to Uncertainty Analysis in Probabilistic Risk Assessment;* NUREG/CR-4836; 1988
2. USNRC; *Handbook of parameter estimation for PRA;* NUREG/CR-6823; 2003

10.6 Spain

[1] "Programa Integrado de realización y utilización de los Análisis Probabilistas de Seguridad (APS) en España" CSN, Colección Otros Documentos.1998.

[2] Guía de Seguridad 1.14. "Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad".2001

[3] Guía de Seguridad 1.15. "Actualización y mantenimiento de los Análisis Probabilistas de Seguridad". 2004.

10.7 Slovenia

[1] NEK Baseline PSA Model "NEKC18"Report number: NEK ESD-TR-07/01, Rev. 0

[2] Re-modeling of Two-component Common Cause Failures: NEK ESD TR-07/01, Rev. 0, Appendix F

[3] NEK PSSA Final Report: NEK ESD-TR-10/98, Rev.1

[4] SPSA-ABS-NEK-2004-003, Seismic Probabilistic Safety Assessment of Krško Nuclear Power Plant, Level 1 and Level 2, Rev. 2, 2004.

[5] Probabilistic Safety Assessment of Nuclear Power Plant Krško Level 1 Report, Volume 1, January 1994.

10.8 Slovak Republic

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

Application of PSA Methodology in the Regulatory Process, UJD, BNS I.4.2/2005, Bratislava, Slovakia, 2005

Full Power Level 1 PSA Study for Unit 2 of J. Bohunice V1 after Implementation of Symptom-based Emergency Procedures, RELKO Report, No. SB-FP-L1V1U1-PSA-MR/ 3R0803/A, Bratislava, January 2004

Shutdown Level 1 PSA Study for Unit 2 of J. Bohunice V1 after Implementation of Symptom-based Emergency Procedures, RELKO Report, No. SB-SD-L1V1U1-PSA-MR/4R0803/A, Bratislava, January 2004

Full Power Level 1 PSA Study for Unit 1 of J. Bohunice V1 after Implementation of Symptom-based Emergency Procedures, RELKO Report, No. SB-FP-L1V1U1-PSA-MR/ 1R0803/A, Bratislava, January 2004

Shutdown Level 1 PSA Study for Unit 1 of J. Bohunice V1 after Implementation of Symptom-based Emergency Procedures, RELKO Report, No. SB-SD-L1V1U1-PSA-MR/2R0803/A, Bratislava, January 2004

PSA Model of Full Power and Shutdown Reactor for Unit 3 of J. Bohunice V2 NPP after Modernization EFWS, RELKO, Bratislava, Slovakia, 2003

Actualization of Level 1 PSA Study for Unit 1 of NPP Mochovce, Main Report, VUJE, Trnava, December 2005

10.9 Netherlands

1. Nuclear Energy Act; Nuclear Installations, Fissionable Materials and Ores Decree (Part of the Nuclear Energy Act)
2. ‘Conditions for installing new nuclear power plants in The Netherlands’; Lower House of the States General, 2006-2007session, 30000 No. 40, september 28, 2006
3. ‘Premises for Risk Management; Risk Limits in the Context of Environmental Policy’; Lower House of the States General, 1988-1989 session, 21137, No. 5, The Hague 1989
4. U.S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisioons on Plant-Specific Changes to the Licensing Basis,”Regulatory Guide 1.174 Rev. 1, 2002.

Guidance documents:

- U.S. Nuclear Regulatory Commission, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities; NUREG/CR-6850, 2005.

10.10 Mexico

1. “An approach for using probabilistic risk assessment in risk informed decision on plant specific changes to the licensing basis”, Regulatory guide 1.174, U.S. Nuclear Regulatory Commission, 2002.
2. “An approach for Plant-Specific, Risk informed Decision making: Technical Specifications”, Regulatory Guide 1.177, U.S. Nuclear Regulatory Commission August 1998
3. NUREG/CR-2815, “Probabilistic Safety Analysis Procedures Guide”, U.S. Nuclear Regulatory Commission, August 1985.
4. NUREG/CR-1150, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants”, U.S. Nuclear Regulatory Commission, May 1989.
5. NSAC-159, “Generic Framework for IPE Back-end (Level 2) Analysis”, Science Applications International Corporation, October 1991.
6. NUREG/CR-4832, Analysis of La Salle Unit 2 Nuclear Power Plant, Risk methods Integration and evaluation Program”, U.S. Nuclear Regulatory Commission, August 1992.
7. NUREG/CR-6143, “ Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, unit 1”, U.S. Nuclear Regulatory Commission, March 1995.

10.11 Korea

1. Chang-Ju Lee, et al., “Proposed Regulatory Guideline on the PSA Quality for Risk-informed Applications,” Proc. of Korean Nuclear Society Fall Meeting, Gyeongju, Oct. 2005.
2. American Society of Mechanical Engineers (ASME), “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” Standard ASME-RA-S-a-2003 Addenda to ASME RA-S-2002, 2003.
3. Chang-Ju Lee, "Development of Multi-purpose PSA Model for Regulatory Uses," Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (PSAM 8), New Orleans, USA, May 14-19, 2006.
4. Woo Sik Jung and et al., A fast BDD algorithm for large coherent fault trees analysis, Reliability Engineering & System Safety, Vol. 83, Issue 3, Pages 369-374, 2004.
5. J. E. Yang, et al., "An Analytic Method to Solve the Logical Loop between the Support Systems in the Fault Tree Model," Reliability Engineering and System Safety, Vol.56, No.2, 1997.
6. Woo Sik Jung and et al., Development of measures to estimate truncation error in fault tree analysis, Reliability Engineering and System Safety, Vol. 90, pp. 30–36, 2005.
7. Woo Sik Jung and et al., An Approach to estimate SBO Risks in Multi-unit Nuclear Power Plants with a Shared Alternate AC Power Source, Proceedings of the 7th International Conference on Probabilistic Safety Assessment and Management (PSAM 7), Berlin, Germany, June 14-18, 2004.

10.12 Japan

1. Special Committee on Safety Goals, Nuclear Safety Commission, Japan, “Interim Report on Research and Deliberations on Safety Goals,” (2003).
2. Special Committee on Safety Goals, Nuclear Safety Commission, Japan, “Performance Goals for Nuclear Power Plants Equivalent to the Interim Safety Goals,” (2006).
3. Nuclear Safety Commission, Japan, “Basic Policy on Introducing Nuclear Safety Regulations using Risk Information,” (2003)
4. Nuclear Safety Commission, Japan, “Revision of Examination Guide for Seismic Design of Nuclear Power Reactor Facilities,” (2003)
5. Nuclear Safety Commission, Japan, “Interim Report on Taskforce for Introduction of Risk Informed Regulation, Issues and Perspectives” (2005)
6. Nuclear and Industrial Safety Agency, Japan, “Basic Concept to Apply ‘Risk Information’ to Nuclear Safety Regulation,” (2005)
7. Nuclear and Industrial Safety Agency and Japan Nuclear Energy Safety Organization, Japan, “A Near-Term Implementation Plans of Risk-Informed-Regulation,” (2005)
8. Nuclear and Industrial Safety Agency, Japan, “High-Level Guidelines for Utilization of “Risk Information” in Safety Regulations for NPPs – Trial Use -,” (2006)
9. Nuclear and Industrial Safety Agency and Japan Nuclear Energy Safety Organization, Japan, “PSA Quality Guidelines for NPP Applications –Trial Use -,” (2006)
10. NUClear Information Archives, **http://www.nucia.jp/**

10.13 Italy

[1] Burgazzi, L. Passive System Reliability Analysis: a Study on the Isolation Condenser. Nuclear Technology, 139, 3-9, 2002

[2] Burgazzi, L. Reliability Evaluation of Passive Systems Through Functional Reliability Assessment. Nuclear Technology, 144, 145-151, 2003

[3] Burgazzi, L. Evaluation of Uncertainties Related to Passive Systems Performance. Nuclear Engineering and Design, 230, 93-106, 2004

[4] Marques, M., Burgazzi, L, et al. Methodology for the Reliability Evaluation of a Passive System and its Integration into a Probabilistic Safety Assessment. Nuclear Engineering and Design, 235, 2612-2631, 2005

[5] Burgazzi, L. Reliability of Passive Systems, Technical Note, NEA/SEN/SIN/WGRISK(2005)2, September 2005

[6] Burgazzi, L. Basics of Reliability Models in the Context of Ageing PSA. International Workshop on Practical Applications of Age-Dependent Reliability Models and Analysis of Operational Data, Fontenay aux Roses, France, October 5-6, 2005

10.14 Germany

[1] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU): Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes - Leitfaden Probabilistische Sicherheitsanalyse, 31. Januar 2005, Bekanntmachung vom 30. August 2005, Bundesanzeiger, Jahrgang 57, Nummer 207a, 3. November 2005

[2] Facharbeitskreis probabilistische Sicherheitsanalyse für Kernkraftwerke (FAK): Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand August 2005, BfS-SCHR-37/05, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Salzgitter, Oktober 2005

[3] Facharbeitskreis probabilistische Sicherheitsanalyse für Kernkraftwerke (FAK): Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand August 2005, BfS-SCHR-38/05, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Salzgitter, Oktober 2005

[4] Kreuser, A., J. Peschke: Coupling Model: A Common-Cause-Failure Model with Consideration of Interpretation Uncertainties, Nuclear Technology, Volume 136, No. 3, Dec 2001, pp. 255-260

10.15 Hungary

[1] Nuclear Safety Code Five Enclosures (Volumes) to the Governmental Decree No. 89/2005. (V.5) Korm.

