

Use and Development of Probabilistic Safety Assessment

An Overview of the Situation
at the end of 2010

Unclassified

NEA/CSNI/R(2012)11

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

03-Jan-2013

English text only

**NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS**

Use and Development of Probabilistic Safety Assessment

An Overview of the situation at the end of 2010

JT03333028

Complete document available on OLIS in its original format

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.



NEA/CSNI/R(2012)11
Unclassified

English text only

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 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, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission 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 OECD Secretary-General.
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 1 February 1958. Current NEA membership consists of 30 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, Poland, Portugal, the Republic of Korea, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission 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 the 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.

Corrigenda to OECD publications may be found online at: www.oecd.org/publishing/corrigenda.

© OECD 2012

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of the OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) contact@cfcopies.com.

THE COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

“The Committee on the Safety of Nuclear Installations (CSNI) shall be responsible for the activities of the Agency that support maintaining and advancing the scientific and technical knowledge base of the safety of nuclear installations, with the aim of implementing the NEA Strategic Plan for 2011-2016 and the Joint CSNI/CNRA Strategic Plan and Mandates for 2011-2016 in its field of competence.

The Committee shall constitute a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development and engineering, to its activities. It shall have regard to the exchange of information between member countries and safety R&D programmes of various sizes in order to keep all member countries involved in and abreast of developments in technical safety matters.

The Committee shall review the state of knowledge on important topics of nuclear safety science and techniques and of safety assessments, and ensure that operating experience is appropriately accounted for in its activities. It shall initiate and conduct programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach consensus on technical issues of common interest. It shall promote the co-ordination of work in different member countries that serve to maintain and enhance competence in nuclear safety matters, including the establishment of joint undertakings, and shall assist in the feedback of the results to participating organisations. The Committee shall ensure that valuable end-products of the technical reviews and analyses are produced and available to members in a timely manner.

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

The Committee shall organise its own activities. Furthermore, it shall examine any other matters referred to it by the Steering Committee. It may sponsor specialist meetings and technical working groups to further its objectives. In implementing its programme the Committee shall establish co-operative mechanisms with the Committee on Nuclear Regulatory Activities in order to work with that Committee on matters of common interest, avoiding unnecessary duplications.

The Committee shall also co-operate with the Committee on Radiation Protection and Public Health, the Radioactive Waste Management Committee, the Committee for Technical and Economic Studies on Nuclear Energy Development and the Fuel Cycle and the Nuclear Science Committee on matters of common interest.”

FOREWORD

The main objective of the Working Group on Risk Assessment (WGRISK) of the Nuclear Energy Agency (NEA)/Committee on the Safety of Nuclear Installations (CSNI) is to advance the Probabilistic Safety Assessment (PSA) understanding and to enhance its utilisation for improving the safety of nuclear installations. Due to its disciplined, integrated and systematic approach, PSA is now considered as a necessary complement to traditional deterministic safety analysis.

To accomplish this mission, WGRISK performs a number of activities to exchange PSA-related information among member countries.

The results of exchanges have been compiled in a CSNI report entitled “The Use and Development of Probabilistic Safety Assessment”, first issued in 2002 [[NEA/CSNI/R\(2002\)18](#)], then updated in 2007 [[NEA/CSNI/R\(2002\)18](#)].

This report provides a description of the PSA activities in the member countries at the time of the report writing. Since there have been significant new developments in PSA since the last version, and considering the interest and usefulness of the previous versions, WGRISK initiated the development of an updated version of the report in early 2011.

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 in Appendix B of this report.

Some persons helped among the national officers to produce the executive summary and the summaries of each section, and the NEA express to provide particular appreciation to these experts who are Mrs Jeanne-Marie Lanore (Task leader, France), Dr. Nathan Siu (USA), Dr. Marina Röwekamp (Germany), Mrs Dominique Vasseur (France), Mr Peter De Gelder (Belgium), Mr Milan Patrik (Czech Republic), Dr. Shane Turner (UK), Dr. P.V. Varde (India) and Mr Smain Yalaoui (Canada).

The NEA responsible administrator was Dr. Abdallah Amri.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	7
1. INTRODUCTION	15
2. PSA FRAMEWORK AND ENVIRONMENT	19
3. NUMERICAL SAFETY CRITERIA	21
4. PSA STANDARDS AND GUIDANCE.....	27
5. STATUS AND SCOPE OF PSA PROGRAMS.....	31
6. PSA METHODOLOGY AND DATA	33
7. PSA APPLICATIONS.....	37
8. RESULTS AND INSIGHTS FROM THE PSAS.....	41
9. FUTURE DEVELOPMENTS AND RESEARCH.....	43
10. OVERALL INSIGHTS.....	53
APPENDIX A.....	55
APPENDIX B.....	95
APPENDIX C.....	411

EXECUTIVE SUMMARY

Background

The main objective of the Working Group on Risk Assessment (WGRISK) of the Nuclear Energy Agency (NEA)/Committee on the Safety of Nuclear Installations (CSNI) is to advance the Probabilistic Safety Assessment (PSA) understanding and to enhance its utilisation for improving the safety of nuclear installations. Due to its disciplined, integrated and systematic approach, PSA is now considered as a necessary complement to traditional deterministic safety analysis.

To accomplish this mission, WGRISK performs a number of activities to exchange PSA-related information among member countries.

The results of exchanges have been compiled in a CSNI report entitled “The Use and Development of Probabilistic Safety Assessment”, first issued in 2002 [1], then updated in 2007 [2].

This report provides a description of the PSA activities in the member countries at the time of the report writing. Since there have been significant new developments in PSA since the last version, and considering the interest and usefulness of the previous versions, WGRISK initiated the development of an updated version of the report in early 2011.

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 the end of 2010. As previously the Task was carried out in cooperation with the International Atomic Energy Agency (IAEA), and 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

Each country that participated in the 2007 report updated their contribution to the different chapters, with emphasis on new developments. Countries which did not participate in the writing of the earlier reports but wishing to be involved have also contributed, following the format provided by the task group.

A small writing group was set up in order to prepare the updated summaries of each chapter and a general overview. 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.

While the compilation is not a complete one, it provides reference information to both PSA practitioners and others involved in the nuclear industry.

Insights

PSA Framework and Environment

The overall environment for the use of PSA in regulatory and licensee decision-making is quite positive in all countries that provided information, and has increased since the previous report.

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. 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.

The new aspect important to note is the increasing place of PSA for new plants. Most countries are formally requiring that a PSA be performed for new plants or plants of advanced design, and following the increasing number of new plants (at the stage of project, design or construction) the corresponding PSAs are developed and extended.

Numerical Safety Criteria

As noted in the 2007 report, there are differences in the status of the numerical safety criteria that have been defined in different countries. The differences 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. Several countries use the numerical criteria as an orientation and as an indicative figure rather than a strict criterion. In a number of countries no numerical safety criteria have been defined.

However, an evolution since the previous report is the place of PSA for new plants. In several countries, criteria have been defined for existing plants and for new plants, and generally the safety criteria for new plants are more precise (concerning numerical value and/or requirements) than for existing 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 for which a PSA is available.

In some countries, high level qualitative and quantitative guidance have been developed and used to derive lower level or surrogate criteria that are easier to address and are sufficient to demonstrate that the higher level criteria are met. The most common metrics used are Core Damage Frequency (CDF) and Large Release Frequency (LRF) or ILarge Early Release Frequency (LERF). However, as mentioned in the previous report, there is some variability between the corresponding numerical values.

Interesting complementary safety goals (new) have been developed that require a minimum conditional probability between CDF and LRF in order to ensure defence-in-depth (USA, Taiwan), to use a Containment Failure frequency (Japan), or to define a Small Release Frequency (SRF) in addition to LRF (Canada).

PSA Standards and Guidance

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 led to a greater need for the PSAs being produced to be of a sufficient quality to support a wide range of applications. This has led to a greater level of effort being applied to the development of PSA standards and guidance in a number of the member countries since the previous report.

Several countries have developed their own standards and guides. Many of these are very detailed and complete.

For other member countries, no specific PSA standards or guidance have 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, taking into account international practices.

The recent answers indicate that PSA quality is always considered as a very important topic for all PSA applications, and often external reviews are carried out (even independent studies performed by different teams in some countries).

Status and Scope of PSA Programmes

All operating nuclear power plants in the reporting countries have been studied using PSA methods. A Level 1¹ internal events PSA has been performed on all plants. In many cases, this has been extended to a Level 1+² or Level 2³ PSA. In several cases, the Level 2 PSA consists mainly of the determination of the Large Early Release Frequency (LERF), although there is an apparent tendency towards a more 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 several¹ countries or have already been considered. Only a few Level 3⁴ PSAs have been performed.

¹ A Level 1 PSA is the assessment of Core Melt Frequency

² A level 1+ PSA is an extension of Level 1 with a classification of Core Melt sequences into release categories taking into account the containment function (without release calculations)

³ A level 2 PSA is the assessment of the frequency and level of releases.

⁴ A level 3 PSA is the assessment of the frequency and level of harm to the public and environment outside of the plant.

Some new examples of scope extension are the use of PSA for the analysis of the Spent Fuel Pool, for plant decommissioning, and for fuel handling. Also to be noted is that some PSAs were developed for multiple units.

Nearly all the countries indicate that they regularly update (or intend to update) their studies (living PSA).

It appears that many countries are heading towards a living PSA including both Level 1 and Level 2, both full power and shutdown situations, and both internal and external initiating events. The number of completed PSAs corresponding to this scope is increasing.

PSA methodology

PSA general methodology, in terms of a fault tree event tree approach, is broadly similar to what was presented in the previous report, and even to what was done in the very early PSAs as WASH 1400. In terms of the current status of PSA methodologies, the following observations are noted from the countries' responses:

- Level 1 PSA methodology appears as mature and similar for all the countries.
- Level 2 PSA methodology is more variable, notably with very different numbers of Plant Damage States and of Release Categories.
- There is also an apparent tendency of more integrated Level 1/Level 2 PSA models.
- An increasing effort is being carried out for including internal and external events (especially fire PSA methodology, which was developed and extended in several countries). Progress is also noted for modelling of Common Cause Failures (CCF) and of human reliability (the use of advanced Human Reliability Assessment (HRA) methods is increasing).
- Some recent PSAs include modelling of digital instrumentation and control (I&C), and several countries have significant activities in this area.
- Recent PSAs relating to new or advanced reactors include modelling of passive systems.

PSA applications and insights

Although there are differences in the regulatory systems, there are strong similarities in the use of PSA. All of the countries contributing to the updated report have identified useful applications of PSA. In general terms, these applications are very similar to those identified in the 2007 survey. However, the number of applications appears to be increasing.

- Applications to plant design:

The main application of the PSA continues to involve 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; and 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 plant weaknesses that need to be addressed.

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 determine what plant improvements should be made.

Meanwhile, PSA is particularly an important part of the design and the licensing process of new plants. Even a simplified PSA during the early stage of the design has led to significant safety improvements.

- Applications to plant operation:

Many countries give examples of the use of PSA for plant operation optimisation, for example:

- The PSA has been used to provide risk information to inform the decisions on 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, to identify the components that need to be given special attention as part of the programme for the management of ageing.
- PSAs have also been used to improve or justify Technical Specifications, to define Risk-Informed In-Service Inspection, and for optimisation of maintenance activities.
- Risk Monitors are now in operation at a large number of plants.
- The analysis of operating events using the PSA is carried out in many countries as part of the analysis of operating experience.
- Several countries have identified new examples of the use of PSA for accident management (before and after core melt).

- Risk Informed Regulation:

The risk information provided by the PSA is increasingly being used by regulatory authorities in planning their activities.

Research

An interesting point is that an important number of research activities are in progress, relating to many different PSA aspects. While the PSA methodology is reasonably robust in most areas, additional research is needed and is 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. Several activities are related to the development of new or advanced reactors.

Key areas of research in progress include the following:

- Development of PSA methods;
- PSA for internal hazards;
- PSA for external hazards;
- Common cause failure modelling;
- Human reliability analysis (HRA);
- Reliability data collection;
- PSA for passive systems;
- Reliability of digital systems;
- Level 2 PSA;
- Level 3 PSA;
- Uncertainties;
- Dynamic PSA;
- Modelling of ageing in PSA;
- Fuel route PSA; and
- Use of PSA in risk-informed decision making.

It can be seen that the general areas of PSA research are not really new, but in each area substantial activities are ongoing, with specific developments that are presented in the detailed report. Of special note is research relating to severe accidents, to fire, and to human factors, which supports improved PSA modelling. Moreover, research relevant to problems relating to new plants (e.g., digital I&C and passive systems) is receiving high priority.

It has to be noted that recent WGRISK activities, completed or ongoing, address many of these areas.

Overall remarks

With the updating of the CSNI Report on “Use and development of Probabilistic Safety Assessment”, some main conclusions could be drawn:

- All the PSA developments and applications already described in the previous versions of the report are still valid and regularly increasing. This applies to the importance of PSA

framework, the number of studies carried out, the PSA scope, the number of applications (for design and operation safety improvements), and the volume of on-going research. It can be noted that although PSA methods and applications have made real progress during these last years a significant level of development is still in progress.

- Moreover the development of new and advanced designs has led to a more rapid development in particular fields. It can be noted for example the definition of a more formal framework, more precise safety goals, efforts relating to the importance of external hazards and to new specific problems like reliability of digital systems and reliability of passive systems. A tendency towards harmonization appears clearly.

- It has to be noted that this report was prepared before March 2011 Fukushima accident and consequently does not take into account the potential new developments and priorities based on lessons learned from Fukushima. This report gives an overview of the situation before Fukushima and a next updating is expected to focus on the post-Fukushima activities.

- As previously, WGRISK will use the results of this report, as moderated by Fukushima response activities, to monitor the conduct of its ongoing activities, and to promote and implement new international collaborative efforts within the framework of the CSNI.

1. INTRODUCTION

Background

The main objective of the Working Group on Risk Assessment (WGRISK) of the Nuclear Energy Agency (NEA)/Committee on the Safety of Nuclear Installations (CSNI) is to advance the Probabilistic Safety Assessment (PSA) understanding and to enhance its utilisation for improving the safety of nuclear installations. Due to its disciplined, integrated and systematic approach, PSA is now considered as a necessary complement to traditional deterministic safety analysis.

To accomplish this mission, WGRISK performs a number of activities to exchange PSA-related information between member countries. The results of exchanges have been compiled in a CSNI report entitled “The Use and Development of Probabilistic Safety Assessment”, first issued in 2002 [1], then updated in 2007 [2]. The task was carried out in cooperation with the IAEA, and this has led to more information and thus provided a better overview on PSA worldwide.

This report, intended to be updated every 3 to 4 years, provides descriptions of the current status of PSA programmes in member countries including basic background information, guidelines, various PSA applications, major results in recent studies, PSA based plant modifications and research and development topics.

In addition, synthetic summaries of each chapter were written and grouped as a Technical Note with the aim of a large diffusion [3]. The experience feedback indicates that these reports were widely used, especially by decision makers.

Objectives of the task

The interest and usefulness of the two previous versions indicated that an updating was necessary. The objective of this task was then to update both the main report and the summary, with emphasis on the new aspects, the general trends and specific points of interest if mentioned by the contributors.

While the compilation is a not complete compilation, it provides a “snapshot” of the current situation in the member and non-member countries and hence it provides reference information and various insights to both PSA practitioners and others involved in the nuclear industry.

These reports also form a basis for identification of new detailed tasks for initiation by WGRISK, and more generally to follow the main trends of PSA development and application in the world.

Process

The CAPS was approved by the CSNI in December 2010 (see Appendix C).

Each country that participated in the 2007 report updated their contribution to the different chapters, with emphasis on new developments. Countries which did not participate in the writing of the earlier reports but wishing to be involved have also contributed, following the format provided by the task group. The updated and new contributions were collected by the Secretariat until March 2011. Contributions were received from about 20 countries totalling several hundred pages of information relating to all PSA aspects (context, regulation, methods, data, results and applications).

A small writing group was setup in order to prepare the updated summaries of each chapter and a general overview, including Bel V, GRS, IRSN and USNRC (as previously), and in addition CSNC, ONR, BARC, UJV and EDF contributed to the writing group. The summaries were written by January 2012. IRSN was the coordinator of the task and proposed the executive summary and the introduction chapter.

Report

The report provides descriptions of the current status of PSA programmes in member countries including basic background information, guidelines, various PSA applications, major results in recent studies, PSA based plant modifications and research and development topics.

The structure of the report (definition of the chapters) is similar to the previous versions, in order to facilitate updating and to make it easier to identify what is new. The new points are summarised in a last chapter (chapter 10: insights).

A difference of presentation with the previous version is that the summaries are grouped for being the main report and the country-by-country replies are given in Appendix A and B.

The anticipated audience for this report is the industry and regulators, those interested in current approaches, as well as NEA working groups interested in collaborative activities.

Insights

With the updating of the CSNI Report on Use and development of Probabilistic Safety Assessment, some main conclusions could be drawn:

With the updating of the CSNI Report on “Use and development of Probabilistic Safety Assessment”, some main conclusions could be drawn:

- All the PSA developments and applications already described in the previous versions of the report are still valid and regularly increasing. This applies to the importance of PSA framework, the number of studies carried out, the PSA scope, the number of applications (for design and operation safety improvements), and the volume of on-going research. It can be noted that although PSA methods and applications have made real progress during these last years a significant level of development is still in progress.
- Moreover the development of new and advanced designs has led to a more rapid development in particular fields. It can be noted for example the definition of a more formal

framework, more precise safety goals, efforts relating to the importance of external hazards and to new specific problems like reliability of digital systems and reliability of passive systems. A tendency towards harmonization appears clearly.

- It has to be noted that this report was prepared before March 2011 Fukushima accident and consequently does not take into account the potential new developments and priorities based on lessons learned from Fukushima. This report gives an overview of the situation before Fukushima and a next updating is expected to focus on the post-Fukushima activities.
- As previously, WGRISK will use the results of this report, as moderated by Fukushima response activities, to monitor the conduct of its ongoing activities, and to promote and implement new international collaborative efforts within the framework of the CSNI.

2. PSA FRAMEWORK AND ENVIRONMENT

PSA is considered as a decision-support tool, and the PSA's ability to support a decision depends on the PSA scope and quality. To better understand the country-to-country variations in PSA elements, practices, and applications discussed later in the report, it's useful to understand the differing environments in which the PSAs are performed.

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 production and use of PSAs to provide information to complement and support the defense-in-depth philosophy used by most regulatory bodies, and to aid 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 an "As Low As Reasonably Practicable" 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 production and use 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 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 recent years, many more activities related to risk-informed safety assessment are being reported. This covers further development of risk-informed regulation (e.g. Finland, Japan, Korea, USA) and a more developed application of Risk Informed Decision Making by regulators (e.g. Canada, Hungary) and by licensees (e.g. Chinese Taipei). For more details on risk-informed applications, see also Chapter 7.

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, including those of advanced design, most countries are formally requiring that a PSA be performed. Since the previous edition of this report, more countries are reporting PSA activities related to new plants. These activities cover further development of regulatory requirements on PSA for new plants (e.g. India, Switzerland), specific licensing projects (e.g. Chinese Taipei) and generic design assessments

(e.g. UK). One of the countries (USA) also refers to plans for developing a more risk informed approach for licensing of advanced reactors, to identify the safety issues and gauge their significance.

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 is required. 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.

3. NUMERICAL SAFETY CRITERIA

Summary

“Numerical criteria” is used in this report as a general term that covers:

- Societal and individual risk metrics expressed by the number of fatalities (death of members of the public, acute fatalities that occur in a short time after the accident or in longer term)
- core damage frequency (CDF) per reactor year;
- large release frequency (LRF) or large early release frequency (LERF), expressed in terms of the quantity of radioactive elements such as I131 and Cs-137 released to the atmosphere
- doses to the public

Although numerical criteria are not required for risk-informed decision making, many countries have found it useful to develop/adopt such criteria to facilitate the use of the PSA quantitative results.

Status of the Numerical Safety Criteria

As noted in the previous report and in a WGRISK task report on the subject [4], there are differences in the status of the numerical safety criteria that have been defined in different countries. The differences 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.

In a number of countries no numerical safety criteria have been defined (Belgium, Hungary, Korea, Mexico). However, an evolution since the previous report is the use of PSA for new plants. In several countries, criteria have been defined for existing plants and for new plants, and generally the safety criteria for new plants are more demanding (concerning numerical value and/or requirements) than for existing 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 for which a PSA is available. Some countries use the numerical criteria as an orientation and as an indicative figure (Czech Rep., France, India, UK), whereas some countries have identified the safety criteria only for the new build (Canada, Finland, Slovenia, Switzerland). In some countries, criteria have been defined for existing plants and for new plants.

Framework for Defining the Numerical Safety Criteria

In some countries, the numerical criteria are derived from the high level metrics, i.e., the qualitative safety objectives such as the individual risk and/or societal risk, whereas in some other countries, the safety goals were adopted by the regulatory bodies or the licensees from IAEA (IAEA-INSAG-12) or from published documents by other bodies.

In most of the countries in which numerical safety criteria have been defined, the latter 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, the UK uses a comprehensive framework for defining the risk criteria. 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. It is noted that these criteria are not legal limits but are guidance, and are used by the regulator to inform the depth of assessment a particular issue is subject to.

Societal Risk Criteria

Qualitative Societal Risk Criteria

Some countries (Canada, USA) have high level qualitative criteria which 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.

Quantitative Societal Risk Criteria

The following approaches to societal risk criteria have been adopted:

- The societal risks are sometimes defined as acute fatalities that occur in a short time after the accident or in the longer term.
- The high level quantitative goals state that the level of increase should be less than about 0.1% of the existing risks.
- In the USA, the risk of death should be < 0.1% of the sum of cancer fatalities from other sources. A similar quantitative criterion is also defined in Korea.

There is no change in definition of the quantitative societal risk criteria since the last report and the criteria defined in the UK and the Netherlands are shown in Table 3-1 below.

Country	Organization	Risk metric	Frequency	Limit/Objective
UK	Regulator	≥ 100 deaths	10^{-5} /yr	Limit (BSL)
			10^{-7} /yr	Objective (BSO)
Netherlands	Law	10 Deaths	10^{-5} /yr	Limit
		100 Deaths ³	10^{-7} /yr	Limit

Individual Risk Criteria

Qualitative individual risk criteria

² Some countries like Japan also consider the impact to the whole society such as economical effects or land contamination

³ 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

Some countries (Canada, USA) have defined the qualitative individual risk criteria so that individual members of the public are provided a level of protection from the consequences of nuclear power plant operation such that there is no significant additional risk to the life and health of individuals.

Quantitative individual risk criteria

There is no any change from the previous report to the criteria for the risk of death for an individual member of the public. The criteria are presented in Table 3.2 below.

Country	Organization	Frequency	Limit/Objective	Notes
UK	Regulator	10^{-4} /yr 10^{-6} /yr	Limit (BSL) Objective (BSO)	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		$\approx 10^{-6}$ /yr	Limit	Acute fatality in the vicinity of the site boundary
		$\approx 10^{-6}$ /yr	Limit	Latent fatality by cancer to individuals within a certain distance from the site
Canada	Licensee	10^{-4} /yr 10^{-5} /yr	Limit for existing plants Objective for existing plants	Late fatality

Core Damage Frequency

The changes compared to the last report is the definition by Slovenia of numerical criteria. For other countries, there is no change to the numerical criteria shown in Table 3-3 of the previous report. The criteria are reported in Table 3-3 below.

Country	Organization	Frequency	Notes
USA	Regulator	10^{-4} /r.y	Objective
UK ⁴	Regulator	10^{-4} /r.y 10^{-5} /r.y	Limit Objective
Taiwan	Licensee	10^{-5} /r.y	Limit
Switzerland	Law	10^{-5} /r.y	Limit for new plants Objective for existing plants
Sweden	Law	Licensee 10^{-5} /r.y – level 1 studies	Objective This is a criterion or safety goal established by the licensees, for CDF from level 1 PSA's.
Slovak Rep	Regulator	10^{-4} /r.y	Objective for existing plants

⁴ 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 published in 2006.

		10^{-5} /r.y	Objective for new build
Slovenia	Regulator	10^{-4} /r.y	Objective for existing plants
		10^{-5} /r.y	Objective for new build
Netherlands	Regulator	10^{-4} /r.y	Limit for existing plants
		10^{-6} /r.y	Limit for new plants
Italy	Regulator	10^{-5} to 10^{-6} /r.y	Objective
Hungary	Regulator	10^{-5} /r.y	Objective
France	Regulator	10^{-6} /r.y	Objective related to shutdown state
France/Germany	Designers of EPR	10^{-6} /r.y	Objective
Finland	Regulator	10^{-5} /r.y	Objective for new build
Czech Rep	Licensee	10^{-4} /r.y	Objective for existing plants
		10^{-5} /r.y	Objective for new plants
Canada	Regulator	10^{-5} /r.y	Limit for new plants
	Licensee	10^{-4} /r.y	Limit for existing plants
		10^{-5} /r.y	Objective for existing plants

Large Early Release Frequency

The change compared to the last report is the definition by Slovenia of numerical criteria. For other countries, there is no change to the numerical criteria shown in Table 3-4 of the previous report. The criteria are reported in Table 3-4 below

Country	Organization	Risk metric	Frequency	Notes
UK	Regulator	10^4 TBq I131, or 200 Tbq Cs137 or other isotopes	10^{-4} /yr 10^{-5} /yr	Limit Objective
		Taiwan	Licensee	Not defined
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 PSAs.
Slovak Rep	Regulator	Not defined	10^{-5} /yr	Limit for existing plants
		Not defined	10^{-6} /yr	Limit for new build
Slovenia	Regulator	Not defined	5×10^{-6} /yr	Limit for existing plants
		Not defined	10^{-6} /yr	Limit for new build
Japan	Regulator	Containment failure	10^{-5} /yr	Objective
France	Regulator	Unacceptable consequences	10^{-4} /yr 10^{-5} /yr	Objective
France/Germany	Designer of EPR	Not defined	Neg ⁵	Objective
Finland	Regulator	100 TBq Cs137	5×10^{-7} /yr	Objective for new builds
Czech Republic	Licensee	Not defined	10^{-5} /yr	Objective for existing plants

⁵ The aim is that the sequences that lead to a large early release should be “practically eliminated”.

			10^{-6} /yr	Objective for new plants
Canada	Regulator	100 TBq Cs137	10^{-6} /yr	Objective for new plants
	Licensee	>1% Cs137 >1% Cs137 \	10^{-5} /yr 10^{-6} /yr	Limit for existing plants Objective for existing plants

Other criteria

In one country, criteria relating to the risk to workers from accidents have 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 five dose bands.

Interesting complementary safety goals (new) are to require a minimum conditional probability between CDF and LRF, in order to ensure defence-in-depth (USA, Taiwan), to use a containment failure frequency (Japan), or to define a Small Release Frequency (SRF) in addition to LRF (Canada).

Table 3-3 below lists other risk criteria.

Country	Organization	Risk metric	Frequency	Notes
Canada	Regulator	Small release Frequency (> 10^{15} Bq of I-131)	$< 10^{-5}$ /r.y	Objective for new builds
Japan	Regulator	Containment failure frequency	$< 10^{-5}$ /r.y	Objective
UK	Regulator	Frequency dose targets for accidents	BSL's and BSO's are defined by Effective dose intervals	Defined for any person on the site as well as for any person off the site

Risk increases

There are no changes from the previous report. Numerical criteria have been defined in some countries for the acceptable increases in risk from plant changes or outages during maintenance and repair. These follow the guidance given in Regulatory Guide 1.174.

Open issues

As noted previously the differences in the numerical safety criteria that have been defined in the countries included in the survey 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.

4. PSA STANDARDS AND GUIDANCE

The position in the member 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 led to a greater need for PSAs to be produced to a high standard so that they can be used to provide one of the inputs into the risk-informed decision making process and to the intended range of PSA applications. This requires the PSA to be based on the as-built/ as-designed plant, have an adequate scope, methodology and data, take account of operating experience, etc. In addition, for countries with a number of power plants, there is a need to ensure that the set of PSAs being produced is consistent.

The requirement to improve the quality of the PSAs being produced has led to a greater level of effort being applied to the development of PSA standards and guidance in the member countries and the replies received indicated that there have been many examples of developments in this area since the previous report was published.

From the replies received, the way that the member countries have approached the development of the PSA standards and guidance falls into four broad categories as follows:

National standards and guidance have been/ are being developed for the production and/or the regulatory review of the PSA. This is the case in 4 of the 21 countries.

High level requirements and guidance have been defined by the regulatory body and the PSAs have been produced to take account of these requirements and guidance. In general, these are less prescriptive than the national standards and guidance included in the previous category and give the requirements that the PSA needs to meet but does not specify how to meet them. This is the case in 4 of the 21 countries.

No specific national PSA standards or guidance have been defined, and the methods used have been developed by the utilities and accepted by the regulatory body. These standards and guidance are project specific rather than national requirements. This is the case in 11 of the 21 countries.

In many countries, no specific PSA standards or guidance has been developed and there is a high reliance on what has been produced elsewhere – in particular, the PSA standards developed in the USA and the guidance produced by IAEA and NRC. This is the case in 2 of the 21 countries.

Countries with national PSA standards and guidance

In some countries, national PSA standards and guidance have been/ are being developed. This is the case in the USA, Japan, Canada and India.

In the USA, the development of the PSA standards and guidance is being supported by professional societies, the industry and the Nuclear Regulatory Commission (NRC) and includes the following:

The American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) have jointly produced a 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, internal hazards (such as fire and flood) and external hazards (such as seismic events and external flood). This PSA

standard is being extended to cover low power and shutdown conditions, new light water reactors and, in the longer term, Level 2 and Level 3 PSA and the PSA for non-light water reactors.

The Nuclear Energy Institute (NEI) has produced peer review guidance for a PSA with the same scope as the ASME standard.

There are many sources of guidance on specific aspects of PSA such as the modelling of common cause failure and human reliability analysis given in the NUREGs published by NRC. In addition, NRC has produced a Regulatory Guide (RG 1.200) on one acceptable approach for determining the acceptability of a PSA which endorses the consensus standards and guidance for PSA and the peer review of PSA.