[2] Procedures for Conducting PSA of NPPs IAEA Safety Series – Level 1: No. 50-P-4, 1992 – Level 2: No. 50-P-8, 1995

[3] Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2. IAEA-TECDOC-1229, July 2001

[4] Review Procedures and Criteria for Different Regulatory Applications to PSA NEA/CNRA/R(97)5, February 1998

[5] State of Living PSA and Further Development. NEA/CSNI/R(99)15, July 1999

[6] Results of COOPRA and WGRISK Surveys on Low Power and Shutdown PSA Joint NEA CSNI and COOPRA Report, under Publication, 2006

[7] Standard Review Plan for SAR of NPPs.19.1 Deterring the Adequacy of PRA Results for Risk-Informed Activities NUREG-0800, November 2002

[8] An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. NRC Regulatory Guide 1.147, July 1998

10.16 France

1. CSNI Fire PSA Workshop – Puerto Vallarta (Mexico) - June 2005
2. CSNI Severe Accidents and Level2 PSA – Koln (Germany) – March 2004
3. JRC/AEN workshop on Emergency and Risk Zoning – 26-27 April 2005
4. CSNI Uncertainties workshop – November 2005
5. IRSN/JRC Workshop – October 2005
6. PSA’05 Conference - San-Francisco (California) - 10-15 September 2005
7. PSAM8 Conference – New Orleans (USA) – 14-20 May 2006.

10.17 Finland

1. Regulatory Guide YVL. 2.8, Probabilistic Safety Analysis (PSA) in the Regulation and Safety Management of NPPs, Finnish Centre for Radiation and Nuclear Safety (STUK), Final draft, Helsinki 2003.
2. Julin A, Virolainen R, PSA Based Event Analysis of Incidents and Failures at TVO BWR, PSA`96- International Topical Meeting on PSA, Moving toward Risk-Based Regulation, Park City, Utah, September 29-October 3, 1996
3. Mononen J, Niemelä I, Virolainen R, Rantala R, Julin A, Valkeajärvi O, Hinttala J, " A Pilot Study On Risk Informed In-service Inspection", Proceedings of PSAM-5, November 28-December 1, 2000, Osaka, Japan
4. Reiman L, Expert Judgment in Analysis of Human and Organizational Behaviour at Nuclear Power Plants, (Doctor Thesis), STUK-A118, Finnish Centre for Radiation and Nuclear Safety, December 1994
5. Regulatory Guide YVL. 2.8, Probabilistic Safety Analysis (PSA) in the Licensing and Regulation of Nuclear Power Plants, Finnish Centre for Radiation and Nuclear Safety (STUK), Helsinki 1996.
6. Sandberg J, Virolainen R, Niemelä I, On the Regulatory Review of the TVOI/II, Low Power and Shutdown Risk Assessment, Proceedings of ESREL`96 - PSAM-III, June 24-28, 1996, Crete, Greece
7. Vaurio J, Jänkälä K, Safety Management of a VVER Plant by Risk Assessment, PSA`96-International Topical Meeting on PSA, Moving toward Risk-Based Regulation, Park City, Utah, September 29-October 3, 1996
8. European Commission, "Report on Risk-Informed In-Service Inspection and In-Service Testing", NRWG, EUR 19153, June 1999
9. NUREG-1602, "Use of PSA in Risk Informed Applications". US NRC, 1998
10. ASME Code Case N-560 "Alternative Examination Requirements for Class 1", 1996
11. ASME Code Case N-577 "Risk-Informed Requirements for Class 1, 2 and 3 Piping , Method A, 1997
12. ASME Code Case N-578, "Risk-Informed Requirements for Class 1, 2 and 3 Piping , Method B, 1997
13. J.Mononen, A.Julin, et al., "A Pilot Study on Risk Informed In-Service Inspection", PSA'99, August 1999
14. S.R.Gosselin, "EPRI's new inservice inspection programme" Nuclear News, November 1997
15. NRC Regulatory Guide 1.178 " An Approach For Plant-Specific Risk-informed Decisionmaking Inservice Inspection of Piping", July 1998
16. K. Simola, U.Pulkkinen, "Expert Panel Approach to Support RI-ISI evaluation", December 1999
17. K.Simola, U.Pulkkinen, et al., "Expert Panel Approach for Supporting RI-ISI Evaluation", PSAM5, November 2000

10.18 Czech Republic

1. INSAG Series No. 12: Basic Safety Principles for Nuclear Power Plants - 75-INSAG-3 Rev. 1, 1999, Vienna, Austria

2. Patrík M.: Living PSA a Support Framework for Risk Based Decision Making; PSAM5, Osaka, November 2000, Proceedings of the 5th International Conference on Probabilistic Safety Assessment and Management

3. Mlady O. : NPP Temelin Safety Analysis Report and PSA Status, Proceedings of the Internationalconference on the Strengthening of Nuclear Safety in Eastern Europe, June 1999, Vienna, Austria

4. NUREG/CR-2300, PRA Procedures Guide: A Guide to the Performance of PRA for NPP, USNRC, 1983

5. Safety Series 50-P-4, Procedures for Conducting PSA of NPPs - Level 1, IAEA, Austria, July 1992

6. Safety Series 50-P-8, Procedures for Conducting PSA of NPPs - Level 2, IAEA, Austria, May 1995

7. IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA), IAEA, Vienna, Austria, August 1999

8. Code of Federal Regulations, 10 CFR 50, Appendix B, USNRC, 1994

9. IAEA TECDOC-719, Defining Initiating Events for PSA for WWER Reactors, IAEA, Austria, September 1993

10. IAEA TM on Comparison of PSAs Level for WWER 1000 Reactors, Erlangen, Germany, 7.-11. June 1999, RER/9/046

11. WWER-SC-195, Harmonization of WWER PSA Model Assumptions and Data, IAEA/DOE Workshop, November 1996, UJV Rez, Czech Republic

12. International Workshop on Safety of VVER-1000 Nuclear Power Plants, April 7-12, 2003, in Piestany, Slovakia

13. NUREG/CR-5750, Rates of Initiating Events at U.S. NPPs: 1987 - 1995, USNRC, February 1999

14. NUREG/CR-2728, Interim Reliability Evaluation Program Procedures Guide (IREP), USNRC, January 1983

15. NUREG/CR-4550, Analysis of Core Damage Frequency: Internal Events Methodology, Vol.1, Rev.1, Sandia National Laboratory, January 1990

16. Reliability Assessment of Specific Components of WWER Plants, Rev. 1, Enconet Consulting, Austria, April 1995

17. IAEA-TECDOC-749, Generic Initiating Events for PSA for WWER Reactors, IAEA, June 1994

18. 27 RKS 85-25, Reliability Data Book for Components in Swedish Nuclear power Plants, RKS, SKI, Sweden

19. Holý J.: Some General Insights Regarding Development of NPP Dukovany PSA Input Data Set Made on the Base of Broad Analysis of Operational Experience; 8th Conference on PSAM, New Orleans, U.S.A., May 2006

20. Holý J.: Some Insights from HRA Related to Low Power and Shutdown Scenarios ; International Conference on Probabilistic Safety Assessment and Management – PSAM7, ESREL´04, Berlin, June 2004

21. Husťák S., Patrík M.: The Use of PSA for Development and Evaluation of NPP Dukovany Symptom-Oriented EOPs; International Conference on Probabilistic Safety Assessment and Management - PSAM 7, ESREL´04, Berlin, June 2004

22. Husťák S.: The NRI Approach for Technical Specifications Evaluation; 8th Conference on PSAM, New Orleans, U.S.A., May 2006

23. Sedlák J.: The Time Consideration in Risk Informed Tools ; International Conference on Probabilistic Safety Assessment and Management – PSAM7, ESREL´04, Berlin, June 2004

24. J. Dienstbier: WP 5.2 Treating of Uncertainties in Level 2 PSA for the VVER 440/213 Dukovany. SARNET PSA 2 meeting Fontenay-aux-Roses, November 23-24, 2004

25. Bareith, J. Dienstbier (presented), G. Lajtha: Comparison of Level 2 PSAs for two VVER-440/213 plants – Paks – Dukovany. SARNET PSA-2 meeting, Varna, Bulgaria, June 28-29, 2005.

10.19 Canada

1. http://laws.justice.gc.ca/en/n-28.3/252272.html
2. http://www.nuclearsafety.gc.ca/eng/regulatory_information/documents/current_docs.cfm
3. P. Hessel, “Regulatory review of a PSA – Benefits of building a replica”, paper presented at PSAM 7 – ESREL 04, Berlin, Germany, June 14-18, 2004
4. “Safety of Nuclear Power Plants: Design”, Safety Standards Series No. NS-R-1, Vienna 2000
5. http://www2s.biglobe.ne.jp/~INSC/INSCAP/Risk.html
6. A. J. Szukiewicz, “Implementing Agreement Between the USNRC and CNSC in the Area of Probabilistc Risk Assessment Research”, CNSC file no. 11-2-5, April 14, 2004

10.20 Belgium

[1] “Development of Guidelines for PSA-Based Event Analysis (PSAEA) in an International Project”; M. Hulsmans et al., OECD Workshop on Precursor Analysis, Brussels, March 28-30, 2001

[2] “Comparison of the level 1 PSA for two similar PWR types: the French 900 MWe series PWR and the Belgian Tihange 1 PWR”; P. Dupuy et al., Proceedings PSAM5, Osaka, Nov. 27- Dec. 1, 2000

[3] “Towards a PSA harmonization: French-Belgian Comparison of the level 1 PSA for two similar PWR types”; P. Dupuy et al., Proceedings PSAM6, San Juan, Puerto Rico, USA, June 23-28, 2002; page 2003

[4] “Regulatory Use of PSA in Belgium – Status, Lessons Learned and Perspectives”; M. Hulsmans et al., Proceedings PSAM7-ESREL’04, Berlin (D), June 14-18, 2004; page 701

[5] “Risk-based precursor analysis in the nuclear industry – experiences on the national and the international scene”; M. Hulsmans, Presented at PSAM8, New Orleans, USA, May 15-19, 2006.