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**, the Nuclear and Industrial Safety Authority (NISA) and the Japan Nuclear Energy Safety Organisation (JNES) have produced guidance for risk-informed regulation which includes guidelines for the use of risk-information in the safety regulation of nuclear power plants and on PSA quality. In addition, guidelines have been produced for PSA quality which give 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, PSA standards and guidance has been produced by academic societies or the nuclear industry and is being endorsed by NISA. This includes the PSA Procedure Guide produced by the Nuclear Safety Research Organisation (NSRA) and the PSA Standard being produced by the Atomic Energy Society of Japan (AESJ) which addresses: Level 1, 2 and 3 PSA for internal events during power operation and shutdown conditions; PSA for seismic events; parameter estimation for PSA; and guidelines for risk-informed applications.

In **Canada**, the Canadian Nuclear Safety Commission (CNSC) has produced a number of regulatory policy documents, standards and guides. This includes a regulatory standard on PSA for nuclear power plants which sets out the requirements for a plant specific Level 2 PSA. CNSC is also in the process of producing the associated guidance on the PSA requirements for specific applications. In addition, the utilities have produced their own PSA standards and guides that are included as part of the company's management system. Their scope 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 addition, standards and guidance have been produced for: the reliability programme that needs to be implemented at nuclear power plant; and the use of cost-benefit information in safety decision making.

In **India**, the Atomic Energy Regulatory Board (AERB) is in the process of adopting a risk-informed approach and has produced the following guidance on PSA: a manual on the approach and methods for carrying out a PSA; a compendium on data for use in the PSA; a compendium for carrying out the human reliability analysis included in the PSA; and guidance for the regulatory review of a PSA. These all take account of international standards and practices.

Countries where high level requirements have been produced by the regulatory body

In some countries, high level requirements and guidance have been defined by the regulatory body and the PSAs that have been produced have taken account of current international standards and guidance. This is the case in the UK, Korea, Germany and Switzerland.

In the **UK**, no national PSA standards or guidance has been produced. The Office for Nuclear Regulation (ONR) has produced high level requirements for the PSAs for nuclear facilities in its Safety Assessment Principles (SAPs). These are supported by the Technical Assessment Guides (TAGs) which give more detailed guidance to assessors on PSA in general and on specific aspects of PSA such as common cause

failure, structural failure, severe accidents, and the modelling of computer based systems and passive systems. The current PSAs have been developed to meet these high level requirements. The methods used have been based on international practices relevant to the reactor types in the UK and these PSAs have been peer reviewed against international standards by a team of international experts commissioned by ONR.

In **Korea**, the Korean Institute of Nuclear Safety (KINS) has produced guidelines on the regulatory review of Level 1, 2 and 3 PSA, and for the use of PSA in risk-informed decision making on safety issues such as making changes to the technical specifications. In addition, regulatory guidance is being produced on PSA quality. The current PSAs have been reviewed against current international standards and guidance.

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. The aim of updating the guideline was to extend the scope of the PSAs and to help to make the PSAs for different plants more comparable.

In **Switzerland**, the Swiss Federal Nuclear Safety Inspectorate (HSK) has produced 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.

Countries where the utilities have developed the PSA methods

In some countries, where there are no specific national standards or guidance, the utilities have developed their own PSA methods and guidance that reflect current international standards and practices as defined in documents published by IAEA, NEA and NRC. In many cases, these methods have been endorsed by the regulatory body. 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. This is the case in France, Finland, Sweden, Spain, Slovenia, the Slovak Republic, the Netherlands, Mexico, Belgium, Hungary and the Czech Republic.

It is usually the case is that the PSA is produced and the regulatory review carried out in a way that reflects international standards and current practice. This typically includes the IAEA Safety Standards, the PSA standards produced by ASME/ ANS and NEI, and the guidance available in the NUREGs produced by NRC. One difference is that the ASME/ ANS standard defines three capability categories for PSA. However, this distinction is not made in other countries.

In **France**, the acceptable methods for PSA developments and applications have been defined in the Safety Rule. This is based on the PSAs that were carried out for the 900 MWe and 1300 MWe plants which were carried out by two independent teams – the Institut de Radioprotection et de Sûreté Nucléaire (IRSN) and Électricité de France (EdF) respectively. A detailed mutual external review was carried out and this has led to important improvements in the quality of the PSA and this is reflected in the Safety Rule.

In **Finland**, the requirement for a PSA is given in the Nuclear Energy Decree and the licensees have developed their own PSA guidance independently. In addition, there are a number of national research activities on PSA development.

In **Sweden**, the required quality of the PSA is specified in national regulations. This is supported by the guidance produced by the Swedish Nuclear Power Inspectorate (SKI) on: the review of PSA; fire frequencies; and the treatment of external hazards, which are based on research that has been carried out. A Review Handbook for PSA has been produced that gives guidance for the regulatory review of a PSA.

In **Spain**, the Nuclear Safety Council (CSN) has produced regulatory guidance for carrying out a PSA that captures the experience gained in the reviews of the existing PSAs.

In **Slovenia**, the required scope and quality of the PSA is set by a new regulation. There are no other standards or guidelines related to PSA.

In the **Slovak Republic**, the Nuclear Regulatory Authority (NRA) has produced guidelines for carrying out a PSA, for the regulatory review of the PSA and for its use in risk-informed decision making.

In the **Netherlands**, the PSA methods used have been developed as the analysis carried out by external contractors has proceeded. The PSA produced have been subjected to IPERS/IPSART reviews by IAEA peer review teams and the feedback received has been used to further refine the PSA methods. The regulatory body - the Ministry of Housing, Spatial Planning and the Environment (VROM) – started to produce a PSA procedures guide but this was not completed and the current approach of using competent analysts and subjecting the analysis to IAEA peer reviews is preferred.

In **Mexico**, the PSAs have been based on international guidance produced by IAEA and NRC. However, the National Commission for Nuclear Safety and Safeguards (CNSNS) has started to develop guidance for the review of a fire PSA and have produced two regulatory guides for the use of PSA results in a risk-informed decision making process.

In **Belgium**, the methods for the main PSA tasks have been defined within the PSA project and this has taken account of international guidance.

In **Hungary**, the requirements for a PSA are given in the Nuclear Safety code. The methods used for the PSAs carried out have been defined during the course of the analysis and is based on international guidance.

In the **Czech Republic**, the methods used have been defined within the PSA projects and are based on international guidance. In addition, project guidelines have been developed on particular PSA topics. The Czech Regulatory Body (SUJB) has developed a policy for a risk-informed approach to regulatory decision making and instructions for the use of the PSA.

No standards and guidance on PSA

In some countries there are no national standards or guidance on PSA. This is the case in **Chinese Taipei** where the regulatory reviews of PSA have been carried out using the NEI guidance and in **Italy** where the PSAs that have been carried out have been based on IAEA guidance.

5. STATUS AND SCOPE OF PSA PROGRAMS

In recent years the scope of PSAs has expanded, due to an important increase of PSA applications (e.g. RIDM). Moreover in the field of new plants, PSA requirements are increasing, with a wider and more formalised scope.

The PSA scope is defined by:

- The categories of Initiating Events (IE) taken into account, (internal IE, internal and external hazards)
- The states of the plant considered (full power, low power and shutdown states)
- The nature of consequences assessed: in a Level 1PSA the consequence assessed is the Core Damage Frequency (CDF), in a Level 1+ PSA the CDF sequences are grouped with a view on containment function status, a Level 2PSA provides the frequency and level of releases outside of the containment and a Level 3PSA provides the frequency of harm to the public and the environment. These different levels are in fact the successive extension of the study to additional problems.

PSA level

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. However, there has been an apparent tendency to move towards more complete Level 2 PSA, with the definition of several releases categories.

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. Level 3 PSA for few plants are also mentioned by USA, UK and Japan (Japan indicates a Level 3 seismic PSA).

Scope of initiating events

More and more, the PSAs have been (or are being) extended to consider low power and shutdown events. Examples include nearly all the countries for Level 1PSA, and some examples for Level 2PSA. Some new examples are the use of PSA for the analysis of the spent fuel pool (France, Hungary), for plants decommissioning (Finland, Slovakia), and for fuel handling (UK).

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, although some complete seismic PSAs have been developed (Japan, Switzerland).

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 have been or will be updated as part of the periodic update of the PSAs.

The general level/scope of PSA practice is indicated in Table 5.1 below. Further detail is also provided in Appendix A which shows the situation by plant in each country.

PSA updating

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. For example in Hungary the update is made annually to ensure usefulness and credibility of PSA results for applications.

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 the regulatory body. Several countries require that a living PSA be maintained (e.g., Finland, Korea, and Switzerland).

Generally speaking there is an increase in PSA applications, which need a PSA reflecting the as-built, as-operated and maintained plant, and all the countries work towards this objective.

PSA for new plants

In the case of new plants it appears clearly that, for all the concerned countries, the PSA requirements are increasing, they are more complete and more formal. The required scope is generally a Level 2 PSA, covering internal and external events and all the plant operating states.

TABLE 5.1: General level/scope of PSA practice – overview

	At-Power		LPSD	
	Internal Events	External Events	Internal Events	External Events
Level 1				
Level 2				
Level 3			?	?

	All
	Most
	Rather few
	Few

6. PSA METHODOLOGY AND DATA

Introduction

PSA has been carried out, at least Level 1 PSA (internal events), by most of the countries. However, there is an increasing trend in extending Level 1 PSA to Level 2 and in some cases to Level 3 PSA. Also, there is noticeable interest in member countries to include low power and shutdown states, and external events within the scope of PSA projects. It is also recognized that the approach used for PSA, the level of details and the scope of PSA need to be consistent with the PSA applications under consideration (see chapter 7). Since the methodology followed and data used forms a core component of a PSA study, there is a trend towards harmonization and standardization of these aspects of PSA.

In respect of the following discussions, PSA methodology highlights the “methods”, “models” and the “tools” adopted while carrying out the analysis. Method describes the procedural steps involved in the overall PSA methodology. Models are the approach followed in performing the intermediate tasks involved in the particular step of the selected method. Tools are the software packages used in the quantification task in the PSA methodology.

General PSA methodology

PSA general methodology is broadly similar, in terms of the general fault tree event tree approach, to what was presented in the previous report, and even to what was done in the very early PSAs as WASH 1400.

PSA modelling requires extensive knowledge of plant design, operation, maintenance and data. Although it is difficult to really appreciate through the countries replies, it appears that the level of detail is variable, depending on the objectives of each study.

There are some aspects which are essential to ensure the quality of PSA. These include: a quality assurance programme, which covers all the steps of the PSA, and is generally developed; and an independent peer review.

Level 1 PSA methodology

Level 1 PSA methodology appears as mature and similar for all the countries. A general framework for carrying out Level 1 PSA is given in IAEA-SS-50-P4 [1] and NUREG/CR-2300 [2]. In addition, national guidelines are also used, if available. The event tree/fault tree linking approach is more common for the Level 1 PSA. The major steps for carrying out Level 1 PSA includes: (1) Plant familiarization (2) Selection and grouping of initiating events (3) Definition of core damage and system success criteria (4) Development of event trees and qualitative assessment of accident scenarios (5) Failure mode and effect analysis and system modelling (6) Data collection and assessment (7) Treatment of CCFs and HRA (8) Initial quantification (9) Uncertainty, sensitivity and importance analysis (10) Final quantification (including verification), and (11) Documentation and presentation of results.

Usually a fault tree approach, backed by a detailed failure mode effect analysis, is used for system reliability modelling safety support systems. Details of system architecture (e.g. redundancy, diversity etc.) are considered in modelling the system.

The Risk Spectrum, ISOGRAPH, CAFTA and WinNUPRA computer codes are widely used in developing Level-1 PSA models in addition to some in-house developed computer codes such as SPSA/Fin PSA (Finland), FTREX (Korea) etc.

Level 2 PSA methodology

The Level 2 PSA methodology is more variable, notably with very different numbers of Plant Damage States. A general framework for carrying out Level-2 PSA is explained in IAEA-SS-50-P8 [3] and NUREG-1150 [4]. In addition, national guidelines are also used, if available. The event tree approach is generally used for level-2 PSA. However, fault trees may also be needed to assess the availability of the containment related engineered safety features while developing the accident progression event tree (APET)/containment event tree (CET). The major steps for carrying out level-2 PSA includes: (1) Re-visit Level-1 PSA and grouping of plant damage states (2) Definition of source term and release categories (3) Development of APET/CET including modelling of physical phenomena (in-vessel and ex-vessel) in qualitative assessment of accident scenarios (4) Failure mode and effect analysis and containment system modelling (5) Assessment of source term and release frequencies (6) Uncertainty, sensitivity and importance analysis, and (7) Documentation and presentation of results.

The MAAP and MELCOR computer codes are widely used for Level-2 PSA. Other codes such as Source Term Code Package (STCP), Code for Analysis of Thermal Hydraulics during Accident of Reactor and safety Evaluation (CATHARE), and Accident Source Term Evaluation Code (ASTEC) are also in use.

There is some trend to extend the level 2 PSA study to a level 3 PSA to have an assessment of consequences in terms of health effects to members of public and to assess the requirements of the counter measures. Simulation based accident consequence analysis has been suggested for carrying out level 3 PSA.

Integrated approach for Level 1 and Level 2 PSA

Integrated approach for Level 1 and Level 2 PSA is gaining popularity since it circumvents the difficulty in grouping the core damage states into plant damage states. There are wide variations in the number of plant damage states and the number of attributes for PDS, number of source terms, and number of release categories in Level 2 PSAs. The nodal questions in APET/CET address the severe accident phenomena such as high pressure melt ejection, direct containment heating, steam explosion, hydrogen detonation and deflagration, and molten core concrete interactions.

Initiating events

The identification, selection and grouping of initiating events are always considered as an important step in the PSA. Different approaches are mentioned such as existing generic IE list for a specific NPP design, engineering analysis, deductive analysis like master logic diagrams, and operating experience.

For initiating event frequency estimation, generic, data operating experience, and generally a combination of both using Bayesian updating is employed.

Success criteria

For accident sequence analysis, and when explicitly mentioned in the reports, conservative success criteria derived from safety analysis reports are generally followed. However, the uses of realistic

success criteria have also been suggested by some countries (for both Level 1 and Level 2 PSA) provided the supporting deterministic analyses are carried out.

Component failures data

Plant-specific data is given utmost importance and systems for plant data collection have been set up in many countries. Some of the PSAs that have been carried out used generic sources such as NUREG/CR-6928 [7], Sweden's T-book, proprietary databases such as EQE International, SAIC, IAEA TECDOC-478 [8], etc. Two common approaches are classical or frequentist method and Bayesian estimation. To differentiate between these two methods, it is required to define event, observations and parameter estimates: event is the possible outcome of the stochastic process; observation is the realization of an event; and parameter estimates refer to inferring the properties of the observation. In a classical method of data modelling, we are looking into the observations, for e.g. r failures in n tests. When such empirical data is sparse, Bayesian methods are applied which can capture a wide variety of data such as expert judgement in addition to statistical data. In a Bayesian framework, analyst uncertainty in data is expressed as a probability distribution. A two stage Bayesian approach is generally used to revise the data, which updates generic data with plant specific information.

Common Cause Failures

Functional and physical dependencies are included in PSA models. Most of them are explicitly modelled in fault trees. Those which are not considered explicitly are modelled with Common Cause Failure models. Typically screening Common Cause Failure (CCF) analysis is used at the preliminary stage, and more detailed model such as α – factor and Multiple Greek Letter (MGL) model are used for the dominating CCF groups in PSA. Practitioners also employ the Unified Partial beta-factor Method (UPM) approach to derive β factors, which concentrates on defences against CCFs and employs judgments for relative weighting of CCF influence factors. CCF parameter data often come from generic sources (such as NUREG/CR-6268 [5]) and plant specific experience. Data from the OECD/NEA International Common-cause-failure Data Exchange (ICDE) project are sometimes considered to estimate CCF probabilities and CCF parameters.

Human Reliability Analysis

Human Reliability Analysis address three categories of human errors: Category A –Pre-initiating events from maintenance and test induced, Category B- leading to initiating events and Category C- Post initiating events. Traditional methods employed are Technique for Human Error Rate Prediction (THERP) [6], Accident Sequence Evaluation Program (ASEP), Human Cognitive Reliability (HCR) for identification and quantification of human errors. In addition, other methods such as MERMOS, the Human Error Assessment and Reduction Technique (HEART)/ Nuclear Action Reliability Assessment (NARA) and A Technique for Human Error aNalysis (ATHENA) have been developed and are used in particular countries.

The new methods are now presented as tools for application (and not only research).

Sources of human error data are from simulator information, field observation, interviews with operators and expert judgment, etc.

All of the PSAs 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. The lack of models for considering safety culture/ organizational factors in PSA is seen as a difficulty or limitation of many of the PSAs that have been produced.

In order to improve the knowledge about HRA, WGRISK has carried out several tasks during the past years. Recently, a WGRISK task group has produced a report summarizing the outcome of a workshop on the use of training simulators for collection of HRA data [5].

External events

Treatment of external events needs special attention.

An increased development of fire PSAs appears in the countries' answers. Some countries carry out fire PSA using Fire Induced Vulnerability Evaluation (FIVE) methodology.

For seismic events, often PSA based Seismic Margin Assessment is carried out in place of full seismic PSA, with the objective to show that High Confidence Low Probability of Failure (HCLPF) of the plant is higher than review level earthquake. In some cases (Japan, Switzerland) a complete seismic PSA is carried out.

Shared systems

Concern is expressed in a number of the country responses on how shared systems are treated in PSA. Examples are provided by Korea and Japan, and the topic is mentioned by Canada, Belgium and France. Two possible approaches for addressing this issue are: (i) Evaluating the initiating event frequency, which puts demand on the shared system to serve more than one unit simultaneously and (ii) Evaluating the system unavailability of the shared system considering the possibility of its use in the other unit. Typical practice is the second approach, in which the probability of the shared system being unavailable to the unit under consideration due its use in the other unit at a time is calculated. The original system unavailability of the shared system is modified using this probability. This modified unavailability value can be used in the quantification of the originally developed accident sequences. Usually technical specification requirements ensure that when a shared system is in use in one unit, all other unit(s) are brought to a safe shutdown state. This eliminates the possibility of simultaneous requirement of safety systems in multiple units. However, a consensus model needs to be evolved for the treatment of shared systems in PSA.

Issues

There are three other issues highlighted in the country responses that need to be addressed in PSA, especially in extending it for new and advanced reactors: (i) the need for including passive system reliability analysis (ii) models for reliability analysis of digital systems and (iii) lack of models for considering safety culture/ organizational factors in PSA.

The modelling and quantification of digital I&C, considered as a very important issue especially for new plants, is an area of increasing importance. Several countries have significant activities relating to this problem (USA, Korea, Japan, India, France). WGRISK has identified a number of key technical issues [6] and currently has a task group developing a failure mode taxonomy for digital I&C systems and guidelines for the use of the taxonomy.

Another issue with new developments is the problem of passive system reliability. This problem is related to the progress of advanced designs, e.g. Sodium Cooled Fast Reactors. Examples are given by Italy, Japan, USA and France.

In addition, the necessity for arriving at appropriate risk metrics for advanced reactors need to be examined. However, this needs a careful interpretation of the definition of Core Damage Frequency.

7. PSA APPLICATIONS

Summary

PSA is used as a decision support tool to enhance a plant's design and operation. The benefits of such applications are of two types:

- Safety benefits with measured risk reduction or improved safety focus; and
- Operational benefits with plant flexibility or complexity reduction.

In a risk informed decision process, PSA insights are used together with other relevant information such as engineering judgment or regulatory requirements. The decisions must be made so that defense-in-depth is always assured and the safety margins are maintained.

The main application of the PSA is for design evaluation.

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; and
- determine whether the design is balanced.

This has been done during periodic safety reviews for existing plants. 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.

It is still 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 and many 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 risk.

The PSA has also been used to provide risk information in making the decisions on issues that have arisen such as: increasing the time between refueling outages; and increasing the power level of the core.

The PSA has proved to be a useful and versatile tool supporting the decision-making process in the following cases: assessing safety aspects of some backfits; and considering equipment innovations or other design or operation changes of existing plants. The review of proposed alternative options is often done as part of a cost-benefit approach. For some countries, PSA insights are also used to support life extension for existing operating plants.

Now, PSA is an important part of the design and the licensing processes of new plants. For example, for European Pressurized water Reactor (EPR) Flamanville 3, PSA contributions addressed the following items among others:

- designing and optimizing the facility during the design phase and life of the site; and
- confirm the balanced risk profile of the design.

In the USA, the Design Certification application for a light-water reactor design must contain a final safety analysis report (FSAR) that includes a description and analysis, based on PSA, of design features for the prevention and mitigation of severe accidents.

PSA is also used to enhance the management of the potential accidents and their consequences.

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 implementations of generic or plant-specific Severe Accident Management Guidelines (SAMG) to guide operators in the event of a severe accident. An example of this is the Level 2 PSA for the Bruce B NPP in Canada, which provides a framework for the development of specific SAMG. Other examples are given by Mexico and Japan, and are also presented in the proceedings of a workshop organised by WGRISK jointly with WGAMA [7].

The source terms and frequencies produced by the Level 2 PSA have been used as the basis for emergency planning. In Canada, the regulator (CNSC) is promoting the use of PSA insights in defining the strategies to cope with the consequences of severe accidents. In Mexico, PSA was used to plan the emergency scenario for the evaluation of the External Radiological Emergency Procedures.

As operators are a key element in the defense in depth, their training on emergency operating procedures (EOPs) is very important. The PSA is being used at a number of plants to provide an input into the training program 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. An example of this is the training of critical human interventions contributing to the CDF identified by unit specific PSA models for the Dukovany NPP in Czech Republic. 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.

PSA insights are important to optimize plant operation and make sure that important SSCs are properly managed.

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 program. The same approach has also been used to identify the active components that need to be given special attention as part of the program for the management of ageing. In Switzerland for example, a component is regarded as significant to safety when one of the following relations applies for CDF (core damage frequency), FDF (fuel damage frequency) or LERF (large early release frequency): $FV \geq 1E-3$ or $RAW \geq 2$, where FV is the Fussell-Vesely and RAW the Risk Achievement Worth importance measure. The guidance for combining both probabilistic and deterministic insights to group SSCs into four categories is given in the Nuclear Energy Institute (NEI) document NEI 00-04, "10 CFR 50.69 SSC Categorization Guideline." In Japan, the new inspection system for NPPs started in January 2010 introducing the following three elements: new maintenance program, root cause analysis of events, and comprehensive plant performance assessment. Importance of systems and functions reviewed on the basis of both PSA findings and deterministic considerations was ranked into class 1 to 4 and non class.

The Technical Specifications 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 countries the PSA has been used to justify and optimize the

LCOs, AOTs and STIs. The PSA has also been used to justify an exemption from a Technical Specification. PSA has been used for identifying situations in which the plant shutdown could cause higher risk than continuing power operation and fixing the failures. For example, if systems used for decay heat removal are seriously degraded (CCF), it may be safer to continue operation than to shutdown the plant immediately, although shutdown may be required by the current Technical Specifications.

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 refueling outages without leading to a significant increase in the risk. Nevertheless, the risk increase due to maintenance and test activities must be kept to an acceptable level. This is often done with use of Risk Monitors. They 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 decisions 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 rule 50.65 (a)(4). The Risk Monitors are used:

- to avoid simultaneous components unavailability that would lead to a high point-in-time risk;
- to plan the maintenance outages over a period of time to minimize 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, EOOS, and RiskWatcher. In addition, other 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 Program (ESOP) in the UK.

To optimize pipes inspection programmes, Risk-Informed In-Service Inspection is being carried out for a number of plants. Both the Westinghouse and the EPRI methodologies are being applied. The U.S. NRC has also approved RI-ISI programmes based, in part, on ASME Code Case N-716 identifying segments that are generically considered high-safety-significant (HSS). A flooding PSA is then used to identify any additional, plant specific HSS segments.

PSA contributes to plant operating experience 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. For example, the U.S. NRC uses PSA models to support decisions regarding the appropriate response to a reported incident. The value of Conditional Core Damage Probability (CCDP) is considered when determining the type of inspection team to send.

PSA results may also be used to set up performance indicators regarding plant safety. For example, the Mitigating Systems Performance Index is proposed to follow safety systems unavailability in the US plants. In Canada, the PSA model is used to derive reliability models for the important systems in order to report on the reliability of these systems.

The risk information provided by the PSA is increasingly being used by regulatory authorities in planning their activities.

This includes:

- the prioritization of inspection tasks so that they focus on risk significant issues;

- determining the significance of inspection findings; and
- the response to non-compliances.

An example of this is the Reactor Oversight Program (ROP) carried out by US NRC. Similar processes to this are carried out in other countries.

In Finland, the decommissioning-related risks are analyzed by the regulator (STUK) to ensure risk-informed NPP decommissioning.

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 pressurized thermal shock. Details of how these changes were made are given in the country responses (see Appendix B).

8. RESULTS AND INSIGHTS FROM THE PSAS

PSA results

PSA provides several categories of results: numerical results (absolute and relative results) and qualitative results (functional and physical description of accident sequences). Each category of results has its specific interest and applications. For example absolute numerical results are necessary for an overall safety assessment and comparison with safety goals, while relative numerical results provide an identification of dominant risk contributors and a hierarchy of potential safety improvements.

Numerical results

Absolute values

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 are also some considerations about the fact that the risk is decreasing, due to safety improvement. It is often mentioned that PSA confirms a balanced design, and also that the results confirm the improved safety level of the new plants.

The results of Level 1 PSA for internal initiators are generally given clearly, and the values are rather consistent (very roughly 10^{-3} to 10^{-5} per reactor year for existing plants, according to the age of the design and to the number of safety improvements). It is more difficult to appreciate the results corresponding to low power and shutdown states and to external hazards (partial or relative values are often provided), and moreover the updating of the studies are different. The Level 2 PSA results are still more difficult to appreciate: simple metrics of LERF or LRF are generally given, but often it does not correspond to the same scope of initiating events, and more complete results with several release categories depend very much on the specific methodology of the countries.

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 particularly outstanding is the high contribution of internal and external hazards. It can be noted among others:

- Fire (USA, Finland, Germany, Hungary)
- Earthquake (Japan, 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 the identification of 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. The results of a WGRISK task group examining current treatments of non-seismic external events are reported in [8].

It has also to be noted that Low Power and Shutdown situations contribute significantly in several results. The results of a WGRISK task group in this area are reported in [9].

Safety improvements

Another particularly interesting result of this survey is the identification of plant 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. 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, there are many examples of modifications aiming to reduce human errors (procedures, signals, automatisms, etc.), many improvements relating to electrical problems and 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 (many examples); and
- All the parts of PSA are used for safety improvements: Level 1 PSA, Level 2 PSA, 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 to support important safety decisions. Although it is often mentioned that PSA was not the only input for a safety decision (a modification can be identified by a deterministic approach and confirmed by PSA), PSA is considered as a key contributor to decision making.

9. FUTURE DEVELOPMENTS AND RESEARCH

The aim of the PSAs currently being produced is to provide estimates of the core damage frequency, large (early) release frequency or the societal risks for a nuclear power plant. The overall approach to doing this, in terms of a fault tree event tree approach, is broadly similar to what was done in the very early PSAs such as the WASH1400 and the Zion-Indian Point studies.

However, since these PSA were produced, many improvements have been made which include better PSA software for the development and quantification of the PSA model, the collection of data from the operation of nuclear power plants and its use to support the quantification of the PSA and specific aspects of the analysis such as the modelling of common cause failure and human error. In addition, further developments are proposed in the longer term such as the application of dynamic PSA which provides a more detailed model of the fault sequences that can occur.

There is still a high level of development and research activities being carried out in the member countries. Since the previous report was published, progress has been made on a large number of topics which includes the following:

- Development of PSA methods;
- PSA for internal hazards;
- PSA for external hazards;
- Common cause failure modelling;
- Human reliability analysis;
- Reliability data collection;
- PSA for passive systems;
- Reliability of digital systems;
- Level 2 PSA;
- Level 3 PSA;
- Uncertainties;
- Modelling of ageing in PSA;
- Fuel route PSA; and
- Use of PSA in risk-informed decision making (RIDM).

Development of PSA methods

In all countries, the PSAs are being developed to take account of changes to the design of the plant (such as the addition of safety systems), changes to the operation of the plant (such as the use of fuel with a higher enrichment), changes to the understanding of how the plant behaves in accident conditions (from new thermal-hydraulic analysis), changes in the data for the plant (including new component failure rate data, initiating event frequencies and common cause failure probabilities from generic and plant specific data collection), improvements in modelling (such as the application of new techniques for human reliability analysis), the scope of the PSAs are being extended (to include further initiating events and modes of operation, and to produce Level 2 and Level 3 PSAs), etc. In general, the PSAs are being maintained as Living PSAs that are updated regularly to take account of any changes.

In a number of countries, efforts are being made to improve the quality and realism of the PSAs produced for nuclear power plants so that they provide an accurate model of how the plant behaves in accident conditions.

In the **USA**, the PSAs are being developed to meet the consensus standards and regulatory guidance that has been produced for PSA (see Chapter 4). As a result of this, it is expected that improved and more complete PSA models will be produced and will be reviewed and approved by NRC. In addition, work is being carried out on the use of phenomenological models in PSA and a review is being carried out of the success criteria used in NRC's SPAR models.

In the **UK**, the focus has been to improve the existing PSAs and this includes research activities to support future PSA scope enhancements, improve the realism of the PSAs and make them suitable for a wider range of applications.

In **Switzerland**, work is being carried out on the harmonization of the PSAs in order to make the PSA results more comparable and on reducing the uncertainty in some selected fields.

In **France**, there has been a high level of activity in EDF and IRSN to develop the methodologies to be used in the PSAs for the various reactor types. In particular, the methodologies are being developed and applied for fire PSA, seismic PSA, Level 2 PSA and the PSA for new reactors.

In **Korea**, work is being carried out to develop the PSA methodology and the Online Consolidation & Estimation Analyzer for Nuclear System (OCEANS) PSA software. The aim of the software is to provide: a means of producing an integrated full scope PSA; easy and fast quantification; and traceability and reproducibility of the analysis. The software has a number of modules which carry out the functions required for the development of the integrated PSA model and its quantification. In addition, the PSA software is being developed to: provide an exact solution of a fault tree model using the Binary Decision Diagram (BDD) algorithm; introduce Conditional Gates to take account of the same fault trees in different parts of the model where the boundary conditions are different; and present the PSA information in a coherent way.

In **Germany**, the focus for developing and enhancing PSA methods is on the reliability of software based digital I&C, combinations of external and internal hazards, Dynamic PSA (Level 1 and 2), and the consideration of severe accidents inside spent fuel pools for PSA Level 2.