[6] “Improving quality of NPP PSA by international comparisons”; F. Corenwinder et al; Presented at PSAM8, New Orleans, USA, May 15-19, 2006.

Appendix A – Overview of the Status of PSA programmes

US

Since the completion of the Individual Plant Examination (IPE) and Individual Plant Examination of External Events (IPEEE) programs in the 1990's, U.S. licensees have continued to update their PSAs to reflect plant changes (many of which involved improvements identified by the IPEs and IPEEEs) and current operational experience. In addition, the NRC has developed Standardized Plant Analysis Risk (SPAR) models for each plant and is in the process of benchmarking these models against licensee PSAs. A discussion on the objectives, PSA level, initiating events addressed, modes of operation addressed, and updating process for the various PSAs is provided in Chapter 5 of this report.

UK

Plant name	Plant type	PSA Scope				PSA usage		
		Level	Initiating events	Plant Operating States	Living PSA	Date of original PSA/ revisions	Reason or PSA	PSA applications
Calder Hall	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1991 Rev: 1998	See note [1]	See note [2]
Chapelcross	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1990 Rev: 1998	See note [1]	See note [2]
Bradwell	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1986 Rev: 1992	See note [1]	See note [2]
Hinkley Point A	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1987 Rev: 1994	See note [1]	See note [2]
Dungeness A	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1992 Rev: 1995	See note [1]	See note [2]
Hunterston A	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1988 Rev: 1994	See note [1]	See note [2]
Sizewell A	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	Plant now shutdown	Prod: 1988 Rev: 1994	See note [1]	See note [2]
Oldbury	Magnox	Level 1+ PSA - see note [3]	All internal events	At power only	No	Prod: 1990 LTSR: 1997	See note [1]	See note [2]
Wylfa	Magnox	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	No	Prod: 1998 PSR: 2006	See note [1]	See note [2]
Hinkley Point B	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1995 PSR2: 2006		
Hunterston B	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1995 PSR2: 2006		
Dungeness B	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1996 PSR2: 2007		

Plant name	Plant type	PSA Scope				PSA usage		
		Level	Initiating events	Plant Operating States	Living PSA	Date of original PSA/ revisions	Reason or PSA	PSA applications
Hartlepool	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1997 PSR2: 2007		
Heysham 1	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1997 PSR2: 2007		
Heysham 2	AGR	Level 1+ PSA - see note [3]	All internal events and limited treatment of hazards	At power only	Yes	Prod: 1986 (L1 PSA) Rev: 1998 (L2 PSA) Rev: 2002 (LPSA) PSR2: 2009		Design evaluation. Risk Monitor. Risk Informed Tech Specs.
Torness	AGR	Level 1+ PSA - see note [3]	Internal events and limited treatment of hazards	At power only	Yes	Prod: 1986 (L1 PSA) Rev: 1999 (L2 PSA) Rev: 2002 (LPSA) PSR2: 2009		Design evaluation. Risk Monitor. Risk Informed Tech Specs
Sizewell B	PWR	Level 3	Internal events Internal and external hazards	All plant states including power operation, low power, shutdown, refuelling	Yes	Prod: 1992 Rev: 1997 (LPSA) PSR: 2007		Design evaluation. Risk Informed Tech Specs, Proposed Risk Monitor

[1] The PSAs for the Magnox reactors were produced for the Long Term Safety Reviews to allow operation beyond 30 years. The have been updated as part of the 10 yearly Periodic Safety Review

[2] Design evaluation only.

[3] The PSA that has been carried out for the gas cooled reactors is a Level 1 PSA plus a calculation of the doses from the fault sequences identified. For the sequences that give rise to the larger releases, these fault sequences are assigned to the >1000mSv dose band without detailed modelling being carried out for the severe accident sequences so that the analysis falls short of what would be expected for a full Level 2 PSA.

Taiwan

Appendix A – Overview of the Status of PSA Programs

Plant	Type	PSA Type	Original PSA Date Completed	Revised PSA Date Completed
Chinshan	BWR 4	Level 1 + LERF	Level 1 – 1991 LERF – 2001	Expected 2007
Kuoshan	BWR 6	Level 1 + LERF	Level 1 – 1985 LERF – 2001	Expected 2007
Maanshan	PWR	Level 1 + LERF	Level 1 – 1987 LERF – 2001	Expected 2007
Lungmen	ABWR	Level 1 + LERF	Expected 2007	-

Switzerland

Plant Name	**Plant type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Beznau (units 1 & 2)	PWR Westinghouse 2 Loop PWR	Level 1 & 2 full power Level 1 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A procedure for updating the PSA has been defined	1993 (full power level 1 & 2) 1998 shutdown Revisions: Living PSA	Regulatory requirement; risk informed regulation	Design review Risk-informed regulation (see Section 7)
Gösgen	PWR Siemens-KWU 3 Loop PWR	Level 1 & 2 full power Level 1 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A procedure for updating the PSA has been defined	1994 (full power level 1 & 2) 1994 shutdown	Regulatory requirement; risk informed regulation	Design review Risk-informed regulation (see Section 7)
Leibstadt	BWR GE BWR/6, Mark-III	Level 1 & 2 full power Level 1 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A procedure for updating the PSA has been defined	1994 (full power level 1 & 2) 2001 shutdown	Regulatory requirement; risk informed regulation	Design review Risk-informed regulation (see Section 7)

Plant Name	**Plant type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Mühleberg	BWR GE BWR/4, Mark-I	Level 1 & 2 full power Level 1 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A procedure for updating the PSA has been defined	1993 (full power level 1 & 2) 1997 shutdown	Regulatory requirement; risk informed regulation	Design review Risk-informed regulation (see Section 7)

Sweden

The aim of the appendix is to give an overview of the PSA:s that have been carried out in the member countries and this information will be presented in a tabular form similar to that in the 2002 Report using the headings given below. Authors should provide the following information for all the power reactors in their country:

Plant name:	(for all the reactors in your country). Plant type: (for all the reactors in your country).
PSA scope:	Level of PSA carried out (Level 1, 2 or 3).
	Scope of initiating events included in the PSA (internal events, internal hazards, external hazards).
	Plant Operating States included in the PSA (power operation, low power, shutdown, refuelling, etc.).
	Whether the PSA is maintained as a Living PSA.
PSA usage:	Date of the original PSA and any subsequent revisions.
	Reason for carrying out the PSA/ stage in the plant life that the PSA was carried out.
	Applications that the PSA has been used for.

Status of PSA activities in Sweden by february 2006										
	Oskarshamn			**Forsmark**			**Ringhals**			
	Unit 1	**Unit 2**	**Unit 3**	**Unit 1**	**Unit 2**	**Unit 3**	**Unit 1**	**Unit 2**	**Unit 3**	**Unit 4**
Level 1										
Power operation	2005	2004	2004	2000	2000	1998	2000	2005	2005	2005
Shutdown, - restart	2005	Pl 2007	2004	1993	1993	Pl 2006	Pl 2006	2005	2005	2005
Refueling	2005	Pl 2007	2003	1999	1999	1995	Pl 2006	2001	2005	2005
Level 2										
Power operation	2005	Pl 2007	Pl 2006	2001	2001	1998	1996	2005	2005	2005
Shutdown, - restart	2005	Pl 2007	Pl 2006	2001	2001	Pl 2006	Pl 2006	2004	2005	2005
Refueling	2005	Pl 2007	Pl 2006	Pl 2006	Pl 2006	Pl 2006	Pl 2006	1996	2005	2005
Legend:										
Pl = Planned										
Remark: Under each subtitel following kinds of analysis are completed or goal for update										
- LOCA / Transienter / CCIer										
- Fire										
- Flooding										
- Heavy lifts										
- External Events										

Spain

Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original [1] PSA/ revisions[2]**	**Reason for carrying out PSA**	**PSA applications**
Santa María de Garoña	BWR GE Mark I	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states	Yes - updated every fuel cycle and every 10 years PSR	Original: 1985 Latest revision: 2005	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor
Almaraz	PWR W 3 loop	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states (under review)	Yes - updated every fuel cycle and 10 years for PSR	Original: 1989 Latest revision: July 2005	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor
Ascó	PWR W 3 loop	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states	Yes - updated every 10 years for PSR	Original: 1992 Latest revision: 2001	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor
Cofrentes	BWR GE Mark III	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states (under review)	Yes - updated every fuel cycle and every 10 years for PSR	Original: 1991 Latest revision: 2005	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor

Plant Name	**Plant type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original [1] PSA/ revisions[2]**	**Reason for carrying out PSA**	**PSA applications**
Vandellos-2	PWR W 3 loop	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states	Yes - updated every 10 years for PSR	Original: 1994 Latest revision: 2002	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor
Trillo	PWR Siemens 3 loop	Full Level 2 PSA	All internal events All internal hazards (no yet fires) All external hazards	All plant operating states (under review)	Yes - updated every fuel cycle and every 10 years for PSR	Original: 1998 Latest revision: 2005	Carried out by require-ment	Design review Risk informed Tech Specs
Jose Cabrera (removed from commercial operation in April 2006)	PWR W 1 loop	Full Level 2 PSA	All internal events All internal hazards All external hazards	All plant operating states	Yes - updated every 10 years for PSR	Original: 1993 Latest revision: 2005	Carried out by require-ment	Design review Risk informed Tech Specs Risk Monitor

Notes:

1. “Original PSA date” is the first version of the PSA and the date of the first submission (partial scope) to the CSN.
2. “Revision” is the currently latest version of the PSA and its date of submission to the CSN.