PSA for internal hazards

Work is being carried out in a number of countries to extend the scope and accuracy of the PSAs carried out for internal hazards.

In the **USA**, work is being carried out in a number of areas of fire PSA which includes: improving the guidance given in NUREG/CR-6850 that would lead to more realistic results being obtained; updating the fire events database; developing methods for fires arising during low power and shutdown conditions; and carrying out HRA for inclusion in the fire PSA. In addition: a verification and validation study of a number of fire models has been carried out; a Phenomena Identification and

Ranking Table (PIRT) exercise has been carried out to identify needed fire modeling capabilities; and a simple cable damage model has been developed for use in general purpose fire models.

In **Japan**, fire severity factors have been defined using fire simulation codes and fire experiments. These have been used in the PSAs for a typical BWR and PWR during power operation and shutdown conditions.

In **Germany**, fire PSA methodology has been enhanced and extended to low power and shutdown states. In particular, the screening process has been significantly improved and generic data from the OECD FIRE database are being applied for plant specific event trees. Additional activities are ongoing with respect developing an approach no longer based on compartment specific but component specific screening.

PSA for external hazards

In many countries, the PSA scope is being increased to include a wide range of external hazards including natural hazards (such as seismic events and extreme environmental conditions) and man-made hazards (such as aircraft crash).

In the **USA**, work is being carried out in a number of areas related to external hazards as follows: to characterise the seismic sources in particular regions and to develop state-of-the art ground motion prediction equations; to develop practical guidelines for implementing the Senior Seismic Hazard Analysis Committee (SSHAC) framework for performing a probabilistic seismic hazard analysis; to develop models for tsunami generation and propagation and explore probabilistic tsunami hazard assessment methods; and to develop models for extreme precipitation and storm surge.

In **Japan**, a set of methodologies has been established for seismic risk analysis of all types of reactors. The work carried out has included: the evaluation of the seismic hazard curves for typical nuclear power plant sites; the development of seismic fragility data based on structural analysis and shaker table tests to find the functional failure limits and failure modes of components; and updating the seismic PSA methodology and extending it to address shutdown modes. In addition, a preliminary study has been carried out on PSA methods for external events other than seismic and fire. This aim is to propose a screening methodology to identify external events for which detailed examinations of hazard and/or plant fragility are necessary.

In **France**, a preliminary feasibility study for a seismic PSA has been carried out and the development of the methodology is ongoing.

In **Finland**, sea level scenarios along the Finnish coast have been developed. This takes into account thermal expansion, melting of glaciers, local land uplift and the water balance in the Baltic sea.

In **Germany**, methods for seismic PSA based on site specific SHA (seismic hazard analysis), have been developed. Enhancements of the approach considering also combinations of seismic with other hazards are ongoing.

Common cause failure modeling

A number of countries are contributing to the various data campaigns being organized by the International Common Cause Failure Data Exchange (ICDE) and this data is increasingly being used to support the modeling of CCF in PSAs.

In **France**, part of the goal of the work on CCF is to develop a method that is able to cover all possible situations including those when the EDF experience feedback show no evidence of common cause events. Also, in **France**, a method has been developed with EPRI to assess the adequacy and the potential impact of modeling inter-system CCFs. The pilot studies carried out so far show that the impact is negligible in comparison to intra-system CCF.

In **Germany**, methods for modeling CCF have been enhanced to consider CCF consistently and systematically in PSA,

Human reliability analysis

In the **USA**, work is being carried out to identify a single method to perform HRA for NRC applications or guidance on which method(s) should be used in which circumstances. The approach being followed incorporates behavioural science knowledge by providing decompositions of human failures, failure mechanisms and failure factors that reflect both PSA-relevant contextual information and findings from scientific papers documenting theories, models, and data of interest. For quantification, the project uses a conventional PSA conditional probability framework, delineated to a level adequate for associating the probability of a human failure event with conditional probabilities of the associated contexts, failure mechanisms, and underlying factors (e.g., performance shaping factors).

In the **UK**, work has been carried out to improve the Human Error Assessment and Reduction Technique (HEART) so that it can be applied more easily to nuclear power plant tasks and takes account of recent research and operating experience data. The outcome has been the formulation of the Nuclear Action Reliability Assessment (NARA) method which uses the same approach as HEART to derive the Human Error Probabilities (HEPs) for specific tasks. It includes an additional functionality that relates to the tasks which can be carried out in an extended timescale (which is the case for loss of decay heat removal for the AGRs where the timescale to restore core cooling is long/ many hours).

In **Switzerland**, work is being carried out to quantify decision-related errors, in particular for errors of commission (EOCs). 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 its trial use, the method is now being revised and user guidance is being prepared.

In **Korea**, a method has been developed for modelling human errors during test and maintenance activities since they have made a significant contribution to unplanned reactor trips. The m-HRA method has been developed for identifying and assessing human errors while performing test and maintenance activities. This provides qualitative predictions of possible human error modes and quantitative estimates of their probabilities. The method is based on the basic error characteristics and performance shaping factors (PSFs) associated with specific error modes, which have been drawn from in-depth analysis of operating experience and a literature survey on maintenance activities.

In addition, in **Korea**, a HRA method has been developed that is capable of modelling the human errors that occur in the Main Control Room (MCR) which incorporates many computer-based systems – referred to as the d-HRA method. This is based on extensive studies which included observation and investigation of operator behaviours in an advanced control room, task analysis and task performance analysis, analysis of error types and performance shaping factors (PSFs). It was found that computer-based control rooms can provide more effective error recovery features than conventional control rooms and there are new PSFs that arise for computer-based procedures and soft controllers.

In **Japan**, there are a number of activities related to HRA which includes the collection and analysis of human behaviour data by the utilities at their training centres.

In **Hungary**, work is being carried out to develop HRA methods that represent human behaviour more accurately 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 aim 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. In addition, data collection and analysis systems are being set up to identify the strengths and weaknesses in human performance and provide an input into the HRA.

In **Finland**, work is being carried out to support the Nordic-German project EXAM-HRA which aims to provide guidance on performing HRA based on a survey of current practices and to contribute to method development in the area of performance shaping factors (PSFs) for contextual HRA. Also in

Finland, work is being carried out on the development and use of a method for modelling HRA in fire scenarios. The existing fire-HRA method will be further developed and applied to a cable tunnel scenario.

In **France**, work is being carried out to extend the scope of the scope of MERMOS which is the reference method used by EDF for HRA.

In **Germany**, a methodology for considering safety significant knowledge based actions in PSA has been developed. It is now possible to quantify the safety significance of organizational factors and of the safety management in the PSA model. Also in **Germany**, activities are ongoing to implement human actions and their reliability in fire PSA by modeling via a Dynamic PSA approach (with MCDET).

Reliability data collection

In many countries, work is being carried out to collect and to analyze operating experience data that can be used in the quantification of reliability parameters for PSA analysis.

In the **USA**, NRC is routinely collecting and analysing operating experience data. This includes the Human Event Repository and Analysis (HERA) database which includes HRA-relevant information from a variety of sources such as nuclear power plant operational events and simulator experiments. This includes a data framework aimed at addressing the issues of sparse and imperfect empirical data. In addition, the fire events database is being updated and this will now include an expert elicitation effort aimed at developing probabilities for fire-induced electrical short circuits in direct current cables.

In **Japan**, component reliability data for commercial light water reactors is being collected by the utilities. This data is stored and a statistical analysis carried out centrally.

In **Hungary**, work was carried out to update the component reliability data base of the Paks. This included the collection of operating experience data from the site. This data was used in a Bayesian approach to combine it with generic failure data for initiating events as well as mechanical and electrical components.

In **France**, EDF have set up a specific organization 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 addition, many countries are continuing to provide data to the OECD data collection systems such as the International Common Cause Failure Data Exchange (ICDE), the OECD Fire Incident Records Exchange (OECD FIRE) and the OECD Piping Failure Data Exchange (OPDE).

In **Germany**, methods for uncertainty analyses of, in particular, epistemic uncertainties have been enhanced.

PSA for passive systems

In a number of countries, the PSA methods are being developed for modelling passive systems in the PSA. This is particularly important for new reactors where more passive systems are being incorporated in the design.

In **Japan**, this is being done as part of development project of the Japan sodium-cooled fast reactor (JSFR) which incorporates passive systems for rapid reactor shutdown and decay heat removal using natural circulation. This is done by combining the sensitivity analysis on plant transient response with evaluation of uncertainty factors of various design parameters such as SASS actuation temperature, coolant flow rate halving time of flow coast down, etc.

In **Finland**, a review is being carried out to identify the passive safety systems included in current or planned reactors, in what scenarios they are claimed, how they affect safety and how they have been analyzed in the past. This is linked to the work on Dynamic Level 2 PSA

In the **USA**, phenomenological models for material degradation are being developed to support risk-informed decision making. This includes work aimed at assessing the probability of rupture for reactor coolant system components and at supporting life extension for operating plants.

In **Germany**, existing methods for estimating leak and break frequencies for pressurized components have been extended and enhanced. Activities on developing a first approach for modeling the reliability of buildings structures are ongoing.

Reliability of digital systems

There is an increased use of digital systems to carry out the control, instrumentation and protection functions and to provide information to the plant operators and they need to be modelled in the PSA. However, there are no widely accepted methods for including software failures of real-time digital systems into current generation PSAs. This is the subject of research being carried out in a number of countries.

In the **USA**, work is being carried out to identify and develop methods, analytical tools, and regulatory guidance to support nuclear power plant licensing decisions on digital systems and their modelling in the PSA. Previous work has identified a set of desirable characteristics for reliability models of digital systems. Currently quantitative software reliability methods are being reviewed and the aim is to develop one or two technically sound approaches to modelling and quantifying software failures.

In **Korea**, the development of the PSA methodology for digital computer systems is seen as an urgent issue because of their increased use in safety-critical systems. The work being carried out addresses a wide range of issues including: the influence of the validation and verification of the software on the failure probability; the coverage of fault-tolerant features such as watchdog timers; the coverage of automated self-checking algorithms; the CCF for many trains (more than 8 redundancies); and the possibility of the digital systems inducing initiating events.

In **Japan**, the failure of both the hardware and software in digital systems has been included in the PSA for the Advanced Boiling Water Reactor (ABWR) based on the approach defined in IAEA documents. The work now being carried out is to collect failure and population data for a wide range of components in digital systems.

In **India**, the experience with the modelling of digital systems indicates clearly that improved method of reliability prediction employing a Physics-of-Failure (PoF) approach needs to be developed. Work is being carried out to develop models and methods for software reliability characterization.

In **France**, work has been carried out to improve the EDF reference approach to modelling I&C – referred to as the “compact model”. This includes the modelling of initiating events induced by spurious actuation of I&C, of the man-machine interface and to improve the way to address digital I&C.

Activities in **Germany** focus on developing approaches for assessing the reliability of software based digital I&C. A first approach for considering the PSA relevance of the man-machine interface of software based I&C has been developed.

Level 2 PSA

The current standard is to carry out a Level 2 PSA for all nuclear power plants and this has led to a number of development and research activities in this area of the PSA.

In the **USA**, work is being carried out to investigate the feasibility of a dynamic event tree approach that uses MELCOR in conjunction with the IDAC dynamic operator response model (developed at the University of Maryland) in the generation and analysis of scenarios.

In the **UK**, work is being carried out to determine the feasibility of producing Level 2 PSAs for the AGRs. A pilot study has been carried out for a limited number of sequences to make a more refined estimate of the frequency of the associated radiological releases and consideration is being given to the practicability of carrying out a full Level 2 PSA.

In **Switzerland**, a number of research activities are being carried out which include the following: Melt-Structure-Water Interactions (MSWI) in light water reactors that could occur inside or outside the vessel. The aim is to create a basis to assess ex-vessel debris coolability and steam explosions in a BWR;

the development of a new MELCOR model for the oxidation process of fuel elements in case of air ingress during severe accident scenarios so that the release of fission products can be calculated more accurately; and

the ADAM system which is a much faster than real-time accident diagnostics and prognostics system which has been implemented at the emergency response centre for all Swiss nuclear power plants.

In **Korea**, work has been carried out to improve the Level 2 PSAs so that they can be used for risk-informed applications. This has included: the combination of the Level 1 and 2 PSA into a single integrated model; development of the containment fragility analysis methodology under severe accident conditions. and improvements in the way that uncertainties are addressed.

In **Japan**, an advanced code THALES-2 has been developed for analyzing the progression of a core melt accident and fission product release and transport. In this code, the models for aerosol transport and iodine chemistry have been improved based on experimental data. In addition, MAAP has been used to examine accident management countermeasures and MELCOR has been used for the analysis of the prevention and mitigation of various severe accident sequences under accident management conditions for the various types of nuclear power plants operating in Japan. The source term profiles have been calculated for all the accident sequences that lead to containment failure including various large early release sequences. In addition, work has been carried out to consolidate the analytical methodologies and technical basis for all phases/sequences to be evaluated in the Level 2 PSA for the sodium-cooled fast breeder reactors. This includes computer codes to evaluate the long term in-vessel and ex-vessel behaviour following a degraded core.

In **France**, work is being carried out to develop and update the Level 2 PSAs to take account of a number of changes which includes: plant modifications (such as the incorporation of recombiners and new severe accident guides); severe accident analysis using the latest versions of the computer codes; improvements in the evaluation of uncertainties for physical phenomena; evaluation of the core re-flooding possibility during the degradation process; and assessment of radiological consequences for each release category (with standard meteorological data). The analysis uses the severe accident codes developed in France which have been supplemented with some specific simplified parametric models where it has been judged that physical phenomena have been inadequately modelled in existing codes.

In **Finland**, work is being carried out to review the state of the art in Dynamic PSA modelling for severe accident phenomena. This includes a feasibility study on the link between a Dynamic PSA and a conventional PSA.

In **France**, work is being carried out to develop a specific software architecture for a Level 2 PSA – which is Risk Spectrum Professional + Crystal Ball.

In addition, in the **USA**, work is being carried out to investigate the feasibility of using a dynamic event tree approach for Level 2 PSA to: reduce reliance on unnecessary modelling simplifications;

address shortcomings in the current methodology; and improve the treatment of human interaction and mitigation. A tool is being developed that uses the MELCOR accident analysis program in conjunction with a dynamic operator response model.

The actual focus with respect to Level 2 PSA in **In Germany** is on considering severe accidents inside spent fuel pools and fission product behavior.

Level 3 PSA

There is a growing interest in developing the methodology and the tools for carrying out a Level 3 PSA.

In the **USA**, work is being carried out to develop a comprehensive site Level 3 PSA to: update the analysis presented in NUREG-1150; to increase the scope to take account of all external hazards, low power and shutdown conditions and all the sources of radioactivity on the site; to include and take account the developments in PSA methods/ models/ tools/ data and the improvements to nuclear power plants that have taken place since then. A scoping study has been initiated.

In **Japan**, a Level 3 PSA is being produced for a generic LWR using the OSCAAR computer code package which consists of interlinked computer codes to predict: the transport of radio nuclide through the environment to man; subsequent dose distributions; and health effects in the population. In addition, a Level 3 PSA program is being carried out using the MACCS-2 code to analyze off-site radiological consequences for seismic events at typical BWR and PWR plant and for multi-unit sites.

In **Finland**, work will be carried out in Level 3 PSA and risk criteria to develop a calculational approach for risk evaluation following a radioactive release to the environment.

Uncertainties

Work is being carried out in many countries to improve the way that uncertainties are being addressed. In the **USA**, NRC is developing guidance for the treatment of uncertainties and the use of alternate methods in risk-informed decision making. This will address the integrated risk-informed decision making process and different approaches appropriate for the treatment of different types of uncertainty.

In **Korea**, the Thermal Hydraulic Uncertainty Analysis Software for PSA (MOSAIQUE) has been developed. This is a best estimate thermal hydraulic methodology that performs sampling calculations based on a Monte-Carlo approach. The software uses a number of PCs on the intranet to reduce the computing time.

In **France**, EDF have carried out a pilot study using the EPRI guidelines for the treatment of uncertainties for the Level 1 and 2 internal events PSA and adapted the methodology to the specificity of EDF PSA models. This methodology is now applied for each PSA update.

In **Germany**, the existing methods and tools or treating uncertainties in PSA Level 1 and Level 2 have been significantly improved, in particular concerning epistemic uncertainties.

Another more recent development in **Germany** is the probabilistic dynamics method MCDET. Methods for uncertainty and sensitivity analyses in the frame of Dynamic PSA, e.g. for a more realistic modeling of accident scenarios, have been established.

Modelling of ageing in PSA

The issue of whether to incorporate the effects of aging into a PSA and the way that this should be done have been discussed for many years. Currently, work is being carried out in a number of countries to consider this issue.

In **France** work is being carried out to investigate the possibility of including ageing effects in PSA models. This will be limited to the incorporation of the maintenance data and the operating experience

in the existing 900 MWe plants PSA model. The results will be used in the review for life extension of these plants.

In **Canada**, a research project is being carried out that aims to incorporate ageing effects into the PSA. The aims of the work include: the identification of aging sensitive CANDU specific equipment; and the evaluation of the impact of aging effects on plant-specific PSA. In addition, work is being carried out with Canadian universities on the modelling of ageing effects using time dependent failure rates.

In the **Czech Republic**, guidelines are being developed on how to treat ageing and incorporate its effects into PSA models.

Fuel route PSA

The scope of the PSAs being carried out is being extended to include the risks from refuelling and fuel storage.

In **France**, work has been carried out to assess the risk of core uncovering in the fuel pool due to the loss of the Fuel Pool Cooling System or due to uncontrolled level drop in the pool. This analysis is now performed and regularly updated for all PWRs.

In the **UK**, a pilot study has been carried out to determine the risk from refuelling and fuel handling operations using the same methods as for the internal events, at-power PSA. The analysis takes account of protection, mitigation and the factors that influence the magnitude of the off-site release.

Use of the PSA in risk-informed applications

There is a growing trend to use a risk-informed approach to making decisions on safety and regulatory issues which requires that high quality, wide scope PSAs are carried out to provide an input into the decision making process. In addition, risk-informed applications such as Risk Monitors are being implemented in a number of countries. This is the case in a number of countries (such as the **Netherlands, Mexico and India**) where there is a move towards a risk informed approach and work is being carried out to improve the PSAs that provide an input to this.

In the **USA**, in order to support the ongoing efforts to risk-inform its regulatory processes, NRC has established the Risk-informed and Performance-based Plan (RPP) which is designed to coordinate NRC's strategy. In addition, a broad spectrum of activities is being carried out that aim to enhance the safety and improve the economics of existing and future nuclear power plants.

In **Hungary**, work has been carried out to support the introduction of a systematic approach to monitor the effectiveness of maintenance and to investigate the potential applicability of risk-informed inspections.

10. OVERALL INSIGHTS

With the updating of the CSNI Report on “Use and development of Probabilistic Safety Assessment”, some main conclusions could be drawn:

- All the PSA developments and applications already described in the previous versions of the report are still valid and regularly increasing. This applies to the importance of PSA framework, the number of studies carried out, the PSA scope, the number of applications (for design and operation safety improvements), and the volume of on-going research. It can be noted that although PSA methods and applications have made real progress during these last years a significant level of development is still in progress. This amount of research activity indicates that PSA results are sufficiently useful to justify this amount of work.
- The development of new and advanced reactor designs has led to a more rapid development in particular topic areas. Examples include the definition of a more formal framework for PSA development and risk-informed decision making, more precise safety criteria (concerning numerical values and/or requirements), additional efforts relating to the importance of external hazards and to new specific problems like reliability of digital systems and reliability of passive systems. A tendency towards harmonization appears clearly.
- Some particular new points have been noted:
 - A more formal framework (more precise requirements especially in case of new plants)
 - More precise Safety Goals (for example safety criteria relating to containment)
 - Extended PSA scope: the general tendency is PSA level 2 covering internal and external hazards and all the plant operating modes. Moreover some new extensions include for example the spent fuel pool and shared systems between multi-units plants.
 - Increased efforts towards PSA quality including new standards and guidance documents and increasing external reviews.
 - A current use of new HRA methods (in addition to continuing HRA developments)
 - An important activity relating to Fire PSAs (including supporting research).
 - New developments and applications relating to external hazards.
 - Research activities and already some applications relating to modeling of passive systems and modeling of digital I&C.....

- It has to be noted that this report was prepared before March 2011 Fukushima accident and consequently does not take into account the potential new developments and priorities based on lessons learned from Fukushima. This report gives an overview of the situation before Fukushima and a next updating is expected to focus on the post-Fukushima activities.
- As previously, WGRISK will use the results of this report, as moderated by Fukushima response activities, to monitor the conduct of its ongoing activities, and to promote and implement new international collaborative efforts within the framework of the CSNI.

References

- [1]. The Use and Development of Probabilistic Safety Assessment in NEA Member Countries, [NEA/CSNI/R\(2002\)18](#)
- [2]. Use and Development of Probabilistic Safety Assessment, [NEA/CSNI/R\(2007\)12](#)
- [3]. Overview on Use and Development of Probabilistic Safety Assessment, [NEA/SEN/SIN/WGRISK\(2008\)3](#)
- [4]. Probabilistic Risk Criteria and Safety Goals, [NEA/CSNI/R\(2009\)16](#)
- [5]. Proceedings of the OECD/NEA Workshop on Simulator Studies for HRA Purposes, Budapest, 4-6 November 2009, to be issued as [NEA/CSNI/R\(2012\)1](#)
- [6]. Recommendations on Assessing Digital System Reliability in Probabilistic Risk Assessment of Nuclear Power Plants, [NEA/CSNI/R\(2009\)18](#)
- [7]. Proceedings of the Workshop on Implementation of Severe Accident Management Measures, Bottstein, 26-28 October 2009 [NEA/CSNI/R\(2010\)10](#)
- [8]. Probabilistic Safety Analysis (PSA) of Other External Events Than Earthquake, [NEA/CSNI/R\(2009\)4](#)
- [9]. Low Power and Shutdown Operation Risk: Development of Structure for Information Base and Assessment of Modelling Issues, [NEA/CSNI/R\(2009\)17](#)

APPENDIX A

OVERVIEW OF THE STATUS OF PSA PROGRAMMES IN MEMBER AND NON-MEMBER COUNTRIES

- 1. Belgium**
- 2. Canada**
- 3. Chinese Taipei**
- 4. Czech Republic**
- 5. Finland**
- 6. France**
- 7. Germany**
- 8. Hungary**
- 9. India**
- 10. Italy**
- 11. Japan**
- 12. Korea**
- 13. Mexico**
- 14. Spain**
- 15. Sweden**
- 16. Switzerland**
- 17. Slovak Republic**
- 18. Slovenia**
- 19. The Netherlands**
- 20. UK**
- 21. USA**

1. 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: 2011 2015 for F&F PSA	Periodic safety review Continuous PSA project WENRA R.L.	Design review PSA based event analysis Ranking of safety critical components Training of operators
		Level 2- ^A	Internal events only	Original: At power only Update: Power and Shutdown	No	Original: 2005 Revised: 2011 ^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: 2011 2015 for F&f PSA	Periodic safety review Continuous PSA project WENRA R.L.	Design review PSA based event analysis Ranking of safety critical components Training of operators
		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 WENRA R.L.	Design review PSA based event analysis Ranking of safety critical components Training of operators
		Level 2 ^B	Internal events only	Original: At power only Update: Power	No	Original: 2000 Revised: 2010 ^C	Periodic safety review Continuous PSA	Design review

				and Shutdown			project	
Doel4 Tihange 3	PWR	Level 1	Internal events Internal hazards (fire/ flood only) ^F	Power & Shutdown	No	Original: 2000 Revised: 2011 2015 for F&f PSA	Periodic safety review Continuous PSA project WENRA R.L.	Design review PSA based event analysis Ranking of safety critical components Training of operators
		Level 2 (only after update)	Internal events only	Original: None Update: Power and Shutdown	No	Original:/ Revised: 2011 ^C	Periodic safety review Continuous PSA project	Design review

A: Original Level 2 (Level 2-) limited to containment response; no source term analysis – Source Term & Shutdown Modes introduced during update

B: Original Level 2 limited to deterministic analysis of containment response for characteristic core melt scenarios – Probabilistic analysis of containment response, source term & shutdown modes introduced during update

C: Selected as representative unit

D: Doel 3 selected as representative unit

E: Tihange 3 selected as representative unit

F: Not in the original PSA

2. CANADA –

Plant name	Plant Type ⁶	Scope of the PSA carried out				PSA usage		
		Level of PSA	Initiating Events	Plant Operating states	Living PSA	Date of Original PSA Reviews	Reason for Carrying out PSA	PSA applications
PA	4x540 MWe	3	Internal	At power & shutdown		1995/2007		
PB	4x540 MWe	3	Internal	At power & shutdown		2003/2006		
Darlington	4x880 MWe	3	Internal	At power & shutdown		1987/2000		
BA	4x820 MWe	3	Internal	At power & shutdown	Being maintained as living PSA	2003/2005/2005	U3-U4 Restart	U1-U2 Restart/Refurbishment
BB	4x860 MWe	3	Internal	At power & shutdown		1999/2002		
PLE	600 MWe	1	Internal	At power		2001		Refurbishment
		1	External	At power		2003		
		2	internal	At power		2004		
G-2	600 MWe							Refurbishment

PA: Pickering A (Ontario Power Generation)

PB: Pickering B (Ontario Power Generation)

BA: Bruce A (Bruce Power)

BB: Bruce B (Bruce Power)

PLE: Point-Lepreau (New Brunswick Power)

G-2: Gentilly 2 (hydro-Quebec)

⁶ All Canadian Nuclear Power Plants are CANDU

CANADA: Canadian PSA's AFTER S-294 implementation

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 Reviews	Reason for Carrying out PSA	PSA applications
PA	4x540 MWe							
PB	4x540 MWe							
Darlington	4x880 MWe	1	internal	At power		2011	S-294 Compliance	Refurbishment EOOS
BA	4x820 MWe							
BB	4x860 MWe							
PLE	600 MWe	2	Internal	At power & shutdown		2007	S-294 Compliance	Refurbishment/ Risk Informed Integrated Safety Management System
		2	External Fire	At power		2007		
		2	External Flood	At power		2007		
		2	External Seismic	At power		2007		
G-2	600 MWe	1	internal	At power		2011	S-294 Compliance	Refurbishment
NRU⁷	130 MWt	2	internal	At power		2005/2008		

⁷ Atomic Energy of Canada Limited (AECL) performed the Level 1 and Level 2 PSA, internal events at power on a voluntary basis. S-294 is only applicable to NPPs

3. CHINESE – TAIPEI

Plant	Type	PSA Type	Original PSA Date Completed	Revised PSA Date Completed
Chinshan	BWR 4	Level 1 + LERF	Level 1 – 1991 LERF – 2001	Expected 2011
Kuoshan	BWR 6	Level 1 + LERF	Level 1 – 1985 LERF – 2001	Expected 2011
Maanshan	PWR	Level 1 + LERF	Level 1 – 1987 LERF – 2001	Expected 2011
Lungmen	ABWR	Level 1 + LERF	2007	2012

4. CZECH REPUBLIC

Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
		Level of PSA	Initiating events	Plant States	Operating	Living PSA	Date of original PSA/ revisions	Reason for carrying out PSA
Dukovany	WWER 440/213	Level 2 (external events only for Level 1)	Internal events Internal hazards (fires and floods) human-induced external events	All plant operating states /Level 2 at power and hot shutdown/	Yes Updated periodically	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 Updated as required	Original: 1996 Revised: 2003 Revised 2011	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

5. 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 1 and 2	<p>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</p>		Yes, for all initiators	<p>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</p>	<p>Identification of weak points, improvement of design Support of PSA applications and risk informed decision making, Improvement of operator training,</p>	<p>Design modifications Risk informed TechSpecs Safety monitor RI ISI – pilot safety classification of equipment, Economic optimization and prioritization of design options,</p>

Plant Name	Plant type	Scope of the PSA carried out				PSA usage			
		Level of PSA	Initiating events	Plant States	Operating	Living PSA	Date of original PSA/ revisions	Reason for carrying out PSA	PSA applications
Olkiluoto1/2	BWR 660	Level 1 and 2	<p>Level 1 power: Internal, fires, flood, seismic, harsh weather conditions (+oil), Level 1 shutdown: Internal, fires,</p> <p>Level 2 power: Initiators as level 1</p>			Yes, for all initiators	<p>Original: 1989- 94, 99, 97 1992-94, 98 1991-94, 97, 04 1996 1994- 97, 98, 03, 05</p> <p>1992-97, 06, 1998</p> <p>1997-03</p>	<p>Identification of weak points, improvement of design Support of PSA applications and risk informed decision making Improvement of operator training,</p>	<p>Design modifications, Risk informed TechSpecs, RI ISI – pilot, PSA based event analysis, safety classification of equipment,</p>

6. FRANCE

<u>Plant</u> Name	<u>Plant</u> type	Scope of the PSA carried out				PSA usage			
		Level of PSA	Initiating events	Plant States	Operating	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	Operating	Yes - updated for 10 yearly PSR	Original: 1990 (level 1) Last revision in 2007	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 Level 2	Internal events + Fire + internal flooding, earthquake (last revision) Level 2 (internal events only)	All plant operating states	Operating	Yes - updated for 10 yearly PSR	Original: 1990 Last revision in 2010	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	Operating	Yes – updated for 10 yearly PSR	Original: 2001 Last revision in 2007	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	Operating	Design PSA	Original:	Carried out as	Design review

				states		2001 Revised: 2006	part of the initial design and licensing	AOT and IST
EPR Flamanville 3	PWR	Level 1 Level 2	Internal events, fire, internal flooding, explosion, SMA	All plant operating states	Construction PSA	Last update 2009 (internal events) 2011 for external events		

7. GERMANY

Plant name		Plant type	Scope of most recent PSA within PSR			Date of PSR	
			Level of PSA	Plant Operating States	Initiating Events	Original	Follow-up
Biblis A	KWB A	PWR	Level 1	FP	IE, IH, EH ⁸	31.12.2001	31.12.2011 ⁹
				LPSD	IE ¹⁰		
			Level 2 ¹¹	FP			
Biblis B	KWB B	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2000	31.12.2010
				LPSD	IE		
			Level 2	FP			
Neckarwestheim 1	GKN 1	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2007	-
				LPSD	IE		
			Level 2	FP			
Brunsbüttel	KKB	BWR	Level 1	FP	IE, fire, EH ¹	30.06.2001	30.06.2011
				LPSD	IE		
			Level 2	FP			
Isar 1	KKI 1	BWR	Level 1	FP	IE, IH, EH ¹	31.12.2004	
				LPSD	IE		
			Level 2	FP			
Unterweser	KKU	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2001	31.12.2011 ²
				LPSD	IE		
			Level 2	FP			

⁸ see separate table⁹ not yet completed before end of commercial operation¹⁰ conservative estimate

Plant name		Plant type	Scope of most recent PSA within PSR			Date of PSR	
			Level of PSA	Plant Operating States	Initiating Events	Original	Follow-up
Philippsburg 1	KKP 1	BWR	Level 1	FP	IE, IH	31.08.2005	
				LPSD	IE		
			Level 2	FP			
Grafenrheinfeld	KKG	PWR	Level 1	FP	IE, IH, EH ¹	31.10.2008	
				LPSD	IE		
			Level 2	FP			
Krümmel	KKK	BWR	Level 1	FP	IE, IH, EH ¹	30.06.2008	
				LPSD	IE		
			Level 2	FP			
Gundremmingen B	KRB B	BWR	Level 1	FP	IE, IH, EH ¹	31.12.2007	
				LPSD	IE		
			Level 2	FP			
Grohnde	KWG	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2000	31.12.2010
				LPSD	IE		
			Level 2	FP			
Gundremmingen C	KRB C	BWR	Level 1	FP	IE, IH, EH ¹	31.12.2007	
				LPSD	IE		
			Level 2	FP			
Philippsburg 2	KKP 2	PWR	Level 1	FP	IE, IH, EH ¹	31.10.2008	
				LPSD	IE		
			Level 2	FP			
Brokdorf	KBR	PWR	Level 1	FP	IE, IH, EH ¹	31.10.2006	
				LPSD	IE		

Plant name		Plant type	Scope of most recent PSA within PSR			Date of PSR	
			Level of PSA	Plant Operating States	Initiating Events	Original	Follow-up
			Level 2	FP			
Isar 2	KKI 2	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2009	
				LPSD	IE		
			Level 2	FP			
Emsland	KKE	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2009	
				LPSD	IE		
			Level 2	FP			
Neckarwestheim 2	GKN 2	PWR	Level 1	FP	IE, IH, EH ¹	31.12.2009	
				LPSD	IE		
			Level 2	FP			

FP: full power operational states
external hazards

LPSD: low power and shutdown states

IE: internal events

IH: internal hazards

EH:

Depth of PSA analysis for the external hazards earthquake (SPSA), flooding (FPSA) and extreme weather conditions (WPSA)

NPP (last SR)	SPSA		FPSA	WPSA (and additional remarks)
	Intensity	Depth of Analysis	Depth of Analysis	
GKN 1 (2007)	VIII	(3) SPSA	(2) restricted analysis	WPSA: no indications of potentially endangering plant
GKN 2 (2009)		(3) SPSA	(2) restricted analysis	
KKP 1 (2005)	VII - VIII	not necessary	not necessary	Last SR in 2005, hazards PSA not required
KKP 2 (2008)		(3) SPSA	(2) restricted analysis	It is demonstrated that contribution of flooding to CDF < 10 ⁻⁶ /a
KRB B (2007)	VII	(2) restricted analysis	(3) FPSA	WPSA: hazard exclusion at site (historical data assessment)
KRB C (2007)		(2) restricted analysis	(3) FPSA	WPSA: hazard exclusion at site (historical data assessment)
KKG (2008)	VII	(1) no analysis	(2) restricted analysis	WPSA: negligible
KKI 1 (2004)	VI < intensity < VII	(2) restricted analysis	(2) restricted analysis	WPSA: negligible
KKI 2 (2009)		(2) restricted analysis	(2) restricted analysis	WPSA: negligible
KWB A (2001)	VII < intensity < VIII	not necessary	not necessary	Last SR completed in 2001, hazards PSA not required
KWB B (2000)		(3) SPSA	(2) restricted analysis	
KKU (2001)	VII	(1) no analysis	(3) FPSA	WPSA: negligible
KWG (2000)	VI < intensity < VII	(2) restricted analysis	(2) restricted analysis	
KKE (2009)	6	(1) no analysis	(1) no analysis	
KBR (2006)	6	(1) no analysis	(3) FPSA	WPSA: negligible
KKB (2001)	≤ VI	(1) no analysis	(2) restricted analysis	WPSA: hazard exclusion at site SPSA: only occurrence frequency calculated
KKK (2008)	VI	(2) restricted analysis	(2) restricted analysis	WPSA: negligible SPSA: only occurrence frequency calculated

8. HUNGARY

Overview of the PSA Programmes									
Plant Name	Plant type	Scope of the PSA carried out				PSA usage			
		Level of PSA	Initiating events	Plant States	Operating	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	VVER-	Level 1	Internal fires,	Full power		Yes	Original:	Regulatory	*

2	440/213		internal flooding			2001 Revision: annually	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 2	VVER- 440/213	Level 1	Internal fires, internal flooding	Low power and shutdown states of a refuelling outage	Yes	Original: 2007 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 3	VVER- 440/213	Level 1	Seismic events	Low power and shutdown states of a refuelling outage	Yes	Original: 2006 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, units 2-4, 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	*
Paks, unit	VVER-	Level 2	Internal events,	Full power, Low	No	Original:	Regulatory	*

1, reactor and spent fuel storage pool	440/213		internal fires and internal flooding	power and shutdown states of a refuelling outage for reactor, all planned plant operational states for spent fuel storage pool		2003 Revision: none	requirements	
Paks, unit 3	VVER-440/213	Level 2	Seismic events	Full power	No	Original: 2006 Revision: none	Regulatory requirements	*

*PSA applications are made on plant level rather than on a unit specific basis. The actual PSA application areas are listed in the corresponding chapter ('PSA Applications') of the report.

9. INDIA

Sr. No	NPP	Scope of PSA (Internal events)	Submission Date
1	TAPS#1&2	Level-1	Part-I: Nov. 2000 - Part-II: April 2002
		Revised Report	June 2009
2	KAPS#1&2	Level-1	April 2002
		Level-2	March 2006
3	NAPS#1&2	Level-1	June 2006
4	MAPS#1&2	Level-1	January 2010
5	KGS#1&2	Level-1	Jan. 2007
6	RAPS#3&4	Level-1	May 2007
7	KGS#3&4 Project	Level-1	March 2007
8	RAPS#5&6 Project	Level-1	Oct. 2007
9	TAPS#3&4 Project	Level-1	March 2005
10	KK-Project	Level-1	Dec. 2005
11	RAPS#2	Level-1	March 2009

Development of external event PSA (i.e. flood, seismic), internal hazards (i.e. fire, flood) are in progress for a representative NPP (KAPS-1&2). Shutdown PSA has been completed for a representative NPP (KAPS-1&2). A level-2 PSA study for a representative NPP (KAPS-1&2) also has been completed. The objective of this study was to familiarize with the methodology and identification of sever accident scenarios where further analysis is required.

10. ITALY *No information provided*

11. JAPAN (JNES)

JNES performed level 1, level 2 and level 3 PSA for eight NPPs which represent each plant type. Depending on the purposes of studies, modifications are made to reflect the difference of plants in each group. The results of these PSAs are used to review AM strategies established by utilities for their individual plant, review of maintenance program and SDP. In addition, level 1 and 1.5 PSA during shutdown, level 1, level 2 and level 3 seismic PSA have been conducted.

Plant name	Plant type	PSA Scope				PSA usage		
		Level	Initiating events	Plant Operating States	Living PSA	Date of original PSA/revisions	Reason for PSA	PSA applications
500MW class BWR	BWR-3	Level 1-3	Internal event and seismic event	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
800MW class BWR	BWR-4	Level 1-3	Internal event and seismic event	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
1100MW class BWR	BWR-5	Level 1-3	Internal event, seismic event, fire	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
1500MW class BWR	ABWR	Level 1-3	Internal event and seismic event	At power	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP

500MW class PWR	2 loop PWR	Level 1-3	Internal event and seismic event	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
800MW class PWR	3 loop PWR	Level 1-3	Internal event and seismic event	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
1100MW class PWR with large dry CV	4 loop PWR	Level 1-3	Internal event, seismic event and fire	At power and shutdown	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
1100MW class PWR with ice condenser CV	4 loop PWR with ice condenser CV	Level 1-3	Internal event and seismic event	At power	No	1992/2000	Review of AM	Evaluate effectiveness of AM, ASP, Maintenance Program, SDP
FBR	FBR	Level 1-1.5	Internal event	At power	No	2003/2011	Review of AM	Evaluate effectiveness of AM

(JAEA)

JAEA performed level 1 and 1.5 PSA during power operation of “Monju.” The results of level 1 and level 1.5 PSA are used to derive AM measures of Monju..

(Utilities)

Utilities performed level 1 and 1.5 PSA during power operation and level 1 PSA during shutdown for their plants. The results of level 1 and level 1.5 PSA during power operation are used to derive AM measures, to evaluate effectiveness of AM measures and to establish maintenance programs.

12. KOREA

Plant Name	Type	Scope of the PSA carried out			PSA usage		
		Level of PSA	of 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

13. 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 1 and 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	

14. SPAIN

Plant Name	Plant type	Scope of the PSA carried out				Utility / PSA usage		
		Level of PSA	Initiating events	Plant Operating States	Living PSA Revision number	Date of PSA revisions	Reason for carrying out PSA	PSA applications
Trillo	PWR KWU 3 loops	Level 1	Internal events	Power Low Power &Shutdown Including Spent fuel pool	Rev 6 Rev. 1	2012 2012	Continuous PSA project Next Periodic safety review (PSR): 2013	Design review Risk Monitors (Maintenance managing) Shutdown safety
			Internal hazards: fire flood	Power	Rev. 0 Rev. 6	2008 2012		Design Review
		Level 2	Internal events	Power	Rev. 6	2012	Continuous PSA project	Design review
Vandellós II	PWR W 3 loops	Level 1	Internal events	Power Low Power &Shutdown	Rev 5 Rev. 2	2011 2012	Continuous PSA project Last Periodic Safety Review (PSR) 2011	Design review Risk Monitors (Maintenance managing) Shutdown safety

Plant Name	Plant type	Scope of the PSA carried out				Utility / PSA usage		
		Level of PSA	Initiating events	Plant Operating States	Living PSA Revision number	Date of PSA revisions	Reason for carrying out PSA	PSA applications
			Internal hazards: fire flood	Power	Rev. 1 Rev. 1	2010 2012	Idem	Design Review
		Level 2	Internal	Power	Rev. 1	2012	Idem	Design review
Cofrentes	BWR GE-BWR6	Level 1	Internal events	Power Low Power &Shutdown	Rev 5 Rev. 2	2012 2012	Continuous PSA project Last Periodic Safety Review (PSR) 2011	Design review ETF Risk Monitor (Maintenance managing). RI- ISI / IST Personal Training Shutdown safety
			Internal hazards: fire ¹² flood	Power	Rev. 3 Rev.4	2006 2010		Design review
		Level 2	Internal and flood	Power	Rev. 2	2012	Idem	Design review
Ascó	PWR	Level 1	Internal events	Power	Rev 5	2012	Continuous	Design review

¹² Next review 2013 Methodological review (NUREG 6850)

Plant Name	Plant type	Scope of the PSA carried out				Utility / PSA usage		
		Level of PSA	Initiating events	Plant Operating States	Living PSA Revision number	Date of PSA revisions	Reason for carrying out PSA	PSA applications
2 Units	W 3 loops			Low Power & Shutdown	Rev. 2	2011	PSA project Last Periodic Safety Review (PSR) 2011	Risk Monitor – Maintenance managing. RI- ISI / IST Personal Training Shutdown safety
			Internal hazards: fire flood	Power	Rev. 2 Rev.2	2010 2010	Idem	Design review.
		Level 2	Internal	Power	Rev. 2	2010	Idem	Design review
Almaraz 2 Units	PWR W 3 loops	Level 1	Internal events	Power Low Power & Shutdown	Rev 11 Rev. 3	2012 2012	Continuous PSA project Last Periodic Safety Review (PSR) 2010	Design review Risk Monitors – Maintenance managing. RI- ISI Personal Training Shutdown safety
			Internal hazards:	Power			Idem	Design review.

Plant Name	Plant type	Scope of the PSA carried out				Utility / PSA usage		
		Level of PSA	Initiating events	Plant Operating States	Living PSA Revision number	Date of PSA revisions	Reason for carrying out PSA	PSA applications
			fire flood		Rev. 2 Rev.3	2011 2009		NFPA 805
		Level 2	Internal Fire ¹³	Power	Rev. 5 Rev. 0	2011 2012	Idem	Design review NFPA 805
		Level 1	Internal events	Power Low Power &Shutdown	Continuous review	2011 2011	Continuous PSA project PSR 2008	Design review ETF Risk Monitors – Maintenance managing. Personal Training Shutdown safety
Garoña	GE-BWR3		Internal hazards: fire flood	Power	Continuous review	2012 2009	Idem	Design review.
		Level 2	Internal	Power	Continuous review	2009	Idem	Design review

¹³ Transitioning to NFPA 805

15. SWEDEN

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	PI 2007	2004	1993	1993	PI 2006	PI 2006	2005	2005	2005
Refueling	2005	PI 2007	2003	1999	1999	1995	PI 2006	2001	2005	2005
Level 2										
Power operation	2005	PI 2007	PI 2006	2001	2001	1998	1996	2005	2005	2005
Shutdown, - restart	2005	PI 2007	PI 2006	2001	2001	PI 2006	PI 2006	2004	2005	2005
Refueling	2005	PI 2007	PI 2006	PI 2006	PI 2006	PI 2006	PI 2006	1996	2005	2005
Legend:										
PI = Planned										
Remark: Under each subtitle following kinds of analysis are completed or goal for update										
- LOCA / Transienter / CCIer										
- Fire										
- Flooding										
- Heavy lifts										
- External Events										

16. 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 & 2 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A detailed procedure for updating the PSA has been defined	1993 (full power Level 1 & 2) 1998 shutdown Revisions: Living PSA	Regulatory requirement as an important aspect of the safety analysis	Design review Risk-informed regulation (see Section 7)
Gösgen	PWR Siemens- KWU 3 Loop PWR	Level 1 & 2 full power Level 1 & 2 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A detailed procedure for updating the PSA has been defined	1994 (full power Level 1 & 2) 1994 shutdown Revisions: Living PSA	Regulatory requirement as an important aspect of the safety analysis	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 detailed procedure for updating the PSA has been defined	1994 (full power Level 1 & 2) 2001 shutdown Revisions: Living PSA	Regulatory requirement as an important aspect of the safety analysis	Design review Risk-informed regulation (see Section 7)
Mühleberg	BWR GE BWR/4, Mark-I	Level 1 & 2 full power Level 1 & 2 for low power & shutdown	Full scope All internal and external events	Full power and low power and shutdown	A detailed procedure for updating the PSA has been defined	1993 (full power Level 1 & 2) 1997 shutdown Revisions: Living PSA	Regulatory requirement as an important aspect of the safety analysis	Design review Risk-informed regulation (see Section 7)

17. SLOVAK 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
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 and Level 2	Full scope All internal and external events	Full power and shutdown	Yes	Original: PSA 2006 Living	Regulatory requirements, initiated by utility	Safety Monitor, Safety assessment and upgrading

18. SLOVENIA

-

Plant Name	Plant Type	Scope of the PSA carried out				PSA usage		
		<i>Level of PSA</i>	<i>Initiating events</i>	<i>Plant operating states</i>	<i>Living PSA</i>	<i>Date of original PSA/ revision</i>	<i>Reason for carrying out PSA</i>	<i>PSA applications</i>
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

19. 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 hazards events/	Power states	no	2002-2004	10-yearly periodic safety review	Design review/ Support of backfitting
-------------------------	-------------------------------------	---------	--------------------------------------	--------------	----	-----------	----------------------------------	---------------------------------------

20. UNITED KINGDOM*(i) Plants currently operating*

Plant name	Plant type	PSA Scope				PSA usage		
		Level	Initiating events	Plant Operating States	Living PSA	Date of original PSA/ revisions	Reason for PSA	PSA applications
Oldbury	Magnox	Level 1+ PSA - see note	All internal events	At power only	Yes	Prod: 1990 PSR: 2007	PSR	Design evaluation
Wylfa	Magnox	Level 1+ PSA - see note	Internal events; internal fire; limited treatment of other hazards	At power only	Yes	Prod: 1998 PSR: 2006	PSR	Design evaluation
Hinkley Point B	AGR	Level 1+ PSA - see note Pilot Level 2	Internal events; internal fire; limited treatment of other hazards	At power Pilot shutdown PSA	Yes	Prod: 1995 PSR2: 2006	PSR	Design evaluation
Hunterston B	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power only	Yes	Prod: 1995 PSR2: 2006	PSR	Design evaluation
Dungeness B	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power only	Yes	Prod: 1996 PSR2: 2007	PSR	Design evaluation
Hartlepool	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power Pilot study for refuelling	Yes	Prod: 1997 PSR2: 2007	PSR	Design evaluation

Plant name	Plant	PSA Scope				PSA usage		
Heysham 1	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power only	Yes	Prod: 1997 PSR2: 2007	PSR	Design evaluation
Heysham 2	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power only	Yes	Prod: 1986 (L1 PSA) Rev: 1998 (L2 PSA) Rev: 2002 (LPSA) PSR2: 2009	To support design process	Design evaluation. Risk Informed Tech Specs. Risk Monitor.
Torness	AGR	Level 1+ PSA - see note	Internal events; limited treatment of hazards	At power only	Yes	Prod: 1986 (L1 PSA) Rev: 1999 (L2 PSA) Rev: 2002 (LPSA) PSR2: 2009	To support design process	Design evaluation. Risk Informed Tech Specs. Risk Monitor.
Sizewell B	PWR	Level 3	Internal events and external hazards	Full power; low power; shutdown; refuelling	Yes	Prod: 1992 Rev: 1997 (LPSA) PSR: 2007	To support design process	Design evaluation. Risk Informed Tech Specs. Risk Monitor.

PSR = Periodic Safety Review

Note: The PSA that has been carried out for the gas cooled reactors is a Level 1+ PSA where the Level 1 PSA has been extended by carrying out 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.

(ii) Plants that have now been shut down

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	All internal events	At power only	Plant now shutdown	Prod: 1991 Rev: 1998	LTSR	Design evaluation
Chapelcross	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1990 Rev: 1998	LTSR	Design evaluation
Bradwell	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1986 Rev: 1992	LTSR	Design evaluation
Hinkley Point A	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1987 Rev: 1994	LTSR	Design evaluation
Dungeness A	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1992 Rev: 1995	LTSR	Design evaluation
Hunterston A	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1988 Rev: 1994	LTSR	Design evaluation
Sizewell A	Magnox	Level 1+ PSA	All internal events	At power only	Plant now shutdown	Prod: 1988 Rev: 1994	LTSR	Design evaluation

LTSR = Long Term Safety Review

21. UNITED STATES OF AMERICA

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 has benchmarked 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 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. For new reactors licensed under 10 CFR 52, each holder of a combined license is required to develop a Level 1 and a Level 2 PSA before initial loading of the fuel. The PSA must cover those initiating events and modes for which NRC-endorsed consensus standards on PSA exist one year prior to the scheduled date for initial loading of fuel. NRC's SPAR models are Level 1 PSAs; a small number of extended Level 1 models (to support LERF and Level 2 modeling) have also been developed.

Initiating events addressed

Most of the licensees' 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).

Some of the U.S. plant PSAs address seismic initiating events and others do not. 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. Similarly, a number of past U.S. plant PSAs have addressed internal fire events; the others have used simplified approaches. Currently, about half of the U.S. plants are developing fire PSA models to support adoption of the risk-informed fire protection program under 10 CFR 50.48(c). Only a limited number of plants have performed PSAs for other external events (e.g., high winds, external flooding, accidental aircraft crashes). As discussed above, new reactors are required to address external events since the NRC staff has endorsed the latest combined ASME/ANS Standard on PSA.

NRC's SPAR models address general transients (including anticipated transients without scram), transients induced by loss of a vital alternating current or direct current bus, transients induced by a loss of cooling (service) water, loss-of-coolant accidents, and loss of offsite power. A number of models have been developed to address external events. Work is ongoing to develop models to address internal fires.

Modes of operation addressed

Most of the current licensee PSAs are limited to consideration of events occurring during full power operation. Only a few PSAs address events occurring during LPSD operation. Although consensus standards on LPSD operation have not yet been endorsed by the NRC staff, most new reactor designs have addressed these events in the PSAs using current best practices.

NRC's SPAR models are similarly focused on at-power operations. However, a number of LPSD models have been developed and are being used to support regulatory applications.

APPENDIX B

DETAILED ANSWERS COUNTRY BY COUNTRY

FOR EACH COUNTRY:

- Updated contribution for the following sections

- 2. *PSA Framework and environment***
- 3. *Numerical Safety Goals***
- 4. *PSA Standards and Guidance***
- 5. *Status and Scope of PSA Programs***
- 6. *PSA Methodology and Data***
- 7. *PSA Applications***
- 8. *Results and Insights***
- 9. *Future Developments and Research***

- Contact person

COUNTRIES:

1. Belgium	p. 97
2. Canada	p. 105
3. Chinese Taipei	p. 120
4. Czech Republic	p. 126
5. Finland	p. 141
6. France	p. 158
7. Germany	p. 172
8. Hungary	p. 183
9. India	p. 199
10. Italy	p. 207
11. Japan	p. 212
12. Korea	p. 235
13. Mexico	p. 253
14. Spain	p. 265
15. Sweden	p. 274
16. Switzerland	p. 289
17. Slovak Republic	p. 302
18. Slovenia	p. 305
19. The Netherlands	p. 316
20. UK	p. 337
21. USA	p. 378

1. BELGIUM

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

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 would 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 reevaluation (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 process is linked to the periodic safety reviews, although intermediate updates are also foreseen. More information on the integration of PSA in the PSR projects can be found in a paper presented at PSAM7 [4].

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. As part of the Belgian Action Plan in the framework of the WENRA RHWG (Reactor Harmonisation Working Group), the FANC (Federal Agency for Nuclear Control) will develop a legal framework on nuclear safety, covering also PSA. The activities conducted in the framework of the WENRA RHWG also lead to an action plan for the Belgian nuclear power plants, in which several implementation actions are related to PSA. These actions were defined to achieve in the future compliance with the WENRA RHWG Reference Levels.

At the end of 2006, Electrabel developed a PSA Policy, defining its involvement in PSA and its perspectives on future applications. Following this policy, Electrabel and Tractebel Engineering, the architect-engineer of the Belgium plants, are developing applications such as:

- training of operation engineers;
- event analysis;
- design modification assessment;
- ranking of safety critical components.

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.

Nevertheless, the PSA Policy of Electrabel introduced new objectives for the PSA, to use it more and more as a support for operation. In that way, the PSA can be more integrated in the plant decision-making process.

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. The utility Electrabel is the end user of the PSA and is supported in his PSA applications by TE. Bel V (formerly AVN)¹⁴, as regulatory organisation, is performing an on-line review of the development and the updating of the PSA models. This means that technical documents related to the models (e.g. proposed methodologies, documents describing event tree construction, system reliability studies, etc.) are transmitted continuously to Bel V 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) Bel V establishes a PSA evaluation report.

3. Numerical Safety Criteria

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. Nevertheless, the PSA results are compared to the international safety targets (IAEA INSAG-12 for example).

Until now, the PSAs were not used for quantified cost/benefit analysis, but this application is mentioned in the PSA Policy of Electrabel as an interesting one.

4. PSA Standards and Guidance

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 Programmes

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 support systems (electric sources, heat sink, compressed air, ..). PSA for internal hazards (fire and flooding) is under development. External hazards are not covered.

In the past, the 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.

¹⁴ In April 2008, all regulatory activities were transferred from AVN to Bel V, a newly created subsidiary of the FANC (Federal Agency for Nuclear Control). For more information, see www.belv.be

For the Doel 1 and 2 and Tihange 1 PSAs, a probabilistic level 2 analysis using Containment Event Trees (CETs) is performed, using MELCOR for the analysis of the severe accident progression. The presence of catalytic recombiners has also been included.

In the on-going periodic safety review, a generic level 2 PSA model is being developed, including identification of containments failure modes and source term release for power and shutdown states. This model will be fully quantified for Doel 3. Three other units (Tihange 1, Tihange 3 and Doel 1/2) will be fully quantified in the framework of the WENRA RHWG activities.

As part of the actions defined as a result of the WENRA RHWG activities (see § 2) it was decided to extend the scope of the PSAs for the Belgian NPPs to include internal fire and internal flooding PSA. Tractebel Engineering presented to Bel V a first proposal for the methodology of the internal fire PSA.

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

For more information on the presently ongoing update, we refer to Section 9.

6. PSA Methodology and Data

For the level 1 PSA, the small event tree - large fault tree methodology (using fault tree linking) is used. All models are managed with the RiskSpectrum code. No particular methods have been used.

For the PSA update, the following methodologies are used:

- Initiating event frequencies are generic, plant specific or a bayesian combination of generic and specific data when the feed back of experience is not sufficient to be used alone.
- Unavailabilities of system components or trains (programmed or non-programmed) are based on plant operating experience.
- Component failure rates are based on the T-book. Plant-specific reliability data are not used.
- The CCF-modelling is based on the Alpha factors and uses generic CCF-parameter data.
- 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 will be identified and included in the PSA models. Human errors caused by the change of state of the plant are also included in the PSA models.

For the system analysis, particular attention had to be devoted in the Doel 1 and 2 PSA, because of some shared systems (twin units).

As the PSA studies are not integrated PSA1/PSA2, a detailed Level1/Level2 interface study will be performed. Plant damage states (PDS) are identified and characterized with some attributes.

For level 2, a large Accident Progression Event Tree (APET) approach will be adopted. This large APET is the result of an extensive decomposition process. The choice of a generic APET has been done in order to keep the homogeneity in the quantifications. 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 severe accident behaviour and severe accident management. This results in a single, large event tree with many events (including PDS attributes) and more than 100000 significant branching points. To compose the APET, subtrees are 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.

7. PSA Applications

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

In the past, 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 were 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 [4] and PSAM8 [5]. Bel V intends to continue this activity in the future.

Electrabel also performs PSA event analysis with the objective to improve the safety of its installations. Since 2008, Electrabel organises an annual Technical Meeting on Precursor Analysis¹⁵ (Brussels, normally in November).

Evaluation of Technical Specifications

Insights gained from the PSAs have been used in the past 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 Bel V 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 Bel V's expectation that in future this kind of application will be discussed with the utility.

RI-ISI

RI-ISI has not been applied so far for the Belgian NPPs.

However, TE and AVN participated in the OECD-project RISMET.

PSA Comparison

In the framework of the cooperation between French and Belgian regulatory organisations, a PSA comparison exercise has been carried out for several years. This comparison deals with two PSA level 1 studies for internal events, performed for both power and shutdown states: the French PSA of the 900 MWe-series PWR, and the Belgian PSA of the Tihange 1 PWR, which both concern PWRs with a similar Framatome design. The main goal of this comparison exercise is to increase confidence in the PSA models and to identify opportunities for model improvement and for PSA harmonization [2, 3].

¹⁵ In succession of the series of meetings organised in the past by AVN.

A similar cooperation between French, Belgian and South-African regulatory organisations has been performed. This comparison was based on the updated French 900 MWe PSA (2003), the Tihange 1 PSA and the Koeberg PSA. It focused on internal events for power states, and constituted an extension of the initial French-Belgian comparison, yielding additional or confirming previous insights [6].

The lessons learnt from these PSA comparisons have been considered when defining the update of the Belgian PSA models.

Ranking of safety critical components

Importance measures have been used to rank the components into three categories: high safety significant, medium safety significant and low safety significant. This categorisation has been used to optimize the Preventive Maintenance Plan of Electrabel units.

More information can be found in a paper that was presented at PSAM9 [7].

Use of PSA insights for training

In the framework of the Belgian action plan for WENRA (see § 2), an action was defined concerning the use of PSA insights for training purposes. This action was defined to comply with WENRA Reference Level O 3.5. Electrabel organised (with support of Tractebel Engineering) training sessions on PSA for the Electrabel staff (in corporate divisions and on-site). Further Electrabel investigated how PSA insights can be used to provide input for the training programs of plant staff, including control room operators (for instance in simulator training sessions). This action for Reference Level O 3.5 was declared “closed” mid-2008.

8. Results and Insights from the PSAs

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 past Level 1 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 (17%) Loss of offsite power (14%) ATWS (11%) MBLOCA (11%) Induced LOCA (11%) SLB inducing SGTR (10%)	Loss of RHRS (63%)
Tihange 2	Partial or total loss of component cooling-service water system (33%) Loss of offsite power (19%) SBLOCA (12%)	To be re-evaluated due to modified operating practices
Doel 4	Loss of feedwater (15%) Loss of offsite power (15%) SBLOCA (15%)	Loss of RHRS (80%)
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 in the past PSR 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

In the framework of the ongoing periodic safety reviews of all plants, discussions have been conducted 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, etc.) an evaluation was 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 learnt from PSA comparison with other countries (in particular France) were also considered for implementation.

The update of all PSA models has been performed and is foreseen to be finalised in 2011 (see Appendix A). An important effort has been devoted by Electrabel and Tractebel Engineering for the update of the PSAs, including a revision of several documents on methodological aspects. The review also requires a high manpower effort at Bel V.

As mentioned in § 5 also the preparations for the fire PSAs for the NPPs have recently been started.

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;
 possibly extending the scope of the PSA (e.g. beyond internal events only, or applying the same level 2 approach to all plants including release categories).

Moreover, significant improvements in maintainable PSA documentation and ready-to-use computer models are expected.

10. References

- [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.
- [7] “Utilization of importance measures in the development, the optimization and the justification of preventive maintenance plans”; Isabelle Hendrickx, Benoit Lance, Gérald Stubbe, Erik Bourdiaudhy and Stéphane Palmaerts, Proceedings PSAM9, Hong Kong - China, May 18-23, 2008

Appendix B – Contact Information

Regulatory Authority / Technical Support Organisation	Direct Contact
<p>Bel V Rue Walcourt 148 B-1070 Brussels Belgium</p> <p>Tel: +32 2 528 02 11 Fax: +32 2 528 02 01 Website Address: www.belv.be</p>	<p>Pieter DE GELDER Bel V Rue Walcourt 148 B-1070 Brussels</p> <p>Tel: +32 2 528 02 60 Fax: +32 2 528 02 01 Email: pieter.degelder@belv.be</p>
Owner's Engineer	Direct Contact
<p>TRACTEBEL ENGINEERING (GDF SUEZ) Avenue Ariane 7 B - 1200 Brussels Belgium</p> <p>Tel. + 32 2 773 8000 Fax + 32 2 773 8900 Website address: www.tractebel-engineering.com</p>	<p>Isabelle HENDRICKX Tractebel Engineering Avenue Ariane 7 B-1200 Brussels</p> <p>Tel. + 32 2 773 76 64 Fax + 32 2 773 89 00 Email: isabelle.hendrickx@gdfsuez.com</p>

2. CANADA

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

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 (NSCA) and regulations [1].