Slovenia

Appendix A: Overview of the Status of PSA Programms								
Plant **Name**	Plant **type**	Scope of the PSA carried out				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Krško	2 loop PWR Westinghouse	Level 1 & 2 full power Level 1 for shutdown	Full scope All internal and external events	Full power and shutdown	Yes updated every 2 years	Original: 1992 Revised: Living PSA	Regulatory requirements	Design review, Risk Monitor, PSA based event analysis, OLM, IS VVA

Slovak Republic

Appendix A: Overview of the Status of PSA Programms

Plant **Name**	Plant **type**	Scope of the PSA carried out				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Bohunice V1	(VVER-440/V230)	Level 1 and 2	Full scope All internal and external events	Full power and shutdown	Yes	Original: 1995; Set of revisions; Shutdown in 2006 -unit 1, and 2008 - unit 2	Regulatory requirements, initiated by utility	Risk Monitor, Safety assessment and upgrading
Bohunice V2	(VVER-440/V213)	Level 1 and 2	Full scope All internal and external events	Full power and shutdown	Yes	Original: 1994; Set of revisions; Next scheduled revision: August 2007 (PSR)	Regulatory requirements, initiated by utility	Risk Monitor, Safety assessment and upgrading
Mochovce	(VVER-440/V213)	Level 1	Full scope All internal and external events	Full power and shutdown	Yes	Original: Living PSA 2006	Regulatory requirements, initiated by utility	Safety Monitor, Safety assessment and upgrading

Plant/Unit	PSA Type	CDF for full power operation	CDF for shutdown modes
V1/unit 1	level 1 and 2	2.09E-5/y	5.43E-5/y
V1/unit 2	level 1	2.28E-5/y	6.55E-5/y
V2/unit 3	level 1 and 2	2.36E-5/y	8.59E-6/y
Mochovce/unit1	level 1	3.67E-6/y	8.93E-6/y

The Netherlands

Plant Name	Plant Type	Scope of the PSA carried out				PSA usage		
		Level of PSA	**Initiating Events**	**Plant Operating States**	**Living PSA**	**Date of Original PSA/ revisions**	**Reason for Carrying out PSA**	**PSA Applications**
Borssele	PWR	Full scope level 3	Internal Events Area events /hazards External Events	All plant operating States (at power, Low power and 5 shutdown refuelling states	Yes + Risk Monitor	Original 1990-1994 model update 2004	Original: Identification of weak points; support of first 10-yearly periodic safety review and associated modifications Currently support of daily Operation and Risk-informed decision-making	Risk Informed Tech specs Risk Monitor Change of testing strategy Development of SAMGs Outage planning Emergency planning & preparedness (source terms)
Dodewaard	BWR	Full scope level 3	Internal Events Area events /hazards External Events	All plant operating States (at power, Low power and 5 shutdown refuelling states	No	1991-1994	Original: Identification of weak points; support of first 10-yearly periodic safety review and associated modifications	Design review
High Flux Reactor (HFR)	Research Reactor 45 MW_t	Level 3	Internal events Area events/ hazards	Power states	no	2002-2004	10-yearly periodic safety review	Design review/ Support of backfitting

Mexico

Plant Name	Plant Type	Level of PSA	Initiating events	Plant Operating States	Living PSA	Date of Original PSA/revision	Reason for carrying out PSA	PSA Applications
Laguna Verde	BWR/5, Mark II	Level 1and 2	Internal Events including internal flooding	Full power	Yes – updated almost every refueling	Original January 1996. Revised and approved February, 2000	To develop an overall appreciation of severe accident behavior; understand the most likely severe accident sequences that could happen at Laguna Verde NPP; to gain a quantitative understanding of the overall probability of core damage and radioactive material release; and to reduce the overall probability of core damage and radioactive release by modifying procedures and hardware to prevent or mitigate severe accidents.	Risk-informed tech Specs; Risk-informed plant modification;
Laguna Verde	BWR/5, Mark II	Level 1	Internal Events	Low power and Shutdown (Plant operating states before refueling)		Expected in mid 2007.	To develop an overall appreciation of dominant risk contributors in such operating conditions	

Korea

Plant Name	Type	Scope of the PSA carried out			PSA usage		
		Level of PSA	Initiating events	Plant Operating States	Date of Original PSA/revisions	Reason for carrying out PSA	PSA applications
Kori-1	PWR	Level 1 + 2	All internal/some external events	At power	Nov. 2002	Countermeasure against severe accidents	Design review, Risk monitor
Kori-2	PWR	Level 1 + 2	ditto	At power	Dec. 2003	Countermeasure against severe accidents	Design review, Risk monitor
Kori-3,4	PWR	Level 1 + 2	ditto	At power	Aug. 1992/ Jun. 2003	Countermeasure against TMI accident/ Severe Accident Policy	Design review, Risk monitor
Yonggwang 1,2	PWR	Level 1 + 2	ditto	At power	Aug. 1992/ Dec. 2003	Countermeasure against TMI accident/ Severe Accident Policy	Design review, Risk monitor
Yonggwang 3,4	PWR	Level 1 + 2	ditto	At power	Feb. 1994/ Dec. 2004	Construction permission/ Severe Accident Policy	Design review, Risk monitor
Ulchin 1,2	PWR	Level 1 + 2	ditto	At power	Dec. 2005	Severe Accident Policy	Design review
Ulchin 3,4	PWR	Level 1 + 2	ditto	At power	Oct. 1997/ Dec. 2004	Construction permission/ Severe Accident Policy	Design review, Risk monitor
Yonggwang 5,6	PWR	Level 1 + 2	ditto	At power & shutdown	Dec. 2000/ Dec. 2005	Construction permission/ Severe Accident Policy	Design review, Risk monitor
Ulchin 5,6	PWR	Level 1 + 2	ditto	At power	Jun. 2002	Construction permission	Design review, Risk monitor
Shin-Kori 1,2	PWR	Level 1 + 2	ditto	At power & shutdown	PSA is now in progress	Initial design and licensing	Design review
Shin-Kori 3,4	PWR	Level 1 + 2 + 3	ditto	At power & shutdown	PSA is now in progress	Initial design and licensing	Design review
Wolsong 1	PHWR	Level 1 + 2	ditto	At power	Dec. 2003	Countermeasure against severe accidents	Design review, Risk monitor
Wolsong 2,3,4	PHWR	Level 1 + 2	ditto	At power	Jun. 1997	Construction permission	Design review, Risk monitor

Japan

Table: Status of PSA Programs in Japan

Organization Name	Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
			Level of PSA	Initiating events	Plant Operating States	Living PSA	Date of Original PSA/revisions	Reason for carrying out PSA	PSA applications
JNES	Japanese typical 500MWe-class BWR	BWR-３	Level １	Internal event	At power	No	Original：1992 Revised：2000	• Review of accident managements(AM) of utilities	• Evaluate effectiveness of AM measures • Accident sequence precursor(ASP) Analysis
					At shutdown	No	Original：1999	• Review of shutdown PSA of utilities in PSR	• Confirm safety level in shutdown operation • ASP Analysis
			Level ２	Internal event	At power	No	Original：1998 Revised：2000	• Review of AM of utilities	• Evaluate effectiveness of AM measures
			Level ３	Internal event	At power	No	Original：2004	• Confirmation of safety level	•

JNES	Japanese typical 800MWe-class BWR	BWR-４	Level １	Internal event	At power	No	Original：1988 Revised：1999	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis
					At shutdown	No	Original：1998 Revised：2001	・Review of shutdown PSA of utilities in PSR	・Confirm safety level in shutdown operation ・ASP Analysis
				Seismic event	At power	No	Original：2001	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
					At shutdown	No	Original：2003	・Confirmation of safety level	・Evaluate residual risk at earthquake
			Level ２	Internal event	At power	No	Original：1998	・Review of AM of utilities	・Evaluate effectiveness of AM measures
					At shutdown	No	Original： 2006	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2003	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
			Level ３	Internal event	At power	No	Original：2004	・Confirmation of safety level	・
					At shutdown	No	Original：2006	・Confirmation of safety level	・Confirm the needs of AM at shutdown operation
				Seismic event	At power	No	Original：2005	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake

	Japanese typical 1100MWe-class BWR	BWR- 5	Level 1	Internal event	At power	No	Original：1985 Revised：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis ・Evaluate appropriateness of AOT ・Evaluate appropriateness of inspection
					At shutdown	No	Original：1997 Revised：2001、2002	・Review of shutdown PSA of utilities in PSR	・Confirm safety level in shutdown operation ・ASP Analysis
				Seismic event	At power	No	Original: 1994	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
				Fire event	At power	No	Original：2001 Revised：2004	・Confirmation of safety level at fire	・
			Level 2	Internal event	At power	No	Original：1998 Revised：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures
					At shutdown	No	Original：2004	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2001	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake

			Level 3	Internal event	At power	No	Original：2003	・Confirmation of safety level	・
					At shutdown	No	Original：2005	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2005	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
	Japanese typical 1300MWe-class BWR	ABWR	Level 1	Internal event	At power	No	Original：1988 Revised：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis
				Seismic event	At power	No	Original：2005	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
			Level 2	Internal event	At power	No	Original：1998	・Review of AM of utilities	・Evaluate effectiveness of AM measures
			Level 3	Internal event	At power	No	Original：2004	・Confirmation of safety level	・
	Japanese typical 500MWe-class PWR	2 loop PWR with dry-type CV	Level 1	Internal event	At power	No	Original：1996 Revised：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis
					At shutdown	No	Original：1998 Revised：2001	・Review of shutdown PSA of utilities in PSR	・Confirm safety level in shutdown operation ・ASP Analysis

				Seismic event	At power	No	Original：2002	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
				Fire event	At power	No	Original：2002	・Confirmation of safety level at fire	・
			Level 2	Internal event	At power	No	Original：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures
					At shutdown	No	Original：2005	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2004	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
			Level 3	Internal event	At power	No	Original：2004	・Confirmation of safety level	・
				Seismic event	At power	No	Original：2004	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
	Japanese typical 800MWe - class PWR	3 loop PWR with dry-type CV	Level 1	Internal event	At power	No	Original：1995 Revised：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis
					At shutdown	No	Original：1991 Revised：2001、2002	・Review of shutdown PSA of utilities in PSR	・Confirm safety level in shutdown operation ・ASP Analysis
				Seismic event	At power	No	Original：2006	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake

			Level 2	Internal event	At power	No	Original : 1999	・Review of AM of utilities	・Evaluate effectiveness of AM measures
			Level 3	Internal event	At power	No	Original : 2004	・Confirmation of safety level	・
	Japanese typical 1100MWe-class PWR with dry-type CV	4loop PWR with dry-type CV	Level 1	Internal event	At power	No	Original : 1992 Revised : 2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis ・Evaluate appropriateness of AOT ・Evaluate appropriateness of inspection
					At shutdown	No	Original : 1995 Revised : 2001	・Review of shutdown PSA of utilities in PSR	・Confirm safety level in shutdown operation ・ASP Analysis
				Fire event	At power	No	Original : 2001 Revised : 2005	・Confirmation of safety level	・
					At shutdown	No	Original : 2001	・Confirmation of safety level	・
				Flooding event	At power	No	Original : 2003	・Confirm safety level of flooding event	・
				Seismic event	At power	No	Original : 2001	・Preparation of seismic PSA review of utilities	・Evaluate residual risk at earthquake
					At shutdown	No	Original : 2004	・Confirmation of safety level	・Evaluate residual risk at earthquake

			Level2	Internal event	At power	No	Original：1999	・Review of AM of utilities	・Evaluate effectiveness of AM measures
					At shutdown	No	Original：2001	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2003	・Preparation of seismic PSA review of utilities	・Evaluate residual risk
			Level3	Internal event	At power	No	Original：2003	・Confirmation of safety level	・
					At shutdown	No	Original：2004	・Confirmation of safety level	・Evaluate necessity of AM measures
				Seismic event	At power	No	Original：2005	・Preparation of seismic PSA review of utilities	・Evaluate residual risk
	Japanese typical 1100MWe-class PWR with ICE condenser type containment vessel (CV)	4 Loop PWR with ICE-condenser type CV	Level 1	Internal event	At power	No	Original：2000	・Review of AM of utilities	・Evaluate effectiveness of AM measures ・ASP Analysis
			Level 2	Internal event	At power	No	Original：1999	・Review of AM of utilities	・Evaluate effectiveness of AM measures
			Level 3	Internal event	At power	No	Original：2004	・Confirmation of safety level	・
JNES	Typical BWR	Typical plant	Level 1	Seismic event	At power	No	Original：2004	・Pilot study for seismic risk	・Evaluate residual risk
		BWR-3/4/5 ABWR	Level 1	Internal event	At power	No	Original：2005 ～2006	・Evaluate safety level for strainer blockage	・Evaluate safety level for strainer blockage
		BWR5	Level 3	Internal event	At power	No	Original：2005	・Pilot study for internal risk	・Contribute to performance goals

		ABWR	Level 3	Internal event	At power	No	Original：2005	• Pilot study for internal risk	• Contribute to performance goals
	Typical PWR	Typical plant	Level 1	Seismic event	At power	No	Original：2004	• Pilot study for seismic risk	• Evaluate residual risk
		4LoopPWR	Level 3	Internal event	At power	No	Original：2005	• Pilot study for internal risk	• Contribute to performance goals
JNES	Toukai 2	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
	Tsuruga 1	BWR-2	Level 1	Internal event	At power	No	Original：1994 Revised：2002	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures

	Tsuruga 2	4Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・ ・ ・PSR
					At shutdown	No	Original：2006	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・ ・ ・PSR
JNES	Onagawa 1	BWR- 4	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：1999	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Onagawa 2	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
	Onagawa 3	BWR-5	Level 1	Internal event	At power	No	Original：1995 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：1995 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
	Higashidoori 1	BWR-5	Level 1	Internal event	At power	No	Original：2003	• Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：2003	• Evaluate effectiveness of AM measures	• AM measures
JNES	Fukushima 1 Unit -1	BWR-3	Level 1	Internal event	At power	No	Original：1994 Revised：2002	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures

	Fukushima 1 Unit -2	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2001	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures ・
	Fukushima 1 Unit -3	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2006	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness ・of AM measures	・AM measures
	Fukushima 1 Unit -4,5	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures ・
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Fukushima 1 Unit -6	BWR-5 5	Level 1	Internal event	At power	No	Original：1994 Revised：1999	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：1999	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Fukushima 2 Unit -1	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Fukushima 2 Unit -2	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2001	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Fukushima 2 Unit -3,4	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2002	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Kashiwazaki 1	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2002	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Kashiwazaki 2, 3, 4, 5	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2006	・PSR	・PSR

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Kashiwazaki 6,7	ABWR	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
JNES	Hamaoka 1	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures ・
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Hamaoka 2	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Hamaoka 3	BWR- 5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2002	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Hamaoka 4	BWR- 5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Hamaoka 5	ABWR	Level 1	Internal event	At power	No	Original：2003	・Extract AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：2003	・Evaluate effectiveness of AM measures	・AM measures ・
JNES	Shiga 1	BWR- 5	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2005	・PSR	・PSR

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
	Shiga 2	ABWR	Level 1	Internal event	At power	No	Original：2003	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
			Level 1.5	Internal event	At power	No	Original：2003	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
JNES	Shimane 1	BWR-4	Level 1	Internal event	At power	No	Original：1994 Revised：2003	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
					At shutdown	No	Original：2003	• PSR	• PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2003	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
	Shimane 2	BWR-5	Level 1	Internal event	At power	No	Original：1994 Revised：2002	• Extract AM measures • Evaluate effectiveness of AM measures	• AM measures
					At shutdown	No	Original：2002	• PSR	• PSR

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
JNES	Tomari 1	2LoopPWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・Evaluate effectiveness of AM measures ・PSR
					At shutdown	No	Original：2006	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・ PSR	・AM measures ・Evaluate effectiveness of AM measures ・PSR
	Tomari 2	２Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate ffectiveness of AM measures ・PSR	・AM measures ・Evaluate effectiveness of AM measures ・PSR
					At shutdown	No	Original：2006	・PSR	・PSR

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・Evaluate effectiveness of AM measures ・PSR
JNES	Mihama 1	2 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Mihama 2	2 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2001	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Mihama 3	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2000 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures
					At shutdown	No	Original：2006	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2000 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures
	Takahama 1	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：1997 Revised：2003	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2003	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：1997 Revised：2003	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

	Takahama 2	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：1997 Revised：2003	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2003	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：1997 Revised：2003	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Takahama 3	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2001	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Takahama 4	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2001	・PSR	・PSR

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Ohi 1	４Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2000 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2000 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Ohi ２	４Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2000 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2000 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Ohi ３	４Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Ohi ４	４Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2002	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
JNES	Ikata 1	２Loop PWR	Level 1	Internal event	At power	Ｎｏ	Original：1994 Revised：1998 Revised：2004	・Extract AM measures ・PSR ・Evaluate effectiveness of AM measures	・AM measures ・PSR ・Evaluate effectiveness of M measures
			Level 1.5	Internal event	At power	Ｎｏ	Original：1994 Revised：1998 Revised：2004	・Extract AM measures ・PSR ・Evaluate effectiveness of AM measures	・AM measures ・PSR ・Evaluate effectiveness of AM measures
	Ikata 2	Dry-type ２Loop PWR	Level 1	Internal event	At power	Ｎｏ	Original：1994 Revised：2001	・Extract AM measures ・PSR ・Evaluate effectiveness of AM measures	・AM measures ・PSR ・Evaluate effectiveness of AM measures