The CNSC published, back in April 2005, the Regulatory Policy P-299 "Regulatory Fundamentals" [2] to promote consistency and clarity regarding the way in which the CNSC achieves its regulatory objectives. This Regulatory policy aims at basing the regulatory actions on levels of risk. It specifically states that the CNSC:

- regulates persons, organizations and activities that are subject to the Act (NSCA) 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 (NSCA); and
- makes regulatory decisions and allocates resources in a risk-informed manner .

Consistent with the intent of this policy, the CNSC has developed the Risk-Informed Decision Making (RIDM) approach to be applied to the nuclear power reactor activities. In this approach, the PSA is recognized as a valuable instrument 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, practiced by both the regulator (CNSC) and the nuclear industry, the Level 2 PSA has become a regulatory requirement included in the Regulatory Standard S-294 [3], published in April 2005. This regulatory standard became part of the Licence for all existing operating power plants.

In the past, the licensees with multi-unit Canadian nuclear power plants have developed Level 3 PSAs (see Table A-1): Darlington Probabilistic Safety Evaluation (DPSE), Pickering-A Risk Assessment (PARA); Pickering-B Risk Assessment (PBRA); Bruce-A Probabilistic Risk Assessment (BAPRA); and Bruce-B Risk Assessment (BBRA). 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). CNSC staff has performed off-line reviews of these PSA's. The New Brunswick Power (NB Power) PSA at Point-Lepreau as well as for the Advanced CANDU Reactor ACR-700, were performed by AECL and the review was performed on-line by CNSC.

CNSC staff is currently performing:

- an **on-line review** of the PSA's under development: Darlington Level 1 internal events PSA at shutdown state; Darlington Level 2 internal events PSA at power; and Darlington External events (Seismic, fire and Flood) PSA at power; and
- an **off-line review** of the Darlington and Gentilly-2 Level 1 internal events PSA at full power.

3. Numerical Safety Criteria

The CNSC regulations include quantitative criteria for the availability of the Special Safety. Availability requirements for these special safety systems are embedded in the Regulatory Documents R-7 [4], R-8 [5] and R-9 [6], published in February 1991, for the containment system, the shutdown systems, and the emergency core cooling system, respectively. The requirement states that the fraction of time for which the system is not available can be demonstrated to be less than $1E-3$ years per year.

Lately, the Regulatory Document RD-337 [7] “*Design of New Nuclear Power Plants*”, published in September 2008, includes a section on design for reliability which states: “*The safety systems and their support systems are designed to ensure that the probability of a safety system failure on demand from all causes is lower than 10^{-3}* ”.

RD-337, also introduces qualitative safety goals consistent with the IAEA standard NS-R-1 [8], which identifies the radiation protection, and technical safety objectives. Following the technical safety objective, CNSC defined 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 is the Small Release triggering the evacuation of the public. This 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 opts to specify the releases of radioactive material in absolute quantities.

RD-337 specifies the following criteria and goals:

- Dose acceptance criteria for events within the Design Basis, and;
- Safety Goals for Beyond Design Basis Accidents.

3.1. Dose acceptance criteria:

The committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary is calculated in the deterministic safety analysis for a period of 30 days after the analyzed event.

This dose is less than or equal to the dose acceptance criteria of:

- 0.5 milli-Sievert (mSv) for any anticipated operational occurrence (AOO); or
- 20 mSv for any design basis accident (DBA)

3.2. Safety Goals

RD-337 defines the following safety goals:

1	Core Damage Frequency (CDF)	Sum of frequencies of all event sequences that can lead to core degradation is less than $10E-5$ /reactor-year
2	Small Release Frequency (SRF)	Sum of frequencies of all sequences that can lead to a release of more than $10E+15$ Bq of I-131 is less than $10E-5$ /reactor-year. A greater release may require temporary evacuation
3	Large Release Frequency (LRF)	Sum of frequencies of all event sequences that can lead to a release to the environment of more than $10E+14$ Bq of Cs-137 is less than $10E-6$ /reactor-year. A greater release may require permanent evacuation

RD-337 also states: “*The design should be balanced such that no particular design feature or event makes a dominant contribution to the frequency of severe accidents, taking uncertainties into account*”.

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-1 below. These are applicable to the operating plants and the refurbishment project for the single unit of Point Lepreau.

Table-1: Safety Goals defined by Ontario Power Generation

	Average Risk (per year)		Instantaneous Risk (per year)
	Target	Limit	Limit ¹⁶
Latent Effects ¹⁷ (per site)	10^{-5}	10^{-4}	N/A
Large Release ¹⁸ (per unit)	10^{-6}	10^{-5}	10^{-5}
Severe Core Damage (per unit)	10^{-5}	10^{-4}	10^{-5}

4. PSA standards and guidance

The Regulatory policy, documents, standards and guides published by CNSC are as follows:

Design for New Nuclear power plants (RD-337) [7]:

Published in April, 2008, this regulatory document sets out the expectations of the CNSC with respect to the design of new water-cooled nuclear power plants (NPPs or plants).

RD-337 includes, among other requirements, the following:

- A requirement on the design for the reliability,
- The dose acceptance criteria for the Design Basis Accidents (DBA); and
- The safety goals for Beyond Design Basis Accidents (BDBA) as explained in Section 3 above.

PSA/PRA for Nuclear Power Plants (NPPs) (S-294) [3]: The regulatory standard, published in April 2005, is now incorporated into the Licence of all the existing power plants. 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 events¹⁹, 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.

Reliability Program for Nuclear Power Plants (S-98) [9]: The standard has been revised and re-issued in July 2005 and it requires the licensees to implement a reliability program that shall:

- Identify, using a systematic method, all systems important to safety,
- specify reliability targets for the systems important to safety at the NPP
- Identify and describe the potential failure modes of the systems important to safety at the NPP
- Specify the minimum capabilities and performance levels that the systems important to safety must attain to achieve reliabilities that are consistent with the safety targets at the NPP and the regulatory requirements;

¹⁶ Bruce Power has an identical set of values as OPG except that the instantaneous risk values are interpreted as threshold values instead of limits

¹⁷ Latent effects refer to delayed fatality.

¹⁸ Defined as release of > 1% of core inventory of Cs-137.

¹⁹ 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.

- Provide information to the maintenance program to maintain effectiveness of the systems important to safety at the NPP;
- Provide for inspections, tests, modeling, monitoring or other measures to effectively assess the reliability of the systems important to safety at the NPP;
- Include provisions to assure, verify and demonstrate the reliability program is implemented effectively;
- Include provisions for recording and reporting the results of program activities, including the results of reliability assessments, inspections, tests, or monitoring of the reliability of the systems important to safety at the NPP; and
- Document, clearly and comprehensively, the activities, attributes, elements, results and administration of the reliability program.

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, GD-98 (see below).

Requirements for Containment systems, Shutdown systems and Emergency core cooling systems, in CANDU Nuclear Power Plants (R-7 [4], R8-8 [5] and R-9 [6], respectively):

These regulatory documents include the availability requirement as explained in section 3 above.

Regulatory Policy: “Considering Cost-Benefit Information”, (P-242) [10]:

This Regulatory policy is published in October 2000. 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 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.

Draft Regulatory Program for Nuclear Power Plants (GD-98): This document is under development and aims to provide licensees with guidance on how to meet the reliability program requirements found in S-98, rev.1 “*Reliability Programs for Nuclear Power Plants*”, which is currently referenced in the Nuclear Power Plant (NPP) licence conditions. The guidance will be directly in-line with the current program requirements found in Section 4.2 of S-98, rev.1. The guidance document will also reflect the results of the joint workshops the CNSC staff have had with the industry to discuss the identified S-98 related issues since 2003.

Industry policies, standards and guides in Canada

PSA Guides:

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.

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

As part of S-294 compliance, the Licensees have to submit for CNSC acceptance the PSA methodologies. Table-2 below gives the status of Licensees submissions:

Table-2: Current status of Licensees submissions of PSA methodologies

PSA Methodologies	BP	OPG	HQ	NBP
Level 1 PSA, internal events at power	Yes	Yes	Yes	Yes
Level 1 PSA internal events at Shutdown (outage)	Yes	Yes	No	Yes
Level 2 PSA, internal events at power	No	Yes	No	Yes
Level 2 PSA, internal events at Shutdown (outage)	No	No	No	Yes
Level 1 Fire PSA at Power *	No	Yes	No	Yes
Level 1 Fire PSA at Shutdown *	No	No	No	No
Level 2 Fire PSA at Power *	No	No	No	No
Level 2 Fire PSA at Shutdown *	No	No	No	No
Level 1 Seismic PSA at Power *	No	Yes	Yes	Yes
Level 1 Seismic PSA at Shutdown *	No	No	No	No
Level 2 Seismic PSA at Power *	No	No	No	No
Level 2 Seismic PSA at Shutdown *	No	No	No	No
Level 1 Flood PSA at Power *	No	Yes	No	Yes
Level 1 Flood PSA at Shutdown *	No	No	No	No
Level 2 Flood PSA at Power *	No	No	No	No
Level 2 Flood PSA at Shutdown *	No	No	No	No

[*] As of S-294, alternative methods can be used

BP: Bruce Power (owner of Bruce A and Bruce B Nuclear Generating Stations)

OPG: Ontario Power generation (owner of Darlington, Pickering A and Pickering B Nuclear Generating Stations)

HQ: Hydro-Quebec (Gentilly-2 Nuclear Generation Station)

NBP: New Brunswick Power (Point-Lepreau Nuclear Generating Station)

Interim Implementation Guidelines for CANDU Nuclear Plant Reliability Programs (COG-05-9011)
[11]:

COG Risk and Reliability Working Group published in April, 2006 the Interim Implementation Guidelines for NPP Reliability Program. One of the key objectives was to develop recommended good-practice guidelines for implementing reliability programs in CANDU Nuclear Power Plants. COG members agreed that a common industry approach on reliability program implementation was needed to ensure that the requirements of S-98 could be met effectively and efficiently.

Cost-benefit analysis:

At the beginning of 2004, COG issued, on behalf of the industry, the document “Benefit-Cost Analysis Implementation Guidelines” [12] (available on: <http://canteach.candu.org/catalog.html#COG>) which 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.

The Licensees have used the CBA during the development of the refurbishment projects. The CNSC will consider this document as it develops its own guidance.

5. Status and Scope of PSA Programs

In Canada, the licensees have developed PSAs over the last two decades. The first completed PSAs for multi-unit plants received by CNSC are Level 3 PSAs, at full power and shutdown operating states. These PSAs were developed as a result of the industry initiatives. On the other hand, the development of the Bruce A PRA (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.

Level 2 analysis has been performed initially, with a limited scope, 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.

Level 3 analysis has been performed using the MACCS code to estimate public health and economic consequences of accidents.

Since 1987, when the Darlington Probabilistic Safety Evaluation (DPSE) has been issued, more PSAs have been completed for operating plants (see Table A-1 and Table A-2 of Appendix A), namely:

- Darlington Risk Assessment (DARA): Darlington NGS has issued the first Probabilistic Safety Evaluation (DPSE) in 1987. Darlington NGS has recently (March, 2011) submitted DARA Level1, internal events at power and is currently developing the Level 1 PSA internal events for shutdown state as well as the Level 2 internal events at power; Level 1 Seismic, Fire and Flood PSA at power as part of S-294 compliance by end of 2011.
- Pickering A Risk Assessment (PARA) : First PARA (level 3 PSA, internal events at power and shutdown) is issued in 1995. Lately the PARA 2009 update (Level 1 PSA, internal events, at power) was completed and submitted to CNSC-CCSN. Pickering A Full compliance with S-294 is expected by December 2013, as per the Licence.
- Pickering B PRA (PBRA): First PBRA (level 3 PSA, internal events at power and shutdown) was issued in 2006. PBRA (level 1, internal events at power) update is expected in 2011. As per the operating Licence, Pickering B has to fully comply with S-294 by December 2012.
- Bruce B Risk Assessment (BBRA): First BBRA (level 3 PSA, internal events at power and shutdown) was issued in 1999 and the last BBRA update is done in 2007. As per the Licence, BP has to comply with S-294 by December 2013.
- Bruce A PRA (BAPRA): First BAPRA (level 3 PSA, internal events at power and shutdown) was completed in 2003. As per S-294 compliance, BP has to update the BBRA and submit other PSA’s (level 1 and Level 2, including internal events and externals, both at power and at shutdown state) by December 2013.

- New Brunswick Power (NBP) PSA: NB Power started the PSA in 2001 and completed the Level 1 PSA (internal events at power and shutdown states), Level 2 PSA (internal events at power and shutdown state) as well as the PSA-Based SMA for seismic events at power and shutdown states. CNSC is currently reviewing the Fire PSA and the Flood PSA.
- Hydro-Quebec (Gentilly-2 NGS) has recently (February 2011) submitted the Level 1 PSA internal events at power. Gentilly-2 has to fully comply with S-294 by December 2012.
- NRU Research reactor has completed, on a voluntary basis, the PSA level 1 internal at power and the Level 2 Internal events at Power.

Regarding new designs, AECL produced a Level 1 PSA for ACR-700, for full power and shutdown states, and internal events, including limited flood analysis. The model was a design-assist tool for the ACR-700. AECL also issued the methodologies for Level 1 PSA and Level 2 PSA for ACR-1000.

An update of the PSAs every 3 years has been set as a requirement in S-294

The summary regarding the scope and use of the CANDU plants PSA is presented in Appendix A (Table A-1 and Table A-2).

6. PSA methodology and data

PSA methodology

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.

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 now migrated into a CAFTA-based environment with event-tree based integration.

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 modeling, and the use of the limiting human error concepts.

For CANDU 6 and ACR, the PSA methodology, using fault tree event tree integration is being employed.

The regulatory standard S-294 [3] refers to the IAEA Level 1 and Level 2 PSA methodologies included in the safety series 50-P-4 [13] and 50-P-8 [14] respectively.

Success criteria:

OPG PSAs and Bruce Power PSAs rely heavily on the safety analysis in the safety report to support basis for system “failure criteria” for accident progression used in event tree analysis and system fault trees. The failure criteria for safety-related systems are derived by assuming that system failure occurs if system capability is reduced to slightly below that assumed in the safety analysis. If no engineering analysis or safety analysis is available or there is insufficient information, expert judgment will be used which will be documented. Both OPG and BP are planning to use realistic success criteria whenever the supporting analyses are available.

Other PSAs (e.g., NB Power) are developed using more realistic success criteria based on supporting analyses.

Initiating events quantification:

Various methods are used to quantify IE frequencies including fault tree analysis. Bayesian methodology is also used to derive IE frequencies from generic and station-specific operating experience.

Potential sources for operating experience include the following:

- BP and OPG Station Significant Event Records (SERs) and Station Condition Records (SCRs);
- BP and OPG station Quarterly reports and Annual Reliability Reports;
- CANDU Owners Group (COG) Operating Experience (OPEX) Database; and
- USNRC Licensee Event Reports (LERs)

Jeffrey's Non-Informative prior distributions are used when little or no generic prior information is available.

Current practice for IE frequency update is to use CAFTA to input generic (prior) experience and station-specific experience for each initiating event. CAFTA will automatically generate the posterior distribution

Reliability Data:

Data is obtained partly from plant-specific records and partly from generic data from the Candu industry where available and elsewhere if not.

The Generic data sources include:

- USNRC and USDOE sponsored databases and reports, e.g., NUREG/CR-6928 [16];
- Other International nuclear industry information, e.g., Sweden's T-Book for Nordic Nuclear Power Plants, Spanish database for reliability Data Collection and Maintenance Rule Implementation;
- Proprietary databases maintained by NPP vendors or utilities, e.g., EQE international, SAIC; and
- Non-nuclear industry databases, e.g., RAC, IEEE-500 Standard.

Common Cause failure:

Two major types of dependent failures are considered in system fault tree analysis:

- 1) Explicit Dependencies: those events that can be readily identifiable with a root cause such as loss of common service water supply to a set of plant loads, or an environmental impact like a fire. These dependencies include:
 - a. Functional dependencies: These are explicitly modeled in the event trees
 - b. Physical interactions: Similar dependencies are analyzed in the external events analyses.
 - c. Human Interactions: Post-accident operator actions are modeled in the event trees and pre-accident operator actions are modeled in the fault trees
- 2) Implicit dependencies- those events that not readily identifiable to an explicit cause but are due to faults like engineering design and or manufacturing defects. Generally, these CCFs are modeled implicitly, in the sense that a single fault tree basic event is used to capture all of the possible causes. They are introduced as inputs to an "OR" gate adjacent to each redundant component's independent failure modes to model the failure dependency.

As much as practical, identifiable common cause failures are covered in the PRA models. 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.

The methodology used for CCF quantification by NB Power is the Unified Partial Method (UPM). If a common cause failure is found to be a dominant contributor to Severe Core Damage, the CCF, previously calculated using the Unified Partial Method, is reviewed for conservatism or recalculated via the Alpha factor methodology and by using the latest alpha factor distribution presented in the 2003 USNRC database.

In updating the BBRA following to the migration to CAFTA, Bruce Power will follow recommended COG guidelines on intrinsic common cause.

BAPRA Intrinsic CCFs are also modeled for selected highly-redundant components but are not quantified at this time

Human reliability Analysis:

The generic human actions common to nuclear power plants can be grouped into the three major categories:

- a) Category A actions - pre-accident human actions (pre-initiators);
- b) Category B actions - human actions which lead directly to initiating events (initiators);
- c) Category C actions - post-accident human actions (post-initiators).

The Human Error Probabilities (HEP) are typically calculated using the ASEP Screening HRA and ASEP Nominal HRA models described in NUREG/CR-4772 (Reference 29), as well as the standard Technique for Human Error Rate Prediction (THERP) /Handbook methodology described in NUREG-CR-1278.

In the NBP PSA, if an operator action is found to be a dominant contributor to Severe Core Damage, the operator action, previously calculated using ASEP, is recalculated using THERP methodology. Some errors of commission are included and extensive recovery events are modeled using the Qrecover feature of CAFTA.

Level 2 PSA methodology:

The level 2 analysis is based on about (12 to 20) plant damage states (PDS) which are identified from the Fuel Damage Categories (FDC's) identified in the Level 1 PSA, and which lead to the severe core damage.

The FDCs are integrated into the bridging event tree with top events representing failures of containment system functions. These PDSs form the starting point for the Accident Progression Event Trees (APET) or Containment Event Tree (CET). The APET top events are CANDU specific nodal questions (about 25). The end states of the APETs are binned into release categories which take into account the small release and large release safety goals. Accident progression is analyzed using MAAP-4-Candu. Release estimates representative of each release category are used as input to the offsite calculations, performed by MACCS code.

Seismic PSA:

NBP has analyzed the seismic event using the PSA-based SMA methodology with the objective to show that the plant High Confidence Low Probability of Failure (HCLPF) is higher than the Review Level Earthquake.

OPG submitted a phased-approach methodology. In the Phase 1, the proposed approach will use the PSA-based SMA and in the Phase 2, a seismic-PSA will be used depending on the results of Phase 1.

7. PSA applications*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 at 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.

When undertaking a project to extend the life of a nuclear power plant (NPP), the Commission requires the Licensee to perform an Integrated Safety Review (ISR) following the regulatory document RD-360 [15]. The ISR involves an assessment of the current state of the plant and plant performance to determine the extent to which the plant conforms to modern standards and practices. The Licensee has to issue the safety factor report on the PSA which will show compliance with the safety goals.

Internally, the PSAs have been used for many years now, in a more or less formal manner, to support the traditional safety approach. Over the 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.

CNSC staff is in the process of developing 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 (precursor analysis), maintenance, operator training, operating procedures, design changes or backfit, operational safety system test program, etc., to support safe operation of nuclear plants.

CNSC staff is exploring the potential of developing a precursor program based on the analysis of nuclear power plant events using probabilistic safety assessment. To better understand international practices with precursor programs, the CNSC initiated an international survey to members of the OECD Nuclear Energy Agency Work Group on Risk Assessment. The survey was conducted from June to August 2010 and focussed on the management and logistical aspect of probabilistically based event analysis. The results of the survey are presented in the 13th International PSA based Event Analysis Technical Meeting, Brussels, Belgium

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

In general the industry uses the PSA results for:

1) 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.

PSAs are also used to support design changes that affect system reliability and in event investigation (e.g., loss of offsite 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. The BAPRA was used 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.

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.

Hydro Quebec is planning for Gentilly-2 refurbishment. Inputs to perform the Gentilly-2 PSA are worked out: e.g. site seismic hazard, PSA methodology, and the parameter file for consequence analyses using the MAAP-CANDU code.

Atomic Energy Canada Ltd. (AECL) performs PSA as a design tool to improve the safety of operating CANDU 6 and ACR-1000 nuclear power plants and applies the PSA in making design decisions to determine system configuration. 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. AECL uses the PSA results in Both ACR-700 and ACR-1000 to identify the complementary design features as per RD-337

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.

2) Identification of Systems Important to Safety:

PSA results are used to identify systems and components important to safety, as per S-98 requirements, 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 S-99.

3) Generation of System reliability models from Risk models:

Industry is using the PSA models to derive the reliability models of the systems important to safety for the assessment and the reporting of the reliability of these systems as per S-98 and S-99 regulatory standards, respectively.

4) Severe Accident Management Guidelines:

Accident progression analysis performed for level 2 PRAs was used by COG to support the development of generic SAMG for the Canadian industry and then to customize it to each of the 7 operating stations in Canada.

The BBRA Level 2 framework provided input in support of the development of the Bruce Severe Accident Management Guidelines (SAMG).

5) Risk-informing outage planning and On-line Maintenance (EOOS Risk monitor):

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 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.

NB Power also has generated the risk monitor using EOOS.

8. Results and Insights from the PSAs

REGULATOR

The review of the completed PSA's 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.

The calculated Core Damage Frequency and Large Release Frequency for all completed PSA's are lower than 1E-4 and 1E-5 respectively which are in compliance with the safety goals as per IAEA INSAG-3 [17] as well as with the Industry safety goals.

- The review of Candu 6 Point Lepreau PSA showed that the fire events are the dominant contributor to the overall full power and shutdown state severe core damage frequency, whereas the flood events are minor contributors. The level 1 internal events PSA at full power showed that the dominant accident sequences represent the loss of gland seal cooling (LOCA-2) to all PHT pumps initiating event followed by the failure of ECC low pressure to provide PHT make-up, as well as the single channel flow blockage initiating event followed by the failure of ECC low pressure as a long term heat sink.

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.

OPG used the results of Darlington A Risk Assessment (DARA) to support a request for functional changes. Lately, OPG intends to use the PSA insights in defining define the scope of the refurbishment

Bruce Power 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. Design vulnerabilities were identified and resolved with the designers. The summed mean SCDF is 3.4E-7 occurrences per year, which is well within the design target. 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.

INDUSTRY

In the past years, the Industry used the results and insights from PSA to (1) demonstrate compliance with the industry safety goals and criteria as well as the assessment of the economic impact, (2) identify plant vulnerabilities, (3) operation management, and (4) operator training.

Lately, the Industry is using the PSA results and insights to (1) Risk Informed Integrated Safety Management System, (2) Plant configuration management through risk monitors, (3) help define the scope of the refurbishment for life extension projects, (4) support the applications for testing and maintenance intervals extensions, changes in the Operating Policies & Procedures (OP&P) and other submissions using probabilistic arguments.

As mentioned in the previous sections, AECL developed a design-assist PSA for ACR-700 and ACR-1000.

9. Future Developments and Research

Participation to International organizations

CNSC participates in the International Common-Cause data Exchange (ICDE) project. Canada's participation to Phase 6 of the ICDE project (2011 to 2014) is under review process by CNSC management. If Canada's participation is confirmed, a research contract with an external contractor for collecting data will be launched.

CNSC is also participating in the WGRISK-ICDE sub-task on quantification of the Common-Cause Failures using the ICDE data.

CNSC is also an active member in the International PSA Technical team operating CANDU-type reactors. The Technical team is under the auspices of the IAEA with the purpose to discuss PSA aspects specific for CANDU-type reactors and to identify subsequent steps needed for harmonization of PSAs for NPPs with CANDU-type reactors among Member States.

Research projects and contracts

In 2005, CNSC staff initiated a research project aiming to incorporate Ageing Effects into the PSA. 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 organizations.

The introduction of Regulatory Standard S-294 in the Licence adds requirements to address risk from external events (although non-PSA alternative methods are acceptable). It will be necessary to ensure that PSA methods are in accordance with best industry practice. CNSC issued contract for the review of Point-Lepreau Fire and Flood PSA. CNSC, also initiated a contract with a consultant for developing a Standard Operating Procedure for the review of PSA-Based SMA submissions.

Cooperation with universities

CNSC is fostering the cooperation with the Canadian based alliance of universities, the University Network of Excellence in Nuclear Engineering (UNENE). Potential areas for cooperation are:

- Incorporating the Ageing effect in the PSA models (time dependent failure rates);
- Maintenance optimization in the PSA and systems models;
- Inclusion of common cause effect into the PSA and System models;
- Uncertainty propagation in the PSA models;
- Common Cause Failure Quantification using the ICDE database.

Joint Workshops with the industry

After a series of meetings with the industry to address the PSA aspects required for the Reliability Program Implementation in all Canadian nuclear power facilities arising from Regulatory Standard S-98, CNSC staff identified the areas for further discussions:

- Process and tools for data collection
- Level 2 methods
- Treatment of uncertainty
- Efforts through industry groups to increase the degree of standardization of PSAs for Candu reactors
- PSA for external events
- Operational risk management practices and tools.

The multi-units operator, 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.

10. References

- [0]. Nuclear Safety and Control Act (NSCA), 2000.
<http://laws.justice.gc.ca/en/n-28.3/252272.html>
- [1]. Canadian Nuclear Safety Commission, Regulatory Policy P-299: “Regulatory Fundamentals”, April 2005.
http://www.nuclearsafety.gc.ca/eng/regulatory_information/documents/current_docs.cfm
- [2]. CNSC Regulatory Standard S-294: “Probabilistic Safety Assessment (PSA) for Nuclear Power Plants”, April 2005.
- [3]. CNSC Regulatory Document, R-7: “Requirements for Containment Systems for CANDU Nuclear Power Plants”, February 1991.
- [4]. CNSC Regulatory Document, R-8: “Requirements for Shutdown Systems for CANDU Nuclear Power Plants”, February 1991.
- [5]. CNSC Regulatory Document, R-7: “Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants”, February 1991.
- [6]. CNSC Regulatory Document RD-337: Design of New Nuclear Power Plants, September 2008.
- [7]. IAEA Safety Standard Series NS-R-1: Safety of Nuclear Power Plants: Design. IAEA, Vienna 2000.
- [8]. CNSC Regulatory standard S-98 rev 1: “Reliability Programs for Nuclear Power Plants”, July 2005.
- [9]. Canadian Nuclear Safety Commission, Regulatory Policy P-242: “Considering Cost-benefit Information”, October 2000.
- [10]. COG Risk and Reliability Working Group: “Interim Implementation Guidelines for CANDU Nuclear Plant Reliability Programs”, COG-05-9011. April 2006.
- [11]. COG BCA Industry Working Group: “Benefit-Cost Analysis Implementation Guidelines”. COG 01-003. January 2003.
- [12]. IAEA, Safety Series no.50-P-4, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Vienna, 1992.
- [13]. IAEA, Safety Series no.50-P-8, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Vienna, 1995.
- [14]. CNSC Regulatory Document RD-360: “Life extension of Nuclear Power Plants”, February 2008.
- [15]. US NRC, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (NUREG/CR-6928). February 2007.
- [16]. IAEA, “Basic Safety Principles for Nuclear Power Plants”. 75-INSAG-3 Rev 1, INSAG-12. IAEA, October 1999.

*Appendix B – Contact Information***Canada**

Regulatory Authority/Technical Support Organization	<u>Direct Contact</u>
Canadian Nuclear Safety Commission P.O. Box 1046, Station B 280 Slater Street Ottawa, Canada K1P 5S9	Raducu Gheorghe CNSC-CCSN 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@cnsccsn.gc.ca or raducu.gheorghe@cnsccsn.gc.ca
Regulatory Authority Website Address: http://www.nuclearsafety.gc.ca/	

3. CHINESE TAIPEI

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and environment

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's, some improvements inspired from 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 (ABWR) which is under construction and is scheduled to commercial operation in 2013, PSA was required and already included in PSAR and FSAR. Both PSA model included in Lungmen PSAR and FSAR were developed by the reactor vender, General Electric Company. An independent living PSA model was also developed by INER for future risk-informed applications. The scope includes at-power, low 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 for operating plants had completed the peer review process in 2001 using NEI 00-02^[10]. 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. In 2011, Taipower has completed the RI-ISI (risk-informed inservice inspection) program for all operating plants and also the extension for containment ILRT (integral leak rate test) program. Those programs will be submitted to TAEC for approval during 2011.

Several projects were initiated for further risk-informed applications after the pilot study of 1997. The risk monitor (TIRM)^[11] developed by INER and Licensee was first released in 1999. The second generation (TIRM-2)^[12] was released in 2002 which includes the LERF evaluation with the enhancement of calculation speed and accuracy. The inspection tool (PRiSE)^[13] 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 Δ CDF was calculated by resolving PSA model in less than one minute.

3. Numerical Safety Goals

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 license from TAEC, the Licensee should demonstrate in FSAR that the new built plant meets the safety criteria.

4. PSA Standards and Guidance

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^[14] 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^[10]. In order to extend the application area, INER revised those PSA models according to the suggestions from the peer review. The subsequent peer review process will be completed in 2012. This time, those PSAs will be reviewed per both ASME^[15] standards.

5. Status and Scope of PSA Programs

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 vendor. The living PSA of Lungmen conducted by INER has completed in 2007. The scope is the same with the operating NPPs.

6. PSA Methodology and Data

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^[16] 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^[17]. 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-6268^[18].

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^[19], NUREG-1829^[20], NUREG/CR-6928^[21] and EGG-SSRE-8875^[22] with plant specific data collected from 1994 to 2006 are used to estimate the initiating event frequencies and component failure probabilities. Generic data is updated by plant specific data

using Bayesian update.

7. PSA Applications

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, Kuosheng and Maanshan. 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 applications and the associated design changes to the cable tray fire wrapping of Chinshan, Kuosheng and Maanshan.

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 determine the future regulatory plans in response to the inspection findings.

Risk-Informed Inservice Inspection Program: A pilot study on the development of RI-ISI program for Kuosheng RHR system was performed in 2003 by INER. The study checked the methods developed by EPRI and WOG to show the technique required in each step of those two methods. In 2009, Taipower decided to transfer to RI-ISI program from the fourth inspection interval for Chinshan, Kousheng and Maanshan. The scope of the RI-ISI programs will be limited in Class 1 and 2 piping welds using the method of EPRI TR-112657 Rev B-A^[23]. The RI-ISI programs are scheduled to submit to TAEC for approval in 2011.

8. Results and Insights

The latest PSA update was completed in 2007 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. After collecting plant specific operating data from 1994 to 2006, 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.

9. Future Developments and Research

The ongoing project of operating NPPs is the peer review of the living PSA models per ASME standards and the model update response to the comments of peer review. The project for Chinshan, Kuosheng and Maanshan will be completed in 2011 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 2012, near the startup test of this new ABWR.

The three operating NPPs implement the Maintenance Rule at the beginning of 2007. The results from PSA were 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. PSA will also be used to evaluate the maintenance configuration risk during online maintenance.

10 Reference (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. Nuclear Energy Institute, "Probabilistic Risk Assessment Peer Review Process Guidance," NEI-00-02, Revision A3, March 20, 2000.
 11. 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.
 12. 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.
 13. 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.
 14. 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.
 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, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6268, February 2007.
 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. USNRC, "Estimating Loss of Coolant Accident (LOCA) Frequencies Through the Elicitation Process," NUREG-1829, April 2008.
 21. Idaho National Engineering and Environmental Laboratory, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, February 2007.
 22. Idaho National Engineering Laboratory, "Generic Component Failure Data for Light Water and Liquid Sodium Reactor PRAs," EGG-SSRE-8875, February 1990.
 23. EPRI, "Revised Risk-Informed Inservice Inspection Evaluation Procedure," TR-112657 Rev. B-A, December 1999

Appendix B

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. Chun-Chang Chao	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:6008 Fax: +886-3-471-1404 Email: chuncchao@iner.gov.tw	

4. CZECH REPUBLIC

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and environment

There is no explicit legal requirement to perform PSA studies by licensee in the Czech Republic. Czech regulatory body is building up its own position in this field and therefore PSA activities are mainly initiated by utility based on concrete NPP needs, experience of other countries and consideration of regulatory recommendations. The PSA activities are conducted to enhance the safety level of the plant operation in the frame of existing safety culture environment. The long-term (10 years) operation licence includes the requirement regarding Living PSA and risk monitoring to be performed.

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 PSA Level 1 and Level 2 analyses were started in 1993 and completed in 1996 by developing the real time risk monitoring tool for NPP Temelin for all operating modes and both internal and external events including seismic risk . All Temelin original models were updated in time period 2002 to 2003 to ensure that information and assumptions used in the original PSA still reflects the ultimate design and construction of the plant. This effort provided the risk model that is suitable for both PSA applications and use in licensee-related work.

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

The QA systems implemented within the studies include both 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 or IPSART missions within 1993 to 2003.

3. Numerical Safety Goals

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 explicit 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 have been applied. However, new more conservative criteria based on risk are proposed, where

1) the licensee-initiated change is allowed as long as the risk increase is small, i.e.: ΔCDF or ΔFDF (when the change would have impact on spent fuel pool) $< 5 \times 10^{-6}/\text{y}$ **AND** $\Delta\text{LERF} < 1 \times 10^{-6}/\text{y}$

AND

2) the licensee-initiated change resulting in risk increase should not be allowed, when the overall FDF (including risk from spent fuel pool) exceeds (or is going to exceed) $10^{-4}/\text{y}$ **OR** the overall LERF exceeds (or is exceeding) $10^{-5}/\text{y}$ (to fulfill INSAG 12 objectives).

4. PSA Standards and Guidance

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 and evaluation for the purpose of PSA”
- Me 457, rev. 0“Guideline for use of Safety Monitor”
- 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 instructions were developed within 2004 to 2010 in the frame of “PSA Applications Project”. The instructions are as follows:

- VDMI 092 - QA Procedures for the Use of PSA
- VDMI 093 - Guideline for Independent Review of PSA
- VDMI 102 - Requirements for PSA of NPP operation
- VDMI 110 - Methodology for Use of PSA in Risk Informed Decision Making for Evaluation of Technical Specification Changes Submitted to SÚJB.

A new edition of SUJB notice /No.195/ is under preparation, where development of Level-1 and Level-2 PSA is required as mandatory for Czech NPPs, with the scope covering all operational states and all internal initiating events and hazards and external hazards, both natural and human induced.

5. Status and Scope of PSA Programs

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 and human induced external events, reflect all power plant modifications and are valid for all operating states. These models are developed as specific for each plant unit. RiskSpectrum PSA /RS PSA/ 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 consequential 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 from 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. This model was extended to all units as well as to hot shutdown plant operational mode.

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 including shutdown and internal and external events and updated in 2002-2003. A Level 2 analysis has been included in the scope of the analysis.

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. The WinNUCAP code was used for Temelin Level 2 PSA development and quantification.

An update of the Temelin PSA is done, as required, 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.

6. PSA Methodology and Data

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 guidelines (NUREGs, IAEA guidelines, other PSAs, etc. [4, 5, 6]) have been considered for this purpose.

The PSA for Dukovany consists of unit specific models. The RiskSpectrum PSA 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 2010, the whole plant operation was split into 14 Plant Operating States (POS's) in the PSA model. The comprehensive set of 33 initiating event (IE) groups has been defined. Each IE group contains one or more sub-events, 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 /after 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 Sciencetech 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.

Currently, a plant specific data gathering system is being used to enable flow of data into the PSA models as soon as sufficiently representative statistical sample is available for various populations of components. In 2010, plant specific reliability data were used partly for the first time during regular update of PSA quantitative inputs, resulting in decreasing of conservativeness of overall results in comparison with the results of PSA model based on purely generic data.

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.

7. PSA Applications

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 -2000 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. TS changes necessary to allow relocation of scheduled maintenance from refueling outage to power operation were evaluated in UJV Rez using current PSA model for NPP Dukovany as well. [22], [26].

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:

$$\text{ICCDP} = \Delta\text{CDF} \times \text{AOT} < 5 \times 10^{-7}$$

$$\text{ICLERP} = \Delta\text{LERF} \times \text{AOT} < 5 \times 10^{-8}$$

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.

The Czech Regulatory Body (SUJB) has issued an instruction (VDMI) for the more comprehensive evaluation of TS licensee initiated changes. It is based on three-tiered approach and criteria from RG 1.177.

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 Essential Service Water system. For the risk informed AOT application, RG 1.174, RG 1.177 methodology and acceptance criteria from Czech regulatory body have been adopted.

Event Sequence Analysis: 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.

RI-ISI: 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.

Operational Risk Monitoring: 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. 3.5a (CZ) software installed in the plant LAN environment TEMNET in 2003 and DUKNET in 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 negotiations 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 prior outages beginning. Recommendations are given to the outage schedulers for plant configuration control, as soon as the instantaneous risk exceeds given criteria.

In addition, the planned schedule vs. real outage configuration risk profiles is compared at both plants 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 five 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.

Other applications connected with everyday operation: Both plant PSA models as well as Safety Monitors are used for

- Operation with equipment out of service
- Various LCOs in case of unavailability of equipment
- OLM, etc.

8. Results and Insights

Summary on Dukovany site

The basic living PSA models and related PSA applications tools are at Dukovany site updated regularly since 1996. The latest analysis results (end of 2010) are as follows:

Level 1 PSA - for a list of analyzed initiating events /fires, floods, heavy load drops and human-induced external events included/ and all operating states CDF ranges from $8,8 \times 10^{-6}/y$ to $1,1 \times 10^{-5}/y$ depending on the unit.*

The CDF for unit operation at power ranges from $4,3 \times 10^{-6}/y$ to $5,5 \times 10^{-6}/y$.

Main contributors /about 70 % of the CDF / of Dukovany risk level are:

- loss of natural circulation,
- small and medium LOCA initiators,
- reactivity accidents, cold overpressurization,
- main steam collector breaks.

Plant operating states with the highest contribution to the CDF are:

- POS 1 - Power and low power operation / 100% - 2% of nominal power/
 - contributes about 50 % to the CDF
- POS 8 – RCS Drainage before refueling
 - contributes about 14% to the CDF
- POS S13 - reactor startup with RCS hydrotests
 - contributes about 18% to the CDF

Level 2 – for plant unit at power operation and hot shutdown operation an estimation of LERF is, depending on the plant unit, $1,1 \times 10^{-6}/y$ - $1,3 \times 10^{-6}/y$.

* CDF at power and hot shutdown operation is $5,2 \times 10^{-6}/y$ to $6,5 \times 10^{-6}/y$.

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 0.1×10^{-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.

Summary on Temelin site

Level 1 - at power results

The Level 1 - internal events model has been updated during 2002-2003. 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 1.49×10^{-5} /year.
- LOCAs contribute 4.5×10^{-6} /year (31%), primary to secondary leakage events 3.6×10^{-6} /year (24%) and transients 6.7×10^{-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 (POSSs), 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 POSSes 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 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.

Currently the update of internal events PSA models in Temelin is ongoing followed by all other models update to reflect the specific operational experience as well as operational and design changes performed during the time.

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.

9. Future Developments and Research

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

Continuation of pilot activities on use and implementation of RI ISI methodology, which would allow using this approach in real operational practice.

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

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. Patrik 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 International conference 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., Patrik 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.
26. Husťák S., Pištora V.: Application of Risk-Informed Evaluation on the Selected Changes in NPP Dukovany; PSAM10, Seattle, U.S.A., June 2010

5. FINLAND

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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 YVL A7. 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 A7 devotes special attention to use of various risk informed PRA applications such as risk - informed inservice inspection (RI-ISI), risk - informed inservice testing (RI-IST), risk – informed technical specifications (RI-TechSpecs) and risk - informed safety classification. It gives also 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.

3. Numerical safety criteria

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 A7 “Probabilistic risk assessment 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 5×10^{-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.

4. PSA standards and guidance

The requirements on the use of PSA for the risk informed regulation derives from the Degree level through 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 YVL A7.

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.

5. Status and scope of PSA programs

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 committed 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. The current Regulatory Guide YVL A7 extends the use of PSA to the pre-commissioning tests and the decommissioning of the plant unit

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.

6. PSA methodology and data

The licensee performs 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 may 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.

Example of analysis of dependencies: 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 and installation 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 plant 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. Lately the MELCOR code has replaced the MAAP code.

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/FinPSA, 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.

7. PSA applications

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 and personnel training.

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.

In drawing up pre-commissioning test programmes, the PRA shall be used to assess the coverage and balance of the programmes as well as to reduce risks arising from pre-commissioning tests.

STUK reviews the construction phase PSA and applications before giving a statement about the operating licence application.

TVO in cooperation with AREVA 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 A7 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.

Nuclear power plant's decommissioning: The decommissioning-related risks shall be analyzed and submitted to STUK for approval in good time before the plant's power operation ends.

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.

8. Results and insights from the PSAs

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 $1.9 \times 10^{-5}/a$
 - internal initiators, $4.5 \times 10^{-6}/a$
 - fires, $8 \times 10^{-6}/a$
 - internal floodings, $2.8 \times 10^{-6}/a$
 - harsh weather conditions, $3.1 \times 10^{-6}/a$
 - seismic events, $1 \times 10^{-7}/a$
- Shut down mode $2.7 \times 10^{-5}/a$
 - internal events, $2.2 \times 10^{-5}/a$
 - flooding, $4.4 \times 10^{-7}/a$
 - harsh weather conditions, $4.9 \times 10^{-6}/a$
 - seismic events, $4.6 \times 10^{-8}/a$

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 $2.5 \times 10^{-5}/a$ covering internal events, internal flooding and harsh weather conditions at all operating states. The majority of the risk comes from heavy load drops, boron dilution accidents, oil accidents and leakages in cold states.

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 (1.7×10^{-3} 1/a).

- In the original level 1 PSA 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 $3.3\text{E-}04$ 1/a, and the total core melt probability to $9\text{E-}04$ 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 $1.2\text{E-}05$ 1/a and the total core damage estimate to $6.0\text{E-}04$ 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 $2\text{E-}04$ 1/a to about $1.0\text{E-}05$ 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 $1.3\text{E-}04$ to $1.9\text{E-}05$ 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 suction 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 $5.4\text{E-}05$ /a to $1.4\text{E-}05$ /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.

Summary of Olkiluoto PSA programme

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 $3.5 \times 10^{-6}/a$. 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.

All operating modes Total: $1.2 \times 10^{-5}/a$

Power operation Total: $9.1 \times 10^{-6}/a$

- internal initiators, $5.4 \times 10^{-6}/a$
- fires, $2.2 \times 10^{-6}/a$
- internal floodings, $1.1 \times 10^{-7}/a$
- harsh weather conditions, $1.2 \times 10^{-6}/a$
- seismic events, $1.7 \times 10^{-7}/a$
- missiles, $3.7 \times 10^{-8}/a$

Shut down mode Total: $5.6 \times 10^{-7}/a$

- internal events $3.5 \times 10^{-7}/a$
- fires, $2.1 \times 10^{-7}/a$

Planned Shutdown Total: $1.3 \times 10^{-6}/a$

Runup Total: $1.3 \times 10^{-6}/a$

*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 result 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 uncover 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 $1.9 \times 10^{-5}/a$. The total core damage frequency including all identified initiating events and changes made due to the regulatory review was $3.34 \times 10^{-5}/a$. 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 $4 \times 10^{-6}/a$.

9. Future developments and research

SAFIR 2014 Nuclear Safety Program includes several into future looking projects as like

Human reliability analysis

HRA research consists of two tasks: participation in the international EXAM-HRA project and HRA method development. EXAM-HRA is a Nordic-German project aiming at providing guidance on performing HRA, based on a survey of the HRA practices in Finnish, Swedish and German nuclear power plant probabilistic risk assessments. During 2011 a survey is conducted based on the method developed in 2010. VTT will also contribute to method development in the area of performance shaping factors (PSFs) for contextual HRA.

Passive systems reliability

A review will be made concerning what passive safety systems current or planned nuclear reactors in Finland have, in what scenarios and how they affect safety, and how passive systems have been analyzed. Part of the task for 2011 is to plan the research for years 2012-2014, based on the review and

participation to the DPSA workshop organized partly in task 2.1 Dynamic level 2 PRA. Development of an analysis method for passive systems is closely linked with the progress of task 2.1 Dynamic level 2 PRA.

Dynamic level 2 PRA

In 2011, a review will be made of the state of the art and research priorities in Dynamic PSA modelling and reliability analysis of deterministically driven systems (e.g. severe accident phenomena and passive safety systems). A feasibility study for connection between Dynamic PSA and conventional PSA will also be performed. This subject is closely linked to the more general subject of integrating deterministic and probabilistic safety assessments (DPSA). KTH, ScandPower (part of Lloyd's Register) will jointly organize a DPSA workshop in October 2011. The workshop will be held at Otaniemi, Espoo, and practical matters will be handled by VTT. Funding of the workshop is planned to be by NPSAG, NULIFE and participation fees.

Level 3 PRA

In the level 3 PRA and risk criteria subtask, the target is to investigate and develop the calculation approach for risk evaluation in the case of a radioactive release to the environment. Methods to estimate risk to the society in addition to an individual are studied taking into account realistic approach. Task will be started in 2012.

Imprecise probabilities in PRA

The task develops a method for using probabilities stated as confidence intervals in fault tree analysis, where the risk associated with the failure of a component is evaluated with traditional risk measures. Computational environment for the method is implemented and the method is applied to realistic test data from a fault tree of a nuclear facility. The method and its application are described in a manuscript, which will be submitted to an international journal.

Risk communication

Risk communication is an integral part of risk management. In 2011 the task includes a literature review of practices and guidance on risk communication in the area of reactor safety and spent nuclear fuel management. In addition, a plan for future work in this topic will be made for 2012-2014. As international co-operation is important in this field, participation in, e.g., nordic seminars will also be aimed at in future work.

Development and use of fire-HRA method

The existing Fire-HRA method will be further developed and applied on TVO cable tunnel/room scenario for realistic demonstration and testing. Additional input data will be collected to account for observed anomalies due to the assumed uniform distributions for performance timings. New timings will be based on triangular or other more realistic distributions. The work will be published in international literature.

The Fire-HRA method will be applied on the assessment of defence-in-depth elements during the later years of the project.

Assessment of defence-in-depth

The elements of the defence-in-depth principle in fire protection are specified in the context of the risks associated with large fire loads at Finnish NPPs. The methods to evaluate the fulfillment of defence-in-depth principle are studied. The use of fire event tree for this purpose is studied. The connections to (fire) safe shutdown analysis, as presented by U.S.NRC 10 CFR, Part 50, Appendix R, are examined.

Sea level scenarios for the Finnish coast

The effects of thermal expansion, melting of glaciers, local land uplift and Baltic Sea water balance are combined to update the scenarios for the sea level on the Finnish coast. The 124-year long observed sea level time series, as well as climate model runs of the IPCC Fourth Assessment Report are utilized. The resulting scenarios, their scientific basis, as well as an expert judgment of different factors affecting them, are collected in a scientific article and submitted to an international peer-reviewed journal.

10. References

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
18. 2007 ASME Boiler & Pressure Vessel Code XI. Rules for Inservice Inspection of Nuclear Power Plant Components. Nonmandatory Appendix R Risk-Informed Inspection Requirements for Piping. July 1, 2007.
19. Bergroth, N., Jänkälä, K.E. & Ovcienko, S. Oil spill risk assessment for Loviisa power plant. Proc. Probabilistic Safety Assessment and Management, PSAM 8, May 15-19, 2006, New Orleans, USA.

Contact

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

6. FRANCE

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

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.

3. Numerical Safety Criteria

For 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 damage 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 new 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

- « practical elimination » of sequences with potential for large early releases.

The Safety Authorities considered that implementation of improvements in the "defence-in-depth" of such plants should lead to the achievement of a global frequency of core damage of less than 10^{-5} per plant operating year, uncertainties and all types of failures and hazards being taken into account.

In order to fulfill 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.

4. PSA Standards and Guidance

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.

5. Status and Scope of PSA Programmes

History

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 Nuclear 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). Moreover the designer AREVA is also developing PSA mainly for export. These activities concern the development of PSA models and methods, as well as PSA applications for various safety analysis problems. Moreover, for the project of a new 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 MWe 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 were used for the review of the level 1 PSA performed by EDF in the framework of the Periodic Safety Review of the 900 MWe 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 in 2006. The study has been updated in 2010 in order to be used in the frame of the third Periodic Safety Review of these plants. The study is also used to develop the fire PSA for the 1300 MW NPP (to be accomplished in 2011).

Level 1 PSA for 1450 MWe (N4) reactors

The level 1 PSA for N4 reactors is now under development (to be accomplished in 2012).

Level 1 PSA for EPR

The study is under development. The preliminary study was used to assess the Flamanville 3 (FA3) EDF EPR study presented in the frame of the anticipated instruction of the application for commissioning (2010). The study is now under updating to incorporate the latest design information (mainly I&C). The study is also used to develop the IRSN Level 2PSA.

Level 1 PSA for EPR spent fuel pool

The PSA study of the EPR spent fuel pool is now under development. The study will be mainly used to analyze the similar study which will be presented by EDF in the frame of the application for FA3 EPR reactor commissioning.

Fire PSA for 900 MWe NPP

A version of the fire PSA for 900 MWe was performed in 2004 taking (ou “. It takes”) into account the event oriented operating procedures.

In 2004, results obtained in the framework of the Fire PSA activities were used for the review of 900 MWe fire protection improvements.

Fire PSA for 1300 MWe NPP

The development of the study is ongoing. This study should be available for the third Periodic Safety Review of these plants (2011).

Level 2 PSA for 900 MWe and 1300 MWe NPP

Level 2 PSA for 900 MWe PWR series : the study, extended to “level 2+”, has been updated in 2003, 2007 and 2008, and applied in the framework of the Periodic Safety Review of the 900 MWe plant series. Last version was issued in April 2009. Activities now concern analysis of some dominant risks.

Level 2 PSA PSA for 1300 MWe PWR series : the first version of a LEVEL 2 PSA has been developed with the objective to use the conclusion during the preparation of the third Periodic Safety Review of these plants (2010-2012) (achieved for power states of reactor, in progress for shut-down states)

Level 2 PSA for EPR Flamanville : a Level 2 PSA is now being developed.

PSA development in EDF*Level 1 & 2 PSA for 900 MWe NPP*

The level 1 & 2 internal events PSA for 900 MWe plant series (CPY series) was last updated in year 2007. It includes specific models for BUGEY and FESSENHEIM NPPs (CP0 series).

Those PSA were discussed with the technical Support in the framework of the preparation of the next Periodic Safety Review of the 900 MWe plant series. The last updates / upgrades of the 900 MWe plants include the plant modifications decided after this periodic safety review.

Level 1 PSA for 1300 MWe NPP

The Level 1 internal events PSA for 1300 MWe NPP was last updated in 2008. It takes into account the plant modifications decided during the second periodic safety Review of the EDF 1300 MWe plant series and the most recent experience feed-back.

This model was extended to Level 2 in 2008.

In parallel, the scope of level 1 PSA was extended to Fire, Internal flooding and earthquake in 2010.

Those PSA will be discussed with the technical support organisation (IRSN) in the frame of of the next Periodic Safety Review of the 1300 MWe plant series.

Level 1 PSA for 1450 MWe NPP

Last update of Level 1 PSA for 1450 MWe NPP was achieved in 2007 . It takes into account Safety Authority expectations, future uses of PSA for AOT calculations and a preliminary assessment of containment failure (Level 1+ PSA) and the plant modifications decided during the preparation on the first periodic safety Review of the EDF 1450 MWe plant series.

All level 1 PSA developed by EDF include accidents occurring in the spent fuel pool.

PSA for EPR project (Flamanville 3)

A Level 1 PSA and a simplified Level 1+ PSA (containment failure assessment) was developed for the Preliminary Safety Assessment Report in 2006. This PSA was based on the PSA developed during the EPR basic design and took into account Safety Authority expectations.

For the purpose of commissioning the plant of Flamanville 3, EDF developed a full scope level 1 and level 2 PSA for this plant. All reactor modes are addressed in the PSA (from full power operation to shutdown modes including accidents in the spent fuel pool).

Internal events as well as internal (fire, flooding, explosion,..) and external hazards (earthquake,..) are studied. Scenarios leading to releases without core melt are also included in the PSA studies.

Those PSA were transmitted to the regulator from 2009 to 2011.

6. PSA Methodology and Data

Overall methodology:

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.

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 modeled 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 energy phenomena, which are likely to occur during severe accidents, are much greater than the uncertainties that concern level 1 model. Therefore, level 2 model focuses on the main energy 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 estimates” 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 : > 450 PDS in last version

- A specific CT Quantification software : KANT – developed by IRSN – 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 hydraulic 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 RC
- A very fast model for release assessment based on experimental results or ASTEC calculation
- In progress work to assess radiological consequences for each RC in relation with Emergency Crisis Center tools.

Common cause failures:

The multiple greek letters 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 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 a particular attention was paid to the modelling of supporting systems and of recovery possibilities, including the shared equipment with another unit.

7. PSA Applications

Use of PSA for reducing the risk related to dominant contributions

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 at demonstrating 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 has increased with the introduction of PSA level 2 and of Fire PSA (IRSN). 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.

Use of PSA for Beyond Basis Design Accident

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 according to 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. This application is performed for each periodic safety review, the list of the Beyond Basis Design Basis features being updated according to the data and knowledge evolution.

In 2005, the results of this application have been discussed by EDF and IRSN and eventually approved by ASN. Since then, it was applied to all series (900 MWe, 1300 MWe and 1450 MWe) on routine basis.

Similar methodology is used for the EPR at the design stage in order to define the Risk Reduction Categories (RRC-A) domain and associated design features.

For EPR Flamanville 3, some difficulties with the method appeared and led to methodological changes which were presented to ASN in 2010.

Probabilistic analysis of Operating Events

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 CDF (Core Damage 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 CDF 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.

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.

Other PSA applications for operating plants

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 exemption request .

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 presentation to the standing advisory committee led to some methodological changes. These changes include the way to take into account the safety benefit which can impact different accident scenarios (core damage, early releases,...).

The updated methodology was transmitted to the regulator in 2011. EDF is planning to use it for the assessment of possible plant modifications for the next periodic safety reviews (1300 MWe and 900 MWe) and for the life time extension program.

PSA applications for EPR Flamanville 3

During the design stage, PSA contributions addressed the following items :

- designing and optimizing the facility during the design phase and life of the site,
- confirm the well-balanced risk profile of the design,
- broaden the deterministic design scope of systems, with specific beyond-design analysis (multiple failures conditions),
- justify the maintenance planning,
- support the severe accidents analysis,
- confirm the protections from external and internal hazards,
- assess the safety level increase compared to existing plants.

During commissioning of Flamanville 3, PSA will be used essentially to support the development of technical specifications.

8. Results and Insights from the PSAs

The results of the 1990 PSAs (level 1, internal events, all plant operating modes) were the following:

900 MWe plant: CDF = $5 \cdot 10^{-5}$ / reactor x year

1300 MWe plant: CDF = $1 \cdot 10^{-5}$ / 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 several times by both IRSN and EDF. Moreover the scope was extended to the level 2 (IRSN and EDF) and to some internal and external hazards (internal flooding, fire and earthquake for 1300 MWe (EDF), fire and feasibility study of earthquake and internal flooding for 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 CDF 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.

9. Future Developments and Research

PSA development in EDF

In the future, EDF will continue to update/upgrade the PRA models on a periodic time frame. The major projects in the near future are the following

In 2010, the update of level 1 internal event PRA for 1450 MWe started. It will be transmitted to the regulator and discussed with the TSO in the frame of 2nd periodic safety review of this series.

In 2011, the works to update the 900 MWe PSAs will start in order to prepare the 4th periodic safety review. The Level 1 PSA coverage will be extended to earthquake, fire and internal flooding. Level 2 PSA will also be updated. PSA models will be an important tool for the discussions about the life time of the existing fleet.

In parallel, discussions will take place about the 1300 MWe PSA (including fire, earthquake and internal flooding) in the frame of 3rd periodic safety review of this series. The upgraded cost/benefit analysis method will be applied to assess possible plant modifications.

As far as EPR Flamanville 3 is concerned, the model will continue to be updated in order to be consistent with the most recent status of the plant and to take into account the most recent documentation (upgrade of human reliability analysis based on simulator observations and on final version of EOPs).

PSA development IRSN

Level 2 PSAs development and updating

The updating of level 2 PSA for the French 900 MWe PWR is on-going in IRSN

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 modeled 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. On écrit au conditionnel avec des dates passées

Fuel Pool PSA

PSA were performed at EDF to assess the risk of core uncovering 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. These accidents are now performed and regularly updated for all EDF nuclear series.

Fire PSA

Fire PSA for EPR: The study is planned in the next future.

Ageing PSA

Investigations are in progress at IRSN for introducing ageing effects in PSA models. A workshop was organised (in cooperation with JRC-Petten) in October 2005.

A feasibility study was done in 2010. The future “ageing” PSA study will be limited to the incorporation of the maintenance data and the operating experience in the existing 900 MWe plants PSA model. The model will be then used in the frame of the review of the NPP life extension EDF project.

Hazards PSA

For the internal flooding PSA, a feasibility study was done. The development for EPR is planned in the next future.

For the seismic PSA a preliminary feasibility study was done. The development of the methodology is ongoing.

PSA for research reactors

For the PSA for research reactors a feasibility study was done. The study for Jules Horowitz Reactor (RJH) will be developed in the future..

PSA for new designs

In 2010, the CEA decided to carry out studies in support to the design of the prototype (named ASTRID) of French GEN IV Sodium Fast Reactors.

These studies consist in:

- reliability assessments of specific systems: Reactor Shut Down systems, Decay Heat Removal systems... These studies have been based on data from the European Fast Reactor project and equivalent studies will be performed using the ASTRID design;
- developing a preliminary level 1 PSA in collaboration with his industrial partners EDF and AREVA-NP. In the pre-conceptual design phase of the ASTRID reactor, this PSA will mainly focus on the aspects guiding the design: impact on core damage frequency of an additional shutdown system and of its various architecture, on sensitivity studies of various means and architecture used to remove the decay heat, on comparison of Energy Conversion Systems (water/steam and gas) and on the prioritization of R & D efforts on severe accidents.

The CEA participates in two IAEA projects which aim at obtaining a consensus on a methodology for the reliability of passive systems, to enable their treatment by PSA and the comparison with active safety systems. The methodology proposed by CEA has been applied to a Decay Heat Removal system, working in natural circulation, of the 2400 MWth Gas-cooled Fast Reactor and has been compared with methodologies proposed by other partners. Outcome of this work will be used for introducing DHR passive system in the PSA of ASTRID.

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.

PSA Methodology

In the last five years, some methodological works were performed on various subjects :

- Fire PRA : EDF adapted the EPRI/NRC methodology to the French context and specific needs. It was applied for 1300 MWe series Fire PSA. The feed-back from this first application will be used to upgrade the methodology.

- EDF piloted the EPRI guidelines for treatment of uncertainties for PRA level 1 and 2 internal events and adapted the methodology to the specificity of EDF PSA models. This methodology is now applied for each PSA update.
- Development of a specific software architecture for level 2 PRA (Risk Spectrum Professional + Crystal Ball). This architecture was used for the update of Level 2 900 MWe PSA and for development of 1300 MWe PSA.
- Modelling of I&C in PSA : in the frame of EPR PRA development, some new developments were carried out to improve the EDF reference approach which is called "compact model". These development include the modelling of initiating events induced by spurious actuation of I&C, of man-machine interface and some work to improve the way to address digital I&C. Some works to implement a more detailed modelling is under progress in order to address the needs of specific applications.
- Common Cause Failure Parameters : the goal of these development is to complete a method able to cover all possible situations including those when EDF experience feedback show no evidence of common cause events.
- HRA : methodological developments were performed in different areas such as Fire PRA, Level 2 PRA, pre-accidental HRA, enlarging the scope of EDF reference method MERMOS.
- Intersystem CCF : together with EPRI, a method consistent with NUREG CR-5485, was developed in order to assess the adequacy and the potential impact of modelling such CCF. The different pilot studies performed with this new methodology show that the impact is negligible in comparison to intra-system CCF.
- Some works are also performed to make possible the integration of all initiating events (including hazards) in the PSA model with a medium-term objective to have a modular PSA, facilitating further updates and collaborative work of different teams on the same model.