					At shutdown	No	Original：2001	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2001	・Extract AM measures ・PSR ・Evaluate effectiveness of AM measures	・AM measures ・PSR ・Evaluate effectiveness of AM measures
	Ikata 3	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures ・Evaluate effectiveness of AM measures
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures ・Evaluate effectiveness of AM measures
JNES	Genkai 1	2 Loop PWR	Level 1	Internal event	At power	No	Original: 1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2003	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Genkai 2	2 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Genkai 3	4 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・PSR
					At shutdown	No	Original：2006	・PSR	・
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・PSR
	Genkai 4	4 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・PSR
					At shutdown	No	Original：2006	・PSR	・

			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004 Revised：2006	・Extract AM measures ・Evaluate effectiveness of AM measures ・PSR	・AM measures ・PSR
	Sendai 1	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・	・AM measures
					At shutdown	No	Original：2002	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
	Sendai 2	3 Loop PWR	Level 1	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures
					At shutdown	No	Original：2002	・PSR	・PSR
			Level 1.5	Internal event	At power	No	Original：1994 Revised：2004	・Extract AM measures ・Evaluate effectiveness of AM measures	・AM measures

Hungary

Overview of the PSA Programmes in Hungary								
Plant Name	**Plant type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Paks, unit 3	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1994 Revision: annually	AGNES project and regulatory requirements	*
Paks, units 1 and 2	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1995 Revision: annually	Periodic safety review	*
Paks NPP, unit 2	VVER-440/213	Level 1	Internal events	Low power and shutdown states of a refuelling outage	Yes	Original: 1997 Revision: annually	Regulatory requirements	*
Paks, unit 4	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1998 Revision: annually	Periodic safety review	*
Paks, unit 1	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 1999 Revision: annually	Regulatory requirements	*

Paks, unit 2	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 2001 Revision: annually	Regulatory requirements	*
Paks, units 3 and 4	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 2002 Revision: annually	Regulatory requirements	*
Paks, unit 3	VVER-440/213	Level 1	Seismic events	Full power	Yes	Original: 2002 Revision: annually	Regulatory requirements	*
Paks, unit 1, spent fuel storage pool	VVER-440/213	Level 1	Internal events, internal fires and internal flooding	All planned plant operational states	Yes	Original: 2002 Revision: annually	Regulatory requirements, support to level 2 PSA	*
Paks, unit 1, reactor and spent fuel storage pool	VVER-440/213	Level 2	Internal events, internal fires and internal flooding	Full power, Low power and shutdown states of a refuelling outage for reactor, all planned plant operational states for spent fuel storage pool	No	Original: 2003 Revision: none	Regulatory requirements	*

France

Plant **Name**	Plant **type**	Scope of the PSA carried out				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Standardized 900 MW plant	PWR	Level 1 Level 2	Internal events + Fire (only for IRSN Level 1)	All plant operating states	Yes - updated for 10 yearly PSR	Original: 1990 (level 1) Revised: 2004	No regulatory requirement Safety Assessment	Design review PSR PSA based event analysis Review of Tech Specs
Standardized 1300 MW plant Paluel 3	PWR	Level 1	Internal events	All plant operating states	Yes - updated for 10 yearly PSR	Original: 1990 Revised: 2005	No regulatory requirement Safety Assessment	Design review PSR PSA based event analysis Review of Tech Specs
Standardized N4	PWR	Level 1	Internal events	All plant operating states	Yes – updated for 10 yearly PSR	Original: 2001 Revised 2005	Carried out as part of the initial design and licensing	Design review PSR PSA based event analysis Review of Tech Specs
EPR	PWR	Level 1+	Internal events	All plant operating states	Design PSA	Original: 2001 Revised: 2006	Carried out as part of the initial design and licensing	Design review AOT and IST

Finland

Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Loviisa 1/2	WWER 440/213	Level 1and 2	Level 1 power: Internal, fires, flood, seismic, harsh weather conditions (+oil), Level 1 shutdown: Internal, flood, harsh weather conditions (+oil), Level 2 power: Internal, flood, weather		Yes, for all initiators	Original: 1989-94, 96, 97, 99, 00, 01, 06 1992- 97 1994- 98, 01, 06 1992 1994-97, 98, 00, 03, 06 1997- 06 2003-06 2004- 06 1997- 98, 02, 06 1998-02, 06 2006	Identification of weak points, improvement of design Support of PSA applications and risk informed decision making, Improvement of operator training,	Design modifications Risk informed TechSpecs Safety monitor RI ISI – pilot safety classification of equipment, Economic optimization and prioritization of design options,

Plant **Name**	**Plant** **type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Olkiluoto1/2	BWR 660	Level 1and 2	Level 1 power: Internal, fires, flood, seismic, harsh weather conditions (+oil), Level 1 shutdown: Internal, fires, Level 2 power: Initiarors as level 1		Yes, for all initiators	Original: 1989- 94, 99, 97 1992-94, 98 1991-94, 97, 04 1996 1994- 97, 98, 03, 05 1992-97, 06, 1998 1997-03	Identification of weak points, improvement of design Support of PSA applications and risk informed decision making Improvement of operator training,	Design modifications, Risk informed TechSpecs, RI ISI – pilot, PSA based event analysis, safety classification of equipment,

Czech Republic

Plant **Name**	Plant **type**	Scope of the PSA carried out				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Dukovany	WWER 440/213	Level 2	Internal events Internal hazards (fires and floods)	All plant operating states /Level 2 at power/	Yes Updated every year	Original: 1993/1995 Living since 1996	Identification of weak points, improvement of design Support of PSA applications and risk informed decision making	Design modifications Risk informed TechSpecs Safety monitor RI ISI – pilot PSA based event analysis
Temelin	WWER 1000/320	Level 2	Internal events Internal hazards (fires and floods) External hazards	All plant operating states /Level 2 at power/	Yes	Original: 1996 Revised: 2003	Identification of weak points, improvement of design Support of PSA applications and risk informed decision making	Design modifications Risk informed TechSpecs Safety monitor RI ISI – pilot PSA based event analysis

Canada

Plant Name	**Plant[6] type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Pickering A	4x540 MWe	3	Internal	Full power, shutdown		1995/2007		
Pickering B	4x540 MWe	3	Internal	Full power, shutdown		2003/2006		
Darlington	4x880 MWe	3	Internal	Full power, shutdown		1987/2000 (internal)		
Bruce A	4x820 MWe	3	Internal	Full power, shutdown	Being maintained as Living PSA	2003,/2005, 2005	U3-4 Restart	U1-2 Restart/Refurbis hment
Bruce B	4x860 MWe	3	Internal	Full power, shutdown		1999/2001, 1999/2002		
Gentilly-2	600 MWe	PSA scope is being finalized. Basic inputs for PSA are being prepared.						Refurbishment

[6] All Canadian plants are CANDU.

Plant **Name**	**Plant[6]** **type**	**Scope of the PSA carried out**				**PSA usage**		
Point Lepreau	600 MWe	1	Internal			2001		
		1	External			2003		
		2	Consequence analysis			2002		
		2	Containment performance			2004		
			Internal, external, internal fire, flood, PSA based seismic Margin			2007		

Belgium

Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Doel 1&2	PWR	Level 1	Internal events Internal hazards (fire/ flood only)[F]	Power & Shutdown	No	Original: 2005 Revised: 2010 2015 for F&F PSA	Periodic safety review Continuous PSA project	Design review PSA based event analysis
		Level 2- [A]	Internal events only	Original: At power only Update: Power and Shutdown	No	Original: 2005 Revised: 2010[C]	Periodic safety review Continuous PSA project	Design review
Tihange 1	PWR	Level 1	Internal events Internal hazards (fire/ flood only)[F]	Power & Shutdown	No	Original: 2006 Revised: 2010 2015 for F&F PSA	Periodic safety review Continuous PSA project	Design review PSA based event analysis
		Level 2- [A]	Internal events only	At power only Update: Power and Shutdown	No	Original: 2006 Revised: 2010[C]	Periodic safety review Continuous PSA project	Design review
Doel 3 Tihange 2	PWR	Level 1	Internal events Internal hazards (fire/ flood only)[F]	Power & Shutdown	No	Original: 2000 Revised: 2010 2015 for F&F PSA	Periodic safety review Continuous PSA project	Design review PSA based event analysis
		Level 2 [B]	Internal events only	Original: At power only Update: Power and Shutdown	No	Original: 2000 Revised: 2010[C]	Periodic safety review Continuous PSA project	Design review

Appendix B – Contact Information

USA

Regulatory Authority / Technical Support Organisation	Direct Contact
U. S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Division of Risk Assessment and Special Projects Probabilistic Risk and Applications Directorate MS TWFN 10E50 Washington, DC 20555 301-415-6189	Dr. Nathan Siu, Senior Technical Advisor 301-415-6925 Mr. John Monninger, Deputy Director 301-415-6189
Regulatory Authority Website Address:	www.nrc.gov

UK

Regulatory Authority / Technical Support Organisation	Direct Contact
NII (Nuclear Installations Inspectorate) St Peter's House Balliol Road Bootle Merseyside, UK L20 3LZ Tel: +44 (0)151 951 4000 Fax:: +44 (0)151 951 3942	Ms. Ana GOMEZ-COBO Nuclear Installations Inspectorate Health & Safety Executive Redgrave Court Merton Road Bootle L20 Merseyside Tel: +44 151 951 4047 Fax: E-mail: ana.gomez-cobo@hse.gsi.gov.uk
Regulatory Authority Website Address:	www.hse.gov.uk/nsd/nsdhome.htm