Most of these methodological developments were presented to different PSA conferences (PSA 08, PSAM 2008, PSAM 2010 and PSA 2011).

In support of these activities, EDF has increased its participation to some initiatives with a medium long term target to improve consistency with different methods and to support harmonization of practices. It includes participation to IAEA PSA safety guides, to WG Risk activities (DICREL, ICDE,..), to EPRI scope and quality group. EDF was also one of the organisation at the origin of the creation of HRA society. In 2010, two engineers from EDF were accepted as international members of the ASME/ANS JCNRM (Joint Committee for Nuclear Risk Management) which is in charge to follow the standard development for PSA in the USA. 3 EDF engineers have also participated to 2 peer reviews of American PRAs (Calvert Cliffs and Prairie Island) as active evaluators.

IRSN methodology developments were presented during several international workshops and meetings, in particular:

- CSNI/WGRISK workshops and task groups
- PSA 2008 and 2011 Meetings
- PSAM 9 and PSAM 10 meetings

IRSN continues the coordination of the ASAMPSA2 project of EC 7th FP, aiming at drafting the best-practices guidelines for development and applications of Level 2 PSAs.

A draft version of the guideline has been established and transmitted for external review to EU organizations and members of CSNI/GAMA, WG-Risk and SARNET. The final version will be published in October 2011. An international workshop was organized in March 2011 in Espoo, Finland.

10. References

- . CSNI Seismic PSA Workshop – Jeju Island (Korea) – 6-8 November 2006
- . CSNI Severe Accidents Management measures – Willingen (Switzerland) – 26-28 October 2009
- . PSA 2008 – Knoxville (USA) – 7-11 September 2008
- . PSA 2011 – Wilmington (USA) – 14-17 March 2011
- . PSAM 9 – Hong Kong (China) – 18-23 May 2008
- . PSAM 10 – Seattle (USA) – 7-11 June 2008

Appendix B – Contact Information

Technical Support of the Regulatory Authority	<u>Direct Contact</u>
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@irsn.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

7. GERMANY

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

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 (NPP). Particularly, the installation of accident management measures - as a fourth level of defence - was initiated as a result of PSA insights.

Since 1989 "Periodic Safety Reviews" (PSR) have been performed for all operating NPP in Germany. For most of them, the first 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, "Level 1+" PSA has been an essential part of the assessment in the frame of PSR.

In the German PSA Guideline and its corresponding technical documents on PSA methods and data, first published in 1996, scope and methods of PSA to be performed in the frame of PSR have been described. Level 1+ PSA was to be performed for full power states, not including internal and external hazards. The "+" in the term "Level 1+" indicates the fact that the active functions of the containment isolation are included in the analysis.

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

An update of the German PSA Guideline [BMU 05] along with the corresponding technical documents on PSA methods [FAK 05] and data [FAK 05a] was published in 2005. This requires that a Level 2 PSA is carried out for full power operation and a Level 1 PSA for full power as well as for low power and shutdown states where the scope of the PSA includes internal and external initiating events, in particular internal fire and flooding, as well as - depending on the site specific situation - external hazards such as flooding, explosion pressure (blast) waves, seismic events and aircraft crash. Major goals of updating the guideline were to extend the scope of PSA, to include state-of-the-art methods and data, and to help to make PSA for different plants more comparable. Guidance on probabilistic analyses of other external hazards, in particular from extreme weather conditions, is not covered.

All operating NPP in Germany have performed PSA in the frame of PSR with varying scope depending on the requirements valid at the time of PSR (see Appendix A). Those NPP still under operation after the accelerated phase-out outlined in the recent amendment of the Atomic Energy Act in 2011 after the Fukushima reactor accidents have performed full-scope Level 1 PSA and Level 2 PSA for power operation according to the German PSA Guideline.

In Germany there is no formalized approach to apply the results of PSA to be performed for all NPP. The objective of the PSA is mainly to confirm the robustness of the deterministic design of the NPP, to identify design and/or operational weaknesses (if any), and to address these weaknesses if necessary. 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. In that way, deterministic and probabilistic approaches are used in a complementary way.

Up to now, there is neither a unified approach of the utilities how to apply PSA insights for decision making on operational issues nor a formally issued federal regulatory policy on PSA nor has a risk informed approach formally been introduced.

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.

Because new-builds are legally not permitted in Germany, the use of PSA for design purposes is not foreseen. Vendors based in Germany, however, do apply PSA for design purposes according to internal rules and the respective national requirements.

The German operators have stated that they intend to increasingly use risk information for internal decision making although there are no federal regulations for that purpose. Some state regulators have defined procedures for risk informed decision making for a number of applications including assessment of backfitting applications, optimization of testing intervals, etc.

Prior to 2011, at least one German NPP intended to use a risk monitor.

Currently, activities for developing a first consistent approach for integrated risk informed decision making (IRIDM) potentially to be implemented in the German supervisory process on the federal level in the future are ongoing.

As per definition, Level 2 PSA deals with beyond design basis issues. Therefore, the existing legal framework does not provide direct impact of Level 2 PSA results on decisions within the regulatory process. Level 2 PSA results have particularly been used to estimate off-site consequences of severe accidents and for assessing the effectiveness of offsite emergency preparedness.

3. Numerical Safety Criteria

There are no numerical safety criteria related to PSA results defined on the Federal German level. However, for the assessment on PSA results from PSR, the regulatory authorities of the local states ("Länder") have applied CDF reference values for new-built plants as stated in IAEA SSG-3 [IAE 10].

Full scope Level 1 PSA results for any individual German NPP are clearly far below the target value for core damage frequencies (CDF) of operating plants ($CDF < 1 \text{ E-}04/\text{a}$) issued by IAEA. The ascertained values are even already lower than the values recommended for evolutionary reactors ($CDF < 1 \text{ E-}05/\text{a}$). The present results of Level 2 PSAs show also very low probabilities for large release and large early release frequencies of fission products.

4. PSA Standards and Guidance

In Germany, a PSA Guideline [BMU 05] has been developed along with the corresponding technical documents on PSA methods [FAK 05] and data [FAK 05a], all these having been updated in 2005. The scope is the following:

- Level 1 PSA for all plant operational states (full power as well as low power and shutdown states) for plant internal events and internal as well as site-specifically postulated external hazards,
- Level 2 PSA for full power operation for plant internal events.

Guidance and detailed requirements for internal hazards is only given for fire and internal flooding; for external hazards the detailed guidance is limited to external flooding, explosion pressure (blast) waves, seismic hazards and (accidental) aircraft crash.

Recently, detailed guidance is being particularly developed for low power and shutdown PSA including fire and Level 2.

5. Status and Scope of PSA Programmes

In the Atomic Energy Act of 2012 the dates when PSR results have to be submitted to the regulators are fixed (see the following table for NPP still in operation). The PSR has to be updated every 10 years.

Plant		Type / Electrical power (net) / Year of commissioning	Date of PSR
Grafenrheinfeld	KKG	PWR / 1275 / 1981	Oct. 2008
Gundremmingen B	KRB B	BWR / 1284 / 1984	Dec. 2007
Gundremmingen C	KRB C	BWR / 1284 / 1984	Dec. 2017
Grohnde	KWG	PWR / 1360 / 1984	Dec. 2010
Philippsburg 2	KKP 2	PWR / 1385 / 1984	Oct. 2018
Brokdorf	KBR	PWR / 1370 / 1986	Oct. 2016
Isar 2	KKI 2	PWR / 1365 / 1988	Dec. 2019
Emsland	KKE	PWR / 1290 / 1988	Dec. 2019
Neckarwestheim 2	GKN 2	PWR / 1269 / 1989	Dec. 2019

Based on the end of commercial operation mandated in the Atomic Energy Act and the provisions for performing a PSR, it is likely that only two PSA within a PSR will be performed in Germany up to 2022.

PSA within the PSR have been and are being performed according to the PSA Guideline from 2005 [BMU 05] and its corresponding technical guidance documents on PSA methods [FAK 05] and PSA data [FAK 05a] (scope cf. Section 4).

6. PSA Methodology and Data

The methods to be applied for the PSA, including methods to collect and process reliability data, are outlined in the technical document on PSA methods [FAK 05] and PSA data [FAK 05a] supporting the German PSA Guideline [BMU 05].

The modelling approach of Level 1 PSA for German NPP is a small ET / large FT linking. The PSA models by the licensees are maintained in the RiskSpectrum[®] software. 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 technical document on PSA methods [FAK 05].

The quality of PSA for German NPP strongly depends on a careful quantification of common cause failures (CCF). The degree of redundancy of the safety systems/trains in German NPP is especially high (4 x 50 % or 3 x 100 % redundancy). As a consequence, the core damage frequency is dominated by contributions from CCFs. For consistent consideration of CCF in PSA, a concept for a systematic approach to technically assess the applicability of observed common cause events for the specific component groups in the PSA has been developed applying an specific CCF model ("coupling model", based on a modified BFR model, using empirical data as far as possible. Furthermore, a comprehensive program system for the calculation of CCF probabilities based on CCF events from the operating experience has been established. Further enhancements of modelling CCFs adequately and to reduce uncertainties in the model are ongoing. Studies on inter-

component group and inter-system CCF have been started recently. International cooperation in this field and, in particular, the ICDE project of the OECD/NEA are very important to further develop CCF modelling and quantification.

Currently, other limitations with respect to PSA quality are e.g. 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. Currently, HRA quantification in German PSA is mainly done using the THERP or ASEP approach and remains within the limits of these approaches. A methodology for considering safety significant knowledge based actions in PSA has been developed. This includes an approach for identifying target actions, a cognition model, and a two-stage quantitative assessment approach. In addition, an approach for considering organizational factors in PSA has been established. As a result, it is meanwhile possible to quantify the safety significance of organizational factors and of the safety management and to integrate this in the PSA model. Practical trial applications are needed. Furthermore, activities are ongoing to implement human actions and their reliability in fire PSA by modelling via a Dynamic PSA approach (with MCDET).

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.

With regard to collecting reliability data, a methodology for transforming lognormal distributions expressing uncertainties of reliability parameters (for example failure probabilities per demand or human error probabilities) to more suitable beta distributions has been developed and realized within a user friendly tool. Another goal of the research activities was to find out, if the sub-sequent variance extension of estimated distributions of reliability parameters can be regarded as a reasonable method to cover the influence of sources of epistemic uncertainties which are not explicitly considered and evaluated in the estimation model. Advantages and restrictions of this procedure have been discussed.

Concerning passive systems, the existing methods for estimating leak and break frequencies for pressurized components have been enhanced. Activities on developing a first approach for modelling the reliability of buildings structures are ongoing.

Methods for considering internal and external hazards in Level 1 PSA have been significantly improved and extended. A lot of activities have been carried out for enhancing fire PSA methodology and extending it to low power and shutdown states. In particular, the screening process has been significantly improved and generic data from the OECD FIRE database can be applied for plant specific event trees. Additional activities are ongoing with respect to developing an approach which is no longer based on compartment specific but on component specific screening. Furthermore, a new three step methodology based on site specific SHA (seismic hazard analysis), followed by generating a plant specific seismic PSA database used within a two stage process selecting the seismic equipment list to be considered and classification for obtaining fragility curves for significant SSC (systems, structures and components) has been developed. Enhancements of the approach considering also combinations of seismic with other hazards are ongoing.

With regard to Level 2 PSA, the Guideline and its supporting technical 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.

For the linking between Level 1 and Level 2 PSA, both integrated and separate modelling approaches are permitted according to the German PSA technical document on PSA methods [FAK 05] The licensees have chosen both types of analysis. The actual focus with respect to Level 2 PSA enhancements in Germany is mainly on considering severe accidents inside spent fuel pools and fission product behaviour.

There are no specific activities ongoing in Germany on Level 3 PSA.

7. PSA Applications

In Germany there is no formalized approach to apply the results of PSA to be performed for all NPP. 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 licensee, the regulator in charge and experts from technical safety and review 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 regulatory body of the German local state Baden-Württemberg has put into place a procedure requiring the use of PSA information in a number of regulatory cases.

Design evaluation

As new-builds are legally not permitted in Germany, the use of PSA for design purposes is not foreseen. Vendors based in Germany, however, do apply PSA for design purposes according to internal rules and the respective national requirements.

8. Results and Insights from the PSAs

For all NPP in Germany, the PSA results indicate that the risk during low power and shutdown states is considerable compared to the risk during full power operational states. The overall values for CDF covering full scope Level 1 PSA for all internal events and internal as well as external hazards are typically in the order of $10^{-6}/a$. The contribution of plant internal and external hazards is also considerable (typically for all hazards adding up to values in the order of some $10^{-7}/a$ to some $10^{-6}/a$, however the contribution of postulated external hazards strongly varies site specifically. As far as Level 2 PSA have been performed (for full power states only) mainly LRF have been calculated varying typically from some $10^{-9}/a$ up to $10^{-8}/a$. However, the differences in the results depend on the scope of and the assumptions for the analyses.

As a result of PSA within the frame of PSR, plant specific modifications have been recommended and implemented or are being implemented.

PSA analyses and quantifies the plant response to initiating events conceivable at the site and plant. The German PSA Guideline with its supporting technical documents provides reference spectra (DWR, SWR) of generic initiating events to be postulated. The reference spectra have to be checked with respect to relevance and completeness including plant specific conditions. PSA is used to assess strengths and weaknesses, in particular vulnerabilities and cliff edge effects, in the design and operation and to identify potential improvements. Generally, no absolute but only relative criteria are used for comparing PSA results to those from deterministic safety analyses and engineering judgement. PSA results are also used to assess the determining factors and their significance contributing to plant vulnerabilities and to assess the balance of the plant design and operation.

9. Future Developments

The German federal regulatory body intends to issue new sub-legal safety regulations on NPP, so-called "Safety Requirements for Nuclear Power Plants" in the near future. The current draft of these Safety Requirements and its annexes [BMU 12] increases the importance of PSA analyses in the safety demonstration in regulatory processes. In particular, probabilistic risk analyses will be required in addition to deterministic safety analyses

- to review the balance of the safety design and to identify potential weaknesses,
- to assess the safety significance

- of planned changes to the plant design or its operation, if their impact is non-negligible, or
- of new insights with a non-negligible impact on the PSA results.

Any change in the plant design or operation must not result in a deterioration of the mean CDF value for all plant operational states (full power as well as low power and shutdown) including plant internal events as well as internal and external hazards.

According to the draft Safety Requirements [BMU 12], PSA models used for safety demonstrations to the regulator shall meet the requirements of the technical document on PSA methods [FAK 05] supporting the German PSA Guideline. The update of the model to significant changes of the plant as well as use of recent reliability data is requested.

Concerning research issues, the following activities haven been performed or are still on-going.

Development of PSA methods

In Germany, activities are ongoing for enhancing existing and/or developing new PSA methods with respect to reliability of software based digital I&C, consideration of knowledge based behaviour and organizational influence in PSA, initiating events and external and internal hazards (in particular seismic PSA), effects of uncertainties on PSA results aiming on excluding sources of error in PSA, CCF assessment, dynamic PSA (Level 1 and 2) with MCDET, suitability of ASTEC code for application in Level 2 PSA, consideration of severe accidents inside spent fuel pools for PSA Level 2.

PSA for internal hazards

In Germany, a lot of activities have been carried out for enhancing fire PSA methodology and extending it to low power and shutdown states [BAB 11], [ROE 10a], [ROE 10b], [ROE 11], [TUE 12]. Additional activities are ongoing with respect developing an approach no longer based on compartment specific but component specific screening. It is further intended to enhance the methods for human interactions in fire PSA. Another ongoing activity is the update and extension of the database on failure rates for active fire protection features [FOR 12] by analyzing results of periodic in-service inspections. The update will cover more than 130 plant operational years of in total seven NPP units. In addition to plant specific reliability data, an updated set of generic reliability data will be provided. This database ought to be large enough for trying to gain experience with regard to CCF of active fire protection features.

PSA for external hazards

In Germany, a new three step methodology based on site specific SHA has been developed, followed by generating a plant specific seismic PSA database used within a two stage process selecting the seismic equipment list to be considered and a classification for obtaining fragility curves for significant SSC [TUE 10], [TUE 10a]. This approach shall be further enhanced. Activities to consider the entire combinations of external with other external or internal hazards in external hazards PSA with the interdependencies of the required safety functions are ongoing.

Common cause failure modelling

In Germany, for consistent consideration of CCF in PSA, a concept for a systematic approach to technically assess the applicability of observed common cause events for the specific component groups in the PSA has been developed [STI 09]. Furthermore, a comprehensive program system for the calculation of CCF probabilities based on CCF events from the operating experience has been established [GAL 10]. Further enhancements of modelling CCF adequately and to reduce uncertainties in the model are ongoing. Studies on inter-component group and inter-system CCF have been started recently [PES 10].

Human reliability analysis

In Germany, a methodology for considering safety significant knowledge based actions in PSA has been developed to quantify the safety significance of organizational factors and of the safety management and to integrate this in the PSA model [FAS 10], [FAS 10a]. The HRA database has been extended [PRE 10]. Activities are ongoing to implement human actions and their reliability in fire PSA by modelling via a Dynamic PSA approach (using MCDET).

PSA for passive systems

In Germany, the existing methods for estimating leak and break frequencies for pressurized components have been enhanced [GRE 10], [GRE 10a]. Activities on developing a first approach for modelling the reliability of buildings structures are ongoing.

Reliability of digital systems

Activities in Germany focus on developing approaches for assessing the reliability of software based digital I&C [PIL 10]. In addition, the PSA relevance of the man-machine interface of software based I&C has been analysed and a first approach for its consideration in PSA has been developed [HAR 09], [HAR 10]. Activities for developing methods for evaluating diversity attributes of digital I&C are ongoing aiming at an approach for assessing the implementation of diversity against potential common cause failures of the hardware and software of digital instrumentation and control.

Level 2 PSA

In Germany, research activities have been carried out to improve, enhance and test the suitability of ASTEC for application in Level 2 PSA studies. These investigations including a comparison with MELCOR demonstrated successfully that the most recent version of ASTEC is relevant for performing complete severe accident analyses under PSA specific conditions both matching to the state of the art and with a reasonable calculation speed. The actual focus with respect to Level 2 PSA enhancements in Germany is mainly on considering severe accidents inside spent fuel pools and fission product behaviour and sequences covering low power and shutdown plant operational states.

Uncertainties

Intense research activities have taken place and work is continuously being carried out to improve the way that uncertainties are being addressed in PSA [KLO 10], [PES 10], [PES 10a]. In the frame of Level 1 PSA, the GRS code STREUSL is to some extent applied instead of RiskSpectrum[®], because it can account for more options to consider complete state of knowledge dependencies. SUSA is applied in the frame of Level 2 PSA, but can be also used for sensitivity analyses in both, Level 1 and Level 2 PSA. It is furthermore applied within thermal hydraulics in combination with best estimate codes.

Another more recent development in Germany is the probabilistic dynamics method MCDET. In this context, methods for performing uncertainty and sensitivity analyses in the frame of Dynamic PSA have been established allowing e.g. for a more realistic modelling of accident scenarios to be considered in PSA. In addition, a transformation of uncertainties in the reliability values given as lognormal distributions to the more suitable gamma or beta distributions has been realized. It has been also investigated if the sub-sequent variance extension of estimated distributions of reliability parameters can be regarded as a reasonable method to cover the influence of epistemic sources of uncertainties on distributions of reliability parameters, which are not explicitly evaluated in the estimation model. Hence it will be possible in future to consistently consider relevant epistemic uncertainties from different sources in PSA.

Moreover, a general approach has been provided to account for the influence of epistemic uncertainty sources which did not explicitly contribute to the estimation of a distribution. The method applies a subsequent variance extension of the estimated distribution.

Modelling of ageing in PSA

There are no specific activities in Germany on the consideration of ageing PSA. However, by using recent plant specific data in German PSA models, the detrimental effect of ageing on component reliability is at least partially captured.

Use of the PSA in risk informed applications

Within an ongoing project a first approach for a federal German guideline on integrated risk informed decision making (IRIDM) based on INSAG-25 and in line with the new German Safety Requirements (draft see [BMU 12]) is recently being developed. This guideline will provide recommendations for the harmonization of the decision making process concerning safety relevant issues for German NPP [EIN 11], [EIN 12].

10. References

[BAB 11] Babst, S., et al., Methoden zur Durchführung von Brand-PSA im Nichtleistungsbetrieb, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-A-3579, Köln, Germany, Januar 2011

- [BMU 05] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Leitfaden zur Durchführung der ‘Sicherheitsüberprüfung gemäß §19a des Atomgesetzes – [7/05, Wirtschaftsverlag NW / Verlag für neue Wissenschaft GmbH, Salzgitter ISSN 0937-4469, ISBN 3-86509-414-7, Oktober 2005

- [BMU 12] /Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU), Sicherheitsanforderungen an Kernkraftwerke, Revision E+, 11.06.2012, draft (unpublished)

[EIN 11] Einarsson S., A. Wielenberg, Risikoinformierte Entscheidungsfindung bei sicherheitstechnischen Fragestellungen in Deutschland, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, GRS-A-3624, Köln, August 2011

[EIN 12] Einarsson S., A. Wielenberg, An Integrated Risk Informed Decision Making Approach for Germany, in: Conference Proceedings of PSAM11 Conference, Helsinki, Finland, 2012 (in preparation)

- [FAK 05] Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke, Methoden zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BFS-SCHR-37/05, Salzgitter; Oktober 2005

- [FAK 05a] Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke, Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BFS-SCHR-38/05, Salzgitter; Oktober 2005

- [FAS 10] Faßmann, W., J. Hartung, W. Preischl , Probabilistische Bewertung organisatorischer Einflüsse sowie von Einflüssen des Sicherheitsmanagements auf die Zuverlässigkeit von Personalhandlungen, Technischer Fachbericht, GRS-A-3560, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

[FAS 10a] Faßmann, W., W. Preischl, Quantitative Bewertung wissensbasierter Handlungen in einer probabilistischen Sicherheitsanalyse, Technischer Fachbericht, GRS-A-3561, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

[FOR 12] Forell, B., S. Einarsson, M. Röwekamp, H.P. Berg, Updated Technical Reliability Data for Fire Protection Systems and Components at a German Nuclear Power Plant, in: Conference Proceedings of PSAM11 Conference, Helsinki, Finland, 2012

[GAL 10] Gallner, L, A. Kreuser, M. Leberecht, J.-C. Stiller, Methodenentwicklung zur konsistenten Berücksichtigung gemeinsam verursachter Ausfallereignisse (GVA) in PSA, Technischer Fachbericht, GRS-A-3552, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, August 2010

[GRE 10] Grebner, H., Wang, Y., Schimpfke, T., Sievers, J., Weiterentwicklung der strukturmechanischen Analysemethodik zur Bestimmung der Strukturzuverlässigkeit passiver Komponenten, Phase II, Abschlussbericht, GRS-A-3544, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, 2010

[GRE 10a] Grebner, H., et al., Weiterentwicklung von Methoden zur Ermittlung von Leck- und Bruchhäufigkeiten druckführender Komponenten, Technischer Fachbericht, GRS-A-3555, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, Köln, Juli 2010

[HAR 09] Hartung, J., Verbesserung der Bewertungsbasis für Aspekte des Sicherheitsmanagements und der Schnittstellen zur Sicherheitstechnik sowie für Personalhandlungen, GRS-A-3500, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Oktober 2009

[HAR 10] Hartung, J., E. Piljugin, Entwicklung eines methodischen Ansatzes zur Bewertung menschlicher Zuverlässigkeit beim Einsatz softwarebasierter Leittechnik, Technischer Fachbericht, GRS-A-3548, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Mai 2010

[KLO 10] Kloos, M., Bereitstellung einer Methodik zur Anpassung von Beta-Verteilungen an vorgegebene Lognormal-Verteilungen unter Berücksichtigung zusätzlicher Benutzervorgaben, Technischer Fachbericht, GRS-A-3518, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, März 2010

[PES 10] Peschke, J., Methodik zur Berücksichtigung epistemischer Unsicherheitsquellen bei der Schätzung von Zuverlässigkeitskenngrößen, Technischer Fachbericht, GRS-A-3540, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, April 2010

[PES 10a] Peschke, J., B. Krzykacz-Hausmann, Methodenentwicklung zur Durchführung von Unsicherheits- und Sensitivitätsanalysen im Rahmen einer probabilistischen Dynamikanalyse, Technischer Fachbericht, GRS-A-3556, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

[PIL 10] Piljugin, E., J. Herb, Entwicklung eines aktualisierten Ansatzes zur Berücksichtigung softwarebasierter Sicherheitsleittechnik in der PSA, GRS-A-3550, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, August 2010

[PRE 10] Preischl, W., Verifikation von Zuverlässigkeitsdaten für Personenhandlungen und Datenverbreiterung im Rahmen der PSA, Gesellschaft für Anlagen und Reaktorsicherheit (GRS) mbH, GRS-A-3515, Garching, Januar 2010

[ROE 10] Roewekamp, M., et al., Weiterentwicklung und Erprobung von Methoden und Werkzeugen für probabilistische Sicherheitsanalysen (Development and Test Applications of Methods and Tools for Probabilistic Safety Analyses), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, September 2011

[ROE 10a] Röwekamp, M., M. Türschmann, M. Schwarz, H.P. Berg, Database for A Comprehensive Fire PSA, Paper 0113, in: Conference Proceedings of PSAM10 Conference, Seattle, WA, USA, June 2010

[ROE 10b] Röwekamp, M., W. Werner, A. Huerta, The OECD FIRE Database and Its Applicability in: Fire PSA, Paper 0114, in: Conference Proceedings of PSAM10 Conference, Seattle, WA, USA, June 2010

[ROE 11] Röwekamp, M., M. Türschmann, H.-P. Berg, A Holistic Approach for Performing Level 1 Fire PRA, Paper 95_1, in: Proceedings of, ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Wilmington, NC, March 13-17, 2011, on CD-ROM, American Nuclear Society, LaGrange Park, IL, USA, June 2011

[STI 09] Stiller, J.-C., J. Peschke, Konsistente Berücksichtigung der Unsicherheit bezüglich der Rate von GVA-Ereignissen bei der Anwendung des Kopplungsmodells, GRS-A-3466, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, 2009

[TUE 10] Türschmann, M., et al., Verfahren zur Klassifizierung von Bauwerken, Systemen und Komponenten in Hinblick auf ihre sicherheitstechnische Bedeutung bei seismischen Einwirkungen, Technischer Fachbericht, GRS-A-3472, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln/Berlin, Juni 2010

[TUE 10a] Türschmann, M., et al., Modellierung und Quantifizierung erdbebenbedingter Ereignisabläufe., GRS-A-3549, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln/Berlin, August 2010

[TUE 12] Türschmann, M., W. Werner, M. Röwekamp, Application of OECD FIRE Data for Plant Specific Fire Event Trees, in: Conference Proceedings of PSAM11 Conference, Helsinki, Finland, 2012

Appendix B – Contact Information

Regulatory Authority / Technical Support Organisation	Direct Contact
GRS mbH 50667 Köln Germany Tel: +49 (0)221 2068 0 Fax: +49 (0)221 2068 888 Website Address: www.grs.de	Dr. Marina RÖWEKAMP GRS mbH Schwertnergasse 1 50667 Köln Germany Tel: +49 (0)221 2068 898 Fax: +49 (0)221 2068 10898 Email: marina.roewekamp@grs.de

8. HUNGARY

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and environment

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, EUR, and WENRA 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 was issued in 2008 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 involved in the Implementation Plan a model project has been launched for the time period 2010-2011, in which the HAEA NSD and the Paks NPP, as well as the NUBIKI as the technical support organisation in the area of PSA are involved. The main objectives of the model project is to support the development of tools and methods for risk informed decision making through

- application of risk monitors,

- supervision of maintenance planning,
- and risk-informed classification of SSEs.

3. Numerical Safety Goals

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/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.

4. PSA Standards and Guidance

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 and 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, e.g. IAEA procedure guides [2-3], NEA documents [4-6], NUREG reports [7-8], WENRA and EUR requirements [9-10] have been considered.]

5. Status and Scope of PSA Programs

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' of the same vintage internationally.

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 from 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 startup. Unit 2 was 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. Similarly to internal events, analysis of these internal hazards was done on a unit specific basis. Although the four units are seemingly 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. PSA for internal fires and internal flooding was first performed for full power operation on a unit specific basis, followed by an analysis of low power and shutdown states. The latter is still under development.
- 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 were taken into account by the utility. The original seismic PSA for full power operation was later extended to cover low power and shutdown states too.
- 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. Some of these measures are currently being implemented.
- 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. Initially the level 2 PSA covered 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 due to internal event, internal fires and internal flooding. Level 2 PSA seismic events at full power operation was performed as a follow-on analysis to the initial study.
- As to ongoing analyses for Paks, it should be highlighted that level 1 PSA for external events other than earthquakes has been started. So far a screening analysis has shown that mostly natural hazards should be included in the external event PSA, while man-made hazards could be screened out. As indicated above, low power and shutdown PSA for internal fires and flooding is also underway. This analysis has been completed for unit 2, while extension to the other three units is to be made in 2011.

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 to some degree, 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 and other external events:

- 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 as well as in low power and shutdown states 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 both full power operation and low power and shutdown states.
- Over and above seismic events, other external hazards are currently the subject of PSA for NPP Paks. This analysis is ongoing. Up to now hazard assessment has been made for the various external events that resulted in (1) a list of events that should be covered by PSA modelling and (2) the associated event frequencies.

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 an 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 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 NUBIKI. 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 2010 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. The latest update of the component reliability data base included in the plant PSA was made in 2008. This update focused on the operating experience accumulated at the Paks NPP.

There is no living PSA programme in place for the level 2 PSA of NPP Paks. However, a complete revision and update of the analysis has been started to include the effect of measures for severe

accident management and, also, to reflect the influences of changes made to the level 1 PSA in the living PSA programme. This work is in its initial phase and it has covered the review of plant damage state analysis (interface between level 1 and level 2 PSA) so far.

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

6. PSA Methodology and Data

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 POSS 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 POSS 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.

Event sequence analysis: 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.

System analysis: 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.

Analysis of dependent failures: 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 $\hat{\alpha}$ 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 m² or higher
4. Early Containment Enhanced Leakage (ECL) – Leak size of 0.05 m²
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 vario 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.

Use of results to support severe accident management: 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.

7. PSA Applications

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 has undergone a continuous upgrade process. This is why the systematic PSA based analysis of plant modifications that supports this upgrade process has become 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 more than one order of magnitude since the first PSA study. 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. Currently the annual PSA updates demonstrate a rather homogeneous risk profile and minor year-by-year changes in the risk (CDF) level.

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.

Currently the PSA methods and tools are more and more used for risk-informed decision making both by the regulatory body, and by the utility. For this purpose the application of a risk monitor at Paks NPP has been prepared.

8. Results and Insights

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. Examples of the latest analysis results (2010) for selected units are as follows:

Power operation (unit 3)

CDF for internal initiators: $5.2 \cdot 10^{-6}$ 1/year
 CDF for fires: $2.6 \cdot 10^{-6}$ 1/year
 CDF for internal flooding: $5.3 \cdot 10^{-6}$ 1/year
 CDF for seismic events: $4.3 \cdot 10^{-5}$ 1/year

Shut down mode

CDP for internal events: $5.4 \cdot 10^{-6}$ 1/outage (unit 2)
 CDP for fires: $8.1 \cdot 10^{-7}$ 1/outage (unit 2)
 CDP for internal flooding: $1.6 \cdot 10^{-7}$ 1/outage (unit 2)
 CDP for seismic events: $3.6 \cdot 10^{-6}$ 1/outage (unit 3)

Some of the improvements that were either initiated by the PSA results or were found effective in risk reduction are listed here:

- Relocation of emergency feed water system, to ensure its protection against high-energy line breaks and, fires and flooding 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 to ensure the use of normal power supply to safety systems if there is no need to use emergency power supply from the diesel generators;

- Modification of the primary pressure relief system, introduction of "bleed and feed" possibility, realisation of a protection against cold overpressurisation of the reactor vessel;
- 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 the likelihood of heavy load drops 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 of 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: to provide a basis (1) for the development of plant specific accident management strategies, (2) for the plant specific backfit analysis and evaluation of risk reduction options, and (3) 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 not negligible either.

The risk reduction capability of different accident management possibilities has been assessed. The accident management programme has been reviewed by the regulatory body. 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 reactor shaft door damage as mitigative measures. A number of other improvements, mostly preventive measures have been 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.

Implementation of severe accident measures is currently ongoing. Its main elements include: severe accident hydrogen recombiners, in-vessel melt retention by flooding of reactor cavity and external cooling of the reactor vessel, installation of severe accident measurements and instrumentation as well as introduction of guidelines for severe accident management. These measures are being implemented for all of the four units at Paks.

9. Future Developments and Research

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 develop 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, NUBIKI 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. Currently considerable effort is devoted to the integration of 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 included 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. The statistical information of the electric and C/I component failures has been evaluated, as well as the Bayesian updating of all component data has been performed.

The project has also aimed at the definition of further requirements on failure data collection to be performed through the Integrated Technical Data System (IMR) implemented at the Paks NPP.

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 had to be modified. This modification covered the revision of all event sequences where operator interactions are involved. As a result both the logic structure of the failure event model and the human error probabilities have been modified.

The modelling of the new symptom-based EOPs within the different PSAs has been completed.

Extension of the Scope of the Current PSAs

The main efforts to extend the scope of PSAs are devoted to make the analysis of internal as well as external hazards more complete.

In shutdown modes the level 1 PSA for internal fires and internal flooding is available for unit 2 at present. Similar PSA for the other three units of the Paks plant is near completion. This work will enable the use of unit specific risk models for internal events and internal hazards covering full power operation and shutdown states too.

Level 1 PSA for external hazards other than earthquakes has been started for the Paks plant. An initial screening analysis has shown that mostly natural hazards (e.g. extreme weather conditions, lightning , etc.) should be the subject of plant response analysis as the next step of the external event PSA.

As to the existing seismic PSA, it is planned to extend the scope of the current analysis (that is available for unit 3 as a references unit) to the other three units too.

Updating of the level 2 PSA for Paks has been started to reflect the effect of severe accident management measures and the changes in the level 1 PSA. When completed, it will have to cover the same scope as the level 1 PSA in terms of both plant operational states and initiating events.

Risk-Informed Monitoring of Maintenance Effectiveness

Recently studies have been performed in support of introducing a systematic approach to monitor the effectiveness of maintenance at Paks NPP, as well as to investigate the potential applicability of risk-informed inspections.

The monitoring of maintenance effectiveness comprises both deterministic and probabilistic approaches. The latter one is 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.

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
- [9] EUR – European Utility Requirements for LWR Nuclear Power Plants, Revision C, April 2001
- [10] WENRA Reactor Safety Reference Levels, January 2008

9. INDIA

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

Use of PSA in NPP regulation - Historical Perspective

Atomic Energy Regulatory Board (AERB) is the competent authority for the regulation of nuclear plants, radiation facilities and fuel cycle facilities in India. As a part of regulatory activities, AERB reviews/enforces standards and authorize, from the safety angle, siting, design, construction, commissioning, operation and decommissioning of above-mentioned facilities. The R&D organizations, Bhabha Atomic Research Centre (BARC) and Indira Gandhi Centre for Atomic Research (IGCAR) are technical support organizations to AERB. The Nuclear Power Corporation of India Limited (NPCIL) is responsible organization for design, construction, commissioning, operation and decommissioning of Nuclear Power Plants.

In the early days, the nuclear plants / facilities were licensed by AERB with traditional deterministic methods by applying high-level criteria such as defence-in-depth, adequate safety margin, single failure criteria etc. However, the system reliability analyses were carried out as a part of safety reports. Since late 90s, PSA studies have been developed by research organizations (BARC, IGCAR) and utilities (NPCIL). AERB started using the information provided by these studies as a complementary tool to traditional deterministic methods into regulatory decision-making. The current approach is to integrate the PSA results into regulatory decision-making in a progressive manner. AERB encourages utilities to supplement all license applications with Level 1 PSA studies as a desirable practice.

Regulatory Requirements for PSA

The assessment of system reliabilities was one of the regulatory requirements for the application for renewal of authorization (AERB/SG/O-12, 2000). In 2008, AERB made it mandatory for utilities to submit Level-1 PSA (internal events, full power) for all new NPPs before the first criticality (AERB/SC/O, 2008). For NPPs in operations, the stipulation is that the PSA studies shall be updated and presented as a part of periodic safety review. The PSA shall be kept up-to-date during the plant lifetime taking into account design modifications, changes in operational practices and updated statistical data on initiating event frequencies and component reliability data.

Development of PSAs

The Level 1 PSA activities in India started in early eighties at BARC. The first Level 1 PSA study was completed for Narora Atomic Power Station in 1988. Subsequently Level 1 PSA was also completed for Kaiga Nuclear Power Station in 1996. These studies remained part of R&D activities at BARC. As part of this programme Level 1+ PSA for research reactors at BARC were also performed. These studies provided necessary academic background for PSA activities in India. Later AERB stipulations, time to time, required that Level 1 PSA is desirable. Here, the NPCIL took the responsibility of submitting PSA studies for all the nuclear power plants in India. This included revisiting the available Level 1 PSAs to comprehensive Level 1 PSAs.

As shown in Table 1, from 2000 to 2002, NPCIL submitted level-1 PSA for internal events at full power for TAPS-1&2 (BWR) and KAPS-1&2 (PHWR). Since then, the level-1 PSA for internal events at full

power has been carried out by NPCIL for all NPPs. AERB set up a 'Committee on PSA for Nuclear Facilities' for regulatory review of PSA studies. The AERB committee on PSA consists of experts within AERB, BARC IGCAR and NPCIL.

3. Numerical Safety Criteria

As a part of safety demonstration, it is desirable that safety case should meet numerical guidelines (i.e. system reliability targets, core damage frequency, large early release frequency etc.) as a good practice. However, it is not a mandatory requirements. AERB's current view on the numerical safety criteria is that the benefit of PSA comes from getting an understanding of safety status in terms of relative importance of contributors to risk metrics. In addition, it helps in making comparative assessment, rather than in deriving bottom-line absolute numbers for core damage frequency (CDF) or large early release frequency (LERF), to be checked against formal numerical goals. In view of this, for CDF and LERF, the INSAG-12 recommendations are used as reference values.

4. PSA standards and Guidance

One of the mandates of the AERB is to develop safety documents that lay down requirements for meeting safety criteria for activities related to nuclear energy and provide guidance on methods for fulfilling the requirements. In the process of adopting 'risk-informed' approach, the need is felt to revise the existing AERB safety codes to include the requirements of PSA in the safety analysis reports and other safety related submittals. Safety codes establish the objectives and set minimum requirements that shall be fulfilled to provide adequate assurance of safety.

AERB has prepared a manual on PSA (AERB/NPP&RR/SM/O-1, 2008) which provides support information and broad procedures for carrying out PSA studies. The approaches and methods suggested are based on relevant international/national documents. These procedures are primarily meant for NPPs and research reactors, however, the same could be useful for performing PSA in non-reactor nuclear facilities. This document gives comprehensive coverage on various elements of PSA, guidance on regulatory review and quality assurance in PSA.

Few studies performed till 2002 used data from generic sources. Among these databases, IAEA-TECDOC-478 was one of the major sources of data. Based on the insights gained from the regulatory review of PSA studies, AERB prepared a compendium on generic component reliability database (AERB/NPP/TD/O-1). The document covers the database format, definition of component boundary, various component groups, different failure modes and operating environment.

Based on the insights gained from the regulatory review of PSA studies, a need was felt to prepare a technical document on HRA methods. AERB prepared a compendium on HRA for PSA of NPPs (AERB/NPP/TD/O-2). The document covers basic concepts of human reliability and human errors, steps involved in HRA process and integration of HRA into PSA. The document also describes various HRA methods, discusses data collection schemes and data formats for collection of HRA data from NPP operating experiences. Few case studies are also presented as illustrative purpose by applying different HRA methods.

PSA expert Committee of AERB consisting of experts from BARC, NPCIL, India has carried out a comparison of ASME standard on PSA and IAEA safety series 50-P4 to ensure the 'technical adequacy' of existing PSA models for Risk Informed Decision-making (RIDM) approach. Based on the insights outcome of this effort, AERB is currently developing a regulatory guide for the review of full scope level-1 PSA for nuclear power plants.

5. Status and Scope of PSA Programs

The Level-1 PSAs considering the internal events at full power stage are performed for all Indian NPPs. These PSAs are reviewed by the AERB's 'Committee on PSA for Nuclear Facilities'. PSA methods and models got improved progressively since the first report on TAPS PSA (December 2002) till the last report on MAPS-1&2 PSA (January 2010). The status of the PSA studies is given as below:

Table 1: Level 1 PSA Performed by NPCIL Since 2000

Sr. No	NPP	Scope of PSA (Internal events)	Submission Date
1	TAPS#1&2	Level-1	Part-I: Nov. 2000 Part-II: April 2002
		Revised Report	June 2009
2	KAPS#1&2	Level-1	April 2002
		Level-2	March 2006
3	NAPS#1&2	Level-1	June 2006
4	MAPS#1&2	Level-1	January 2010
5	KGS#1&2	Level-1	Jan. 2007
6	RAPS#3&4	Level-1	May 2007
7	KGS#3&4 Project	Level-1	March 2007
8	RAPS#5&6 Project	Level-1	Oct. 2007
9	TAPS#3&4 Project	Level-1	March 2005
10	KK-Project	Level-1	Dec. 2005
11	RAPS#2	Level-1	March 2009

Development of external event PSA (i.e. flood, seismic), internal hazards (i.e. fire, flood) are in progress for a representative NPP (KAPS-1&2). Shutdown PSA has been completed for a representative NPP (KAPS-1&2). A level-2 PSA study for a representative NPP (KAPS-1&2) also has been completed. The objective of this study was to familiarize with the methodology and identification of severe accident scenarios where further analysis is required.

6. PSA Methodology and Data

The Level-1 PSAs considering the internal events at full power stage for Indian NPPs are performed as per the procedure given in IAEA-SS-50-P4. The IAEA procedure guide is intended to provide guidance on conducting a level 1 PSA for internal events in NPPs. The main emphasis is on procedural steps of the PSA rather than the details of the corresponding methods. A particular aim is to promote a standardized framework, terminology and form of documentation for PSAs so as to facilitate external review of the results of such studies. The document not only describes methods, but also considers advantages and limitations of alternative approaches and indicates those most widely used to date.

AERB has prepared a PSA manual, which provides the PSA methodology and other document on component failure database provides the generic data for use in PSAs. Different approaches are used for various PSA elements such as initiating event analysis, accident sequence analysis, data analysis, common cause failure analysis, Human reliability analysis. The salient features of the PSA methodology followed, in general, is given below:

Initiating event analysis:

The initiating events are selected based on engineering evaluation, reference to previous PSAs, using fault tree analysis and some times using the operational feedback. They are grouped in such a way that all events in the same group impose essentially the same success criteria on the front line systems as well as the special conditions (challenges to the operator, to automatic plant response etc). The initiating event frequencies are estimated based on the plant-specific data. Where data are not 'adequate', Bayesian approach is followed in which the generic prior is updated using the limited plant-specific evidence.

Accident sequence analysis:

Fault tree/Even tree approach is followed for accident sequence analysis.

For each initiating event, the safety functions that need to be performed in order to prevent core damage should be identified. For each safety function, all the frontline systems and associated support systems are then identified. Once accident initiating events have been identified and grouped, the plant response including operator actions to each group of initiating events are identified. To gain an early understanding of the relationship between frontline and support systems, a dependence table of front line/support systems can be prepared. The dependence table is updated to include the additionally identified support systems and the corresponding dependences. The end state is assigned to different accident sequences derived based on the thermal-hydraulic safety analysis.

Success criteria and mission times:

The core damage is defined based on the IAEA-SS-50-P4 guidelines. The condition for the core damage is translated into system failure states to allow the PSA to proceed and where possible these should be based on realistic analyses. In absence of such analyses 'core damage' may be conservatively assumed to occur if the design basis of the plant is exceeded. The relevant information for the assessment of front line system success criteria are derived from final safety analysis report. These success criteria are derived from the conservative deterministic calculations. Appropriate mission times are also derived from the accident analysis for different accident sequences.

Data Analysis:

Wherever, adequate plant-specific data are available, the same has been used in the PSA studies. For all other cases, Bayesian update was done (using available plant-specific data and the generic component failure data). For common cause failure (CCF) analysis, α -factor model has used with generic α -factor values given in NUREG/CR-5801.

7. *PSA Applications*

Application of PSA has so far been mainly in the areas of configuration management, design modifications, changes in allowed outage time and surveillance test intervals in Technical Specifications for Operations.

8. *Results and Insights from the PSAs*

- Confirmation of well balanced designed and the contribution from individual PIEs to the CDF is the range of 10% to 20%.
- Results of PSA also indicate that a fairly high level of redundancies exists at the safety function level.
- Staggered testing was suggested to reduce the probability of common cause failures.
- Physical inspection of all manual valves is revealed to be an important step during reactor startup to insure their desired position after maintenance.
- Flow blockage through the passive components is making a significant contribution.

9. *Future Development and Research*

The insights gained on the development and application of PSA to address various issues has brought in focus future R&D requirements. The major areas where the research work being performed in India can broadly be classified as follows:

- a) Development and Application of improved Methods for Reliability Modeling
- b) Digital System Reliability Assessment
- c) Development of tools and methods to consolidate the component reliability database.
- d) Human Factor development and Human Reliability prediction
- e) Structural System Reliability modeling
- f) Uncertainty Characterization
- g) Passive System Reliability modeling
- h) Development of PSA based Applications, like Risk-based ISI, Risk-based Configuration Management Systems, Risk-based Maintenance Management, Accident Sequence Precursor Analysis, etc.

The experience on electronic system reliability modeling in general and digital system in particular indicates clearly that improved method of reliability prediction employing Physics-of-failure (PoF) approach need to be developed. It is well accepted fact that even though PoF approach though provides a superior method of reliability modeling it also requires considerable R&D, involving material characterization, accelerated testing, understanding effect of operational and environmental stresses. Further advances in digital system like deployment of FPGAs / CPLDs and new design of existing components require in-depth understanding of failure mechanisms as part of reliability characterization of these components. Even though there is no general consensus on any one approach for reliability modeling of software systems and V&V approach forms the major framework for software reliability, work is in progress to develop models and methods for software reliability characterization.

Most part of PSA studies are based on the human error data and models available from generic sources (referred as first and second generation methods). However, the generation of human factor / PSFs and Human Reliability data using simulator experiments will surely reduce uncertainty in the estimates. Similarly, keeping in view the future modeling requirements for advanced nuclear power plants in India, procedures and methods are being developed for passive system reliability modeling. Extensive thermal hydraulic experiments form part of data generation for reducing uncertainty in the estimates.

PSA based applications requires that the data and models should be adequate to address the requirements of a given real-time scenario. This requires adoption of the existing model and interpretation of data and requirements. The issues involved are : a) development and application of modifying factors, b) bench marking of software, c) adequacy of models and data for CCFs, d) uncertainty characterization in the data and models, e) presentation and interpretation of results, and use and interpretation of available guidelines and criteria for operational and regulatory review, etc.

10. References

- 9.1 ATOMIC ENERGY REGULATORY BOARD, AERB Safety Code on Nuclear power Plant Operation, AERB/NPP/SC/O (Rev. 1), 2008.
- 9.2 ATOMIC ENERGY REGULATORY BOARD, Renewal of Authorization for Operation of Nuclear Power Plants, AERB/NPP/SG/O-12, August 2000.
- 9.3 ATOMIC ENERGY REGULATORY BOARD, Probabilistic safety assessment for nuclear power plants and research reactors, AERB/NPP&RR/SM/O-1, March 2008.
- 9.4 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for conducting Probabilistic safety assessments of nuclear power plants (level 1), IAEA-SS-50-P-4, Vienna, 1995.
- 9.5 INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety series No. 50-P-8, IAEA, Vienna, 1995.
- 9.6 INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Series No. 50-P-12, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA, Vienna, 1996.
- 9.7 INTERNATIONAL ATOMIC ENERGY AGENCY, Review of PSAs by regulatory bodies, IAEA-SS-25, Vienna, 2002.
- 9.8 INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, TECDOC-1200, February 2001.
- 9.9 Generic CANDU Probabilistic Safety Assessment – Methodology, 91-03660-AR-001, Rev.-1, July 2002.
- 9.10 AMERICAN SOCIETY FOR MECHANICAL ENGINEERS, Standard for PRA for NPP applications, ASME RA-Sb-2005.
- 9.11 INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the quality of PSA for applications in NPPs, IAEA-TECDOC-1511, Vienna, 2006.
- 9.12 US NUCEAR REGULATORY COMMISSION, An approach for determining the technical adequacy of PRA results for risk informed activities, RG-1.200, February 2004.
- 9.13 US NUCEAR REGULATORY COMMISSION, NUREG/CR-4780, Procedures for treating Common Cause failures in Safety and Reliability Studies, USNRC, 1988.

- 9.14 US NUCEAR REGULATORY COMMISSION, NUREG/CR-5801, Procedure for Analysis of Common Cause Failures in PSA, USNRC, 1993.
- 9.15 US NUCEAR REGULATORY COMMISSION, NUREG/CR-5485, Guidelines on Modeling Common Cause Failures in PRA, USNRC, 1998.
- 9.16 US NUCEAR REGULATORY COMMISSION, NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications; A. D. Swain and H. E. Guttman; August 1983 (THERP).
- 9.17 US NUCEAR REGULATORY COMMISSION, NUREG/CR-4772, Accident Sequence Evaluation Program Human Reliability Analysis Procedure; A. D. Swain; February 1987 (ASEP).
- 9.18 US NUCEAR REGULATORY COMMISSION, An approach for using probabilistic risk assessment In risk-informed decisions on plant-specific changes To the licensing basis, RG-1.174.
- 9.19 US NUCEAR REGULATORY COMMISSION, An approach for plant-specific, risk-informed decision making: Technical specifications, RG-1.177.
- 9.20 US NUCEAR REGULATORY COMMISSION, Issues and recommendations for advancement of PRA technology in risk-informed decision-making, NUREG/CR-6813, 2003.
- 9.21 INTERNATIONAL ATOMIC ENERGY AGENCY, A framework for a quality assurance programme for PSA, IAEA-TECDOC-1101, Vienna, 1999.
- 9.22 INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Component Reliability Data for Research Reactor PSA, IAEA-TECDOC-930, Vienna.
- 9.23 US NUCEAR REGULATORY COMMISSION, NUREG 1150 (Vols1-2), U.S Nuclear Regulatory Commission, Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plant, December 1990.
- 9.24 INTERNATIONAL ATOMIC ENERGY AGENCY, PSA for Shutdown Mode for Nuclear Power Plants, TECDOC-751, IAEA, Vienna, 1994.
- 9.25 INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), TECDOC-1106, August 1999.
- 9.26 MIL-HDBK-217F, Military Handbook: Reliability Prediction of Electronic Equipment, DOD, Washington D.C. (1992).
- 9.27 INTERNATIONAL ATOMIC ENERGY AGENCY, Component Reliability Data for Use. In Probabilistic Safety Assessment, IAEA-TECDOC-478, Vienna, 1988.

Appendix-B**Contact Information: NEA-WGRISK Members**

Regulatory Authority/Technical Support Organization/Utility	Direct Contact
<p>CHANDE, Shridhar K. Vice-Chairman, Atomic Energy Regulatory Board Niyamak Bhavan Anushakti Nagar, Mumbai – 4000 094 INDIA</p> <p>VARDE, P. V. Professor, Homi Bhabha National Inst. Head, Safety Evaluation & MTD Sec RN 104, Dhruva Complex Bhabha Atomic Research Centre, Mumbai 400 085 INDIA</p> <p>BHARDWAJ, S.A. Director (Technical) Nuclear Power Corporation of India Limited Nabhikiya Urja Bhavan Anushaktinagar, Mumbai – 4000 094 INDIA</p>	<p>Tel : +91 22 2557 4024 Fax: +91 22 2556 5717 Email: vc@aerb.gov.in</p> <p>Tel : +91-22-2559 4689 Fax : +91-22-2550 5311 Email : varde@barc.gov.in</p> <p>Tel: +91-22-2558 4689 Fax: +91-22-2599 3308 Email: sabhardwaj@npcil.co.in</p>
<p>Regulatory Authority website: www.aerb.gov.in BARC web-site: www.barc.ernet.in Utility web-site Website: www.npcil.co.in</p>	

10. ITALY

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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.

Despite the renewed interest of Italy in nuclear energy in last years (starting from 2008), substantiated by the newly created agency for nuclear safety (ASN, Agency for Nuclear Safety) in 2010, the framework for PSA hasn't yet been established. Therefore the PSA activities have been still devoted to research in nuclear safety, addressing specific aspects, such as reliability of passive systems and advanced reactors PSA, including Level2 PSA aspects. These activities have been conducted mostly by research organizations (as ENEA, newly denominated Italian National Agency for New Technologies, Energy and Sustainable Economic Development) and technical universities.

3. Numerical safety criteria

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 $10^{-5} - 10^{-6}$

4. PSA standards and guidance

There are no national standards or guidelines on PSA: the concerned studies are based mostly on IAEA guidelines.

5. Status and scope of PSA programs

No information is provided.

6. PSA methodology and data

No information provided.

7. PSA applications

No information provided.

8. Results and insights from the psas

No information is provided.

9. Future developments and research

R&D activities in nuclear safety research with respect to PSA aspects have concerned mainly the following subjects.

- Human reliability analysis [1]
- Development of new methods for digital Instrumentation & Control (I&C) system reliability analysis [2]
- Development of improved and new methods and models for passive system reliability [3,4, 5,6,7,8,9,10,11,12,13,14];
- Modelling of ageing, in reliability and probabilistic safety assessment studies, APSA (ageing PSA) [15]
- Development of computational methods for failure diagnostics and prognostics of NPPs sensors and components [16,17]
- Development of methods for uncertainty analysis and probabilistic safety margins evaluation [18, 19]
- Development of methods for the optimization of the inspection intervals of the components of a nuclear systems [20,21]
- PSA studies concerned with advanced reactors development, such as GenIV reactors as regards aspects like initiating event identification and suitability of Level2 PSA procedures
- Application of PSA approach to Non Reactor Nuclear Facilities, with reference to, e.g., fusion plants and accelerator driven systems for waste transmutation purpose.

10. References

- [1] Zio, E., Baraldi, P., Librizzi, M., Evaluation of crew performance in simulated nuclear emergency procedures by fuzzy expert system, International Journal of Nuclear Knowledge Management, vol. 4, N1, pp 42-58, 2010.
- [2] Di Maio, F., Secchi, P., Vantini, S., Zio, E., Fuzzy C-Means Clustering of Signal Functional Principal Components for Post-Processing Dynamic Scenarios of a Nuclear Power Plant Digital Instrumentation and Control System, IEEE – Transactions on Reliability, Special Issue on Computational Intelligence in Reliability and Risk Management, June 2011.
- [3] Burgazzi, L., State of the Art in the Reliability of Thermal-Hydraulic Passive Systems. Reliability Engineering and System Safety 92, 671-675, 2007.
- [4] Burgazzi, L., Addressing the Uncertainties related to Passive System Reliability.

- Progress in Nuclear Energy 49, 93-102, 2007.
- [5] Burgazzi, L., Thermal-hydraulic Passive System reliability-based design approach, Reliability Engineering and System Safety 92 (9), 1250-1257, 2007.
- [6] Burgazzi, L., Reliability Prediction of Passive Systems based on Bivariate Probability Distributions, Nuclear Technology 161, 1-7, 2008.
- [7] Burgazzi, L., About Time-variant Reliability Analysis with Reference to Passive Systems Assessment. Reliability Engineering and System Safety 93, 1682-1688, 2008.
- [8] Burgazzi, L., Evaluation of the Dependencies related to Passive System Failure. Nuclear Engineering and Design 239, 3048-3053, 2009
- [9] Burgazzi, L., Reliability Prediction of Passive Systems with Multiple Degradation Measures, Nuclear Technology 173, 153-161, 2011
- [10] Zio, E., Pedroni, N., How to effectively compute the reliability of a thermal-hydraulic nuclear passive system, Nuclear Engineering and Design, 241, 310-327, 2011.
- [11] Pedroni, N., Zio, E., Apostolakis, G.E., Comparison of bootstrapped Artificial Neural Networks and quadratic Response Surfaces for the estimation of the functional failure probability of a thermal-hydraulic passive system, Reliability Engineering and System Safety, 95(4), pp. 386-395, 2010.
- [12] Zio, E., Apostolakis, G.E., Pedroni, N., Quantitative functional failure analysis of a thermal-hydraulic passive system by means of bootstrapped Artificial Neural Networks, Annals of Nuclear Energy, 37(5), pp. 639-649, 2010.
- [13] Zio, E., Pedroni, N., An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems, Reliability Engineering and System Safety, doi: 10.1016/j.ress.2010.06.007
- [14] Zio, E., Di Maio, F., Tong, J., Safety Margins Confidence Estimation for a Passive Residual Heat Removal System, Reliability Engineering and System Safety, RESS, Vol. 95, pp. 828-836, doi:10.1016/j.ress.2010.03.006, 2010.
- [15] 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
- [16] Zio, E., Di Maio, F., A Data-Driven Fuzzy Approach for Predicting the Remaining Useful Life in Dynamic Failure Scenarios of a Nuclear System, Reliability Engineering and System Safety, RESS, Volume 95(1), Pages 49-57, 10.1016/j.ress.2009.08.001, 2010
- [17] Zio, E., Di Maio, F., Stasi, M., A data-driven approach for predicting failure scenarios in nuclear systems, Annals of Nuclear Energy, 37, 482-491, 2010
- [18] Zio, E., Di Maio, F., Bootstrap and Order Statistics for Quantifying Thermal-Hydraulic Code Uncertainties in the Estimation of Safety Margins, Science and Technology of Nuclear Installations, Volume 2008 (2008), Article ID 340164, 9 pages, doi:10.1155/2008/340164.
- [19] Secchi, P., Zio, E., Di Maio, F., Quantifying Uncertainties in the Estimation of Safety Parameters by Using Bootstrapped Artificial Neural Networks, Annals of Nuclear Energy, Volume 35(12), Pages 2338-2350, doi: 10.1016/j.anucene.2008.07.010, 2008

- [20] Zio, E., Bazzo, R., Optimization of the Test Intervals of a Nuclear Safety System by Genetic Algorithms, Solution Clustering and Fuzzy Preference Assignment, Nuclear Engineering and Technology, Vol. 42, N. 4, Aug. 2010.
- [21] Zio, E., Bazzo, R., Multiobjective optimization of the inspection intervals of a nuclear safety system: A clustering-based framework for reducing the Pareto Front, Annals of Nuclear Energy, Vol. 37, Issue 6, pag. 798-812.

Contact

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

11. JAPAN

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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

Accident Management (AM)

Through in-depth researches and discussions regarding severe accidents and accident management (AM), the Nuclear Safety Commission (NSC) of Japan issued a decision entitled "Accident Management as a Measure against Severe Accidents at Power Generating Light Water Reactors" in May 1992. In this decision, NSC strongly recommended the regulatory body and utilities to introduce AM measures to nuclear power plants (NPPs), although sufficient safety level has been maintained by current safety systems at operating NPPs. Responding to the decision issued by NSC, the Ministry of International Trade and Industry (MITI), which was the regulatory body of NPPs at that time, encouraged utilities to establish AM implementation plans using benefit of insights obtained from PSA in July 1992. With an investigation period of one year, the utilities submitted their plans of AM implementation to MITI in March 1994. The utilities completed implementation of AM to their NPPs by February 2002 and reported to the Nuclear and Industrial Safety Agency (NISA), which is the new regulatory body of NPPs founded in January 2001. In addition, the utilities submitted evaluation of effectiveness of AM measures for their plants. Besides fifty-two operating NPPs, AM have been studied and implemented to newly constructed NPPs.

Periodic Safety Review (PSR) Since 1992, PSAs during both power operation and shutdown operation have been made to assess the current safety level of NPPs every ten years in PSR based on the recommendation made by NISA.

Safety Goals