Taiwan

Most of the PSA associated research activities are performed by INER in Taiwan. The information of contact person is as follow:

Contact person in Chinese Taipei / Taiwan	Address information	
Dr. Tsu-Mu Kao	Nuclear Engineering Division Institute of Nuclear Energy Research P.O. Box 3-3, Lung Tan, Tao Yuan, Taiwan 32546, R.O.C. Tel:+886-3-471-1400 ext:6070 Fax: +886-3-471-1404 Email: tmkao@iner.gov.tw	

Switzerland

Contact person in Switzerland	Address information	
Dr. Gerhard Schoen	Head of PSA and AM Section HSK, Swiss Federal Nuclear Safety Inspectorate CH-5232 Villigen-HSK Tel : +41 56 310 38 69 Fax : +41 56 310 38 54 E-mail : gerhard.schoen@hsk.ch	

Sweden

Contact persons in Sweden	Address information	
SKI Lars Gunsell	SE-10658 Stockholm, Sweden +46 6 6988476 lars.gunsell@ski.se	
SKI Ralph Nyman	SE-10658 Stockholm, Sweden +46 6 6988478 ralph.nyman@ski.se	
SKI Tomas Jelinek	SE-10658 Stockholm, Sweden +46 6 6988440 tomas.jelinek@ski.se	WG-risk contacts
Forsmarks Kraftgrupp AB Göran Hultquist		
OKG Aktiebolag Anders Rapp		
Ringhals AB Stefan Eriksson		

Spain

Regulatory Authority	Direct Contact
Name and Address *Consejo de Seguridad Nuclear* *Justo Dorado, 11* *28040 Madrid* *SPAIN* Tel: +34 91 3460 100 Fax: +34 91 3460 588	Name and Address *Alfredo Lantarón* *Consejo de Seguridad Nuclear* *Justo Dorado, 11* *28040 Madrid* *SPAIN* Tel: 34 91 3460 259 Fax: 34 91 3460 496 Email: alg@csn.es
Regulatory Authority Website Address:	http://www.csn.es
Reference Documents	*Programa Integrado de realizacion y utilizacion de los Analisis Probabilistas de Seguridad (APS) en España. CSN, Coleccion Otros Documentos, 7.1998.*

Slovenia

Ministry of the Environment and Spatial Planning *Slovenian Nuclear Safety Administration* *Djordje Vojnovič*	*Železna cesta 16* *P.O. Box: 5759* *SI-1001 Ljubljana* *SLOVENIA* e-mail: Djordje.Vojnovic@gov.si webpage: www.ursjv.gov.si

Slovak Republic

UJD, Bajkalska 27, P.O.Box 24, 820 07 Bratislava 27, Slovak Republic Mr. Jan Husarcek	tel.: 00421 2 58221153 fax: 00421 2 58221166 e-mail: jan.husarcek@ujd.gov.sk
RELKO Ltd, Racianska 75, P.O.Box 95, 830 08 Bratislava, Slovak Republic Mr. Zoltan Kovacs	tel: 00421 2 44460138 fax: 00421 2 44460139 e-mail: kovacs@relko.sk

The Netherlands

Contact. M.F. Versteeg KFD Ministry VROM	VI/KFD (IPC 560) PO Box 16191 2500 BD The Hague The Netherlands Tel: + 31 70 3392488 e-mail: magiel.versteeg@minvrom.nl

Mexico

Regulatory Authority	Direct Contact
Comisión Nacional de Seguridad Nuclear y Salvaguardias Dr. Barragán 779 Col. Narvarte 03020 México D.F. México Tel: (52 55) 5095-3200 Fax:: (52 55) 5095-3295	Ramon López Morones Dr. Barragán 779 Col. Narvarte 03020 México D.F. México Tel: (52 55) 5095-3241 Fax: (52 5) 5095-3294 Email: rlopezm@cnsns.gob.mx
Regulatory Authority Website Address:	www.cnsns.gob.mx
Reference Documents	

Korea

Regulatory Authority / Technical Support Organisation	Direct Contact
Korea Institute of Nuclear Safety P.O. Box 114, Yuseong, Daejeon, 305-600, KOREA Tel: 82 42 868 0000 Fax: 82 42 861 1700 Website Address: www.kins.re.kr	Name and Address: Chang-Ju Lee Korea Institute of Nuclear Safety P.O. Box 114, Yuseong, Daejeon, 305-600, KOREA Tel: 82 42 868 0149 Fax: 82 42 868 0457 Email: cjlee@kins.re.kr

Japan

Regulatory Authority / Technical Support Organisation	Direct Contact
Mamoru FUKUDA Director Probabilistic Safety Assessment Group Safety Analysis and Evaluation Division Incorporated Administrative Agency Japan Nuclear Energy Safety Organization(JNES)	Kamiya-cho MT Bldg., 4-3-20 Toranomon, Minato-ku, Tokyo, 105-001 Japan Tel:+81-3-4511-1550, Fax:+81-3-4511-1598 E-mail: fukuda-mamoru@jnes.go.jp URL http://www.jnes.go.jp

Italy

Contact	Address
Luciano Burgazzi ENEA, Italian Commission for New Technologies, Energy and Environment	Via Martiri di Monte Sole, 4 40129 Bologna Italy Tel. +39 051 6098 556 Fax: +39 051 6098279 Email: burgazzi@bologna.enea.it Web site: www.enea.it
Rino Caporali APAT, Italian Agency for Environmental Protection and for Technical Services	Via Vitaliano Brancati, 48 00148 Roma Italy Tel. +39 06 50072152 Fax: +39 06 50072941 Email: rino.caporali@apat.it Web site: info.apat.it

Germany

Regulatory Authority / Technical Support Organisation	Direct Contact
BMU (Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit) Robert-Schuman-Platz 3 D-53175 Bonn Germany Tel: ++/49/228 / 99 305-0 Fax: ++/49/228 / 99 305-3225 Website Address: www.bmu.de GRS (Gesellschaft für Anlagen- und Reaktorsicherheit mbH) Schwertnergasse 1 D-50667 Köln Germany Tel: ++/49/221/2068-0 Fax:: ++/49/221/2068-856 Website Address: www.grs.de	Dr. Marina RÖWEKAMP Gesellschaft für Anlagen- und Reactorsicherheit (GRS) mbH Schwertnergasse 1 50667 Köln Tel: +49 (0) 221 2068 898 Fax: +49 (0) 221 2068 10898 E-mail: marina.roewekamp@grs.de

Hungary

Regulatory Authority/Technical Support Organisation	Direct Contact
Géza MACSUGA Hungarian Atomic Energy Authority H-1539 Budapest, PO Box 676. Tel.: + 36 1 436 4910 Fax: + 36 1 436 4909 E-mail: macsuga@haea.gov.hu	Attila BAREITH VEIKI Institute for Electric Power Research Co. H-1251 Budapest, PO Box 80. Tel.: +36 1 457 8250 Fax: +36 1 457 8253 E-mail: bareith@aed.veiki.hu
Regulatory Authority Website Address:	http://www.haea.gov.hu

France

Technical Support of the Regulatory Authority	Direct Contact
Institut de Radioprotection et de Sûreté Nucléaire (IRSN) 77-83 avenue du Général-de-Gaulle 92140 Clamart France Tel : (33) 1 58 35 88 88 Fax : (33) 1 58 35 84 51	Name and Address: J.M.LANORE IRSN/DSR BP 17 92162 Fontenay-aux-Roses CEDEX FRANCE Tel : (33) 1 58 35 76 48 Fax :: (33) 1 42 53 91 24 Email : jeanne-marie.lanore@ipsn.fr
Technical Support of the Regulatory Authority Website Address:	http://www.irsn.org/
Electricité de France DPI – DIN - SEPTEN 12-14 avenue Dutrievoz 69628 VILLEURBANNE Cedex France	Vincent SOREL Tel : +33 4 72 82 71 56 Fax : +33 4 72 82 77 44 Vincent.sorel@edf.fr

Finland

Reino Virolainen Radiation and Nuclear Safety Authority (STUK)	Laippatie 4 P.O. Box 14 FIN-00881 Helsinki Finland Tel: +358 9 7598 8362 **Fax +** 358 9 7598 8382 E-mail: Reino.Virolainen@stuk.fi

Czech Republic

Technical Support Organisation	Direct Contact
Tel: +420-26617 1111 Fax:: Website Address: www.ujv.cz	Milan PATRIK UJV Rez, a.s. 25068 Rez Czech Republic Tel: +420-2 6617 3560 Fax: +420-2 6617 3561 Email: pat@ujv.cz
Utility	Direct Contact
Tel: +420-381101111 Fax:: Website Address: www.cez.cz	Ondrej MLADY CEZ, a.s. NPP Temelin 37305 Temelin Czech Republic Tel: +420-381103749 Fax: +420-381102794 Email: Ondrej.Mlady@cez.cz

Canada

Regulatory Authority / Technical Support Organisation	Direct Contact
Canadian Nuclear Safety Commision P.O.Box 1046 , Station B 280 Slater Street Ottawa, Canada K1P 5S9	Raducu Gheorghe CNSC P.O.Box 1046 , Station B 280 Slater Street Ottawa, Canada K1P 5S9 Tel: (001) 613-947-0517 Fax: (001) 613-995-5086 e-mail:gheorgher@cnsc-ccsn.gc.ca or raducu.gheorghe@cnsc-ccsn.gc.ca
Regulatory Authority Website Address: http://www.nuclearsafety.gc.ca/	

Belgium

Regulatory Authority / Technical Support Organisation	Direct Contact
AVN (Association Vinçotte Nuclear) Rue Walcourt 148 B-1070 Brussels Belgium Tel: ++/32/2/5280111 Fax:: ++/32/2/5280101 Website Address: www.avn.be	Pieter DE GELDER AVN Rue Walcourt 148 B-1070 Brussels Tel: ++/32/2/5280260 Fax: ++/32/2/5280102 Email: pdg@avn.be
Owner's Engineer	Direct Contact
TRACTEBEL ENGINEERING (SUEZ) Avenue Ariane 7 B - 1200 Brussels Belgium Tel. + 32 2 773 8000 Fax + 32 2 773 8900 Website address: www.tractebel-engineering.com	Isabelle HENDRICKX Tractebel Engineering Avenue Ariane 7 B-1200 Brussels Tel. + 32 2 773 76 64 Fax + 32 2 773 89 00 Email: isabelle.hendrickx@tractebel.com

Appendix C - Questionnaire and guidance to authors

Section Headings for the Report on the Use and Development of PSA

The section headings that authors should use in preparing their submissions are given below. Authors should note that the report will relate to the PSAs for power reactors only. One reply is required for each country participating in the Task. The aim is to produce a stand alone report so that parts of the previous report that are still valid should be copied into the current report and amended as necessary.

Executive Summary*

This section will provide a summary of the report and identify major changes and trends in PSA that have occurred over the past five years.

Section 1 – Introduction*

This section will present the background, the objectives and the scope of the report.

***** ***Note, the Executive Summary and Section 1 – Introduction will be written after the rest of the report has been compiled so that no contributions are expected from the member countries.***

Section 2 – PSA Framework and Environment

Authors should provide a description of the background to the development and use of PSA in their country. This should typically include:

- a description of the regulatory framework in their country and the types of regulations that have been defined; the regulatory policy on PSA.
- the requirement for a PSA to be produced; whether this is a legal or regulatory requirement; what the purposes are of the PSAs that have been produced.
- who has carried out the PSAs that have been produced – that is, whether they have been done by the licensee, the regulatory authority, technical support organisations, contractors, etc.
- the historical development of PSA highlighting the development of the scope and methodology of the PSAs; the insights gained from the early PSAs and the plant improvements that have been made..
- the aims of the PSAs that have been produced and how these aims have changed with time; the relative roles of the deterministic and probabilistic approaches in the safety case; whether a risk-informed approach has been adopted.

Section 3 – Numerical Safety Criteria

Authors should provide a description of the numerical safety criteria/ targets/ guidelines that have been defined in their country and what the basis/ justification is for them. This should include:

- the numerical safety criteria/ targets that have been defined that are addressed by the PSAs that have been produced; the risk metrics used (that is, core damage, large early/ late release, risk metrics for shutdown modes, offsite doses, societal risks, etc.).

- who has defined these criteria/ targets; their legal/ regulatory status (whether they are formal requirements or less formal guidelines).

- the basis/ justification for the numerical values that have been defined; how they relate to other risks to members of the public; whether these are objectives or limits.

If numerical safety criteria have not been defined, give the reason for this.

Section 4 – PSA Standards and Guidance

Authors should identify and give a description of the standards/ guidance documents/ etc. that has been used in producing the PSAs in their country. This should include national standards, national regulatory guides, widely used national industry guidelines, etc. The scope, purpose and status of these documents should be described and the references given in Section 11. In addition, any international guidance and standards such as those produced by NEA, IAEA, NRC, etc. that have been used should also be identified.

Section 5 – Status and Scope of PSA Programmes

Authors should provide a description of the status and scope of the PSAs that have been carried out in their country as follows:

- **objectives of the PSAs**: this should indicate what the objectives were of the PSA; the stage in the life of the plant when the PSA was carried out – that is, during the initial design, as part of licensing/ design certification, as part of a Periodic Safety Review, for life extension, etc.

- **level of PSA**: whether the PSAs have been carried out to Level 1/ core damage, Level 2/ large (early) release, Level 3/ societal risk.

- **range of initiating events included**: this should indicate the range of internal initiating events (such as transients, LOCAs, etc.), the range of internal hazards (such as internal, fire, flood, etc.) and the range of external hazards (such as seismic events, severe weather conditions, etc.) that have been addressed in the PSAs.

- **modes of operation addressed**: this should indicate the plant operating modes that have been addressed in the PSAs (such as operation at power, low power, shutdown, refuelling, etc.).

- **Living PSA**: this should indicate whether the PSAs are being maintained as Living PSAs and, if so, the periodicity and scope with which they are updated.

[Note, a summary of the status and scope of the PSAs that have been produced is given in tabular form in ***Appendix A - Overview of the Status of PSA Programmes*** of NEA/CSNI/R(2002)18 and authors are requested to update this table as well.]

Section 6 – PSA Methodology and Data

Authors should provide a description of the methodologies and sources of data used for the major parts of the PSA including the following:

- **overall methodology**: to cover Level 1 PSA (use of event trees/ fault trees, etc.), Level 2 PSA (number/ definition of plant damage states and how they have been defined, number of nodes in the containment event trees, etc.) and Level 3 PSA (number of source term/ release categories and how they have been defined, the range of off-site consequences addressed, etc.).

- **common cause failure**: to cover the modelling approach used and the quantification/ data used.

- **human reliability**: to cover the modelling approach used, the types of operator actions included (errors or omission, commission, etc.), data used and modelling of interdependencies between operator actions, the treatment of maintenance activities and emergency management actions where relevant, etc.

- **other issues**: this could include the modelling of systems that are shared between multi plant units, etc.

Authors should also indicate how the results of the PSA were used to identify weaknesses in the design or operation of the plant including cut set analysis, importance functions, sensitivity studies, etc.

Section 7 – PSA Applications

Authors should provide a description of the range of applications for which the PSAs are being used which could include the following:

- design evaluation; comparison with risk criteria (where they have been defined).

- identification/ reduction of the risk from dominant contributors; support for back-fitting activities and plant modifications; comparison of options.

- providing an input into risk-informed Technical Specifications; risk informed configuration control; Risk Monitors; Reliability Centred Maintenance; etc.

- providing an input into emergency operating and other procedures; accident management strategies; emergency planning; training of plant operating and maintenance staff.

- the development and monitoring of plant safety indicators.

- analysis of operational events; PSA based event analysis.

- risk informed decision making; risk informed regulation.

- risk informed in-service inspection, in-service testing.

- as the basis for the implementation of graded QA.

- review of security arrangements.

The information provided should focus on the most recent applications of the PSA and describe how the PSA was used, the quality requirements for the PSA before it could be used for the application and any changes that needed to be made to the PSA to make it suitable for the application

Section 8 – Results and Insights from the PSAs

Authors should provide a description of the results that have been obtained from the PSAs and the insights that have been derived – for example, any weaknesses that have been identified where changes need to be considered to the design or operation of the plant. For member countries with a large number of reactors, authors should aim to give an indication of the results that have been obtained for the most recent/ state of the art PSAs that have been carried out.

Section 9 – *Future Developments*

Authors should provide a description of the work being carried out in their country to increase the scope or otherwise improve the PSAs that have been carried out, or to provide better support for them. The aims of these future developments should be indicated.

This section should address:

- work carried out to make improvements to the PSAs that have been produced; increase in the scope or level of detail of the PSAs; amendments to the PSA so that it can be used for a wider range of applications; removal of conservatisms, shortcomings or limitations in the usability of the PSAs.

- data collection exercises - including data for initiating event frequencies, component failure probabilities, common cause failure probabilities, human error probabilities, etc.

- work being carried out to improve the understanding of the physical processes involved; transient analysis to support the success criteria used in the PSA; consequence modelling; modelling of the physical phenomena that occur following core damage; modelling of the consequences of releases of radioactive material from the plant.

- development of improved or new methods and models including the modelling of computer based systems/ software reliability; passive system reliability; modelling of common cause failure; modelling of human reliability and dependencies; modelling the influence of organisational processes; modelling of ageing; development of alternative methods – for example, dynamic PSA.

- developments in the way that the results and insights from the PSA are communicated – particularly to non-specialists in PSA; PSA training to increase the level of acceptance of the PSA.

Section 10 - References

Authors should provide a description of the detailed references to the information they have cited in the earlier sections.

Appendix A - Overview of the Status of PSA Programmes

The aim of the appendix is to give an overview of the PSAs that have been carried out in the member countries and this information will be presented in a tabular form similar to that in the 2002 Report using the headings given below. Authors should provide the following information for all the power reactors in their country:

Plant name:	(for all the reactors in your country).
Plant type:	(for all the reactors in your country).
PSA scope:	Level of PSA carried out (Level 1, 2 or 3).
	Scope of initiating events included in the PSA (internal events, internal hazards, external hazards).
	Plant Operating States included in the PSA (power operation, low power, shutdown, refuelling, etc.).
	Whether the PSA is maintained as a Living PSA.
PSA usage:	Date of the original PSA and any subsequent revisions.
	Reason for carrying out the PSA/ stage in the plant life that the PSA was carried out.
	Applications that the PSA has been used for.

Appendix B – Contact Information

This section gives a contact point in each of the countries for obtaining further information or details about the PSA programme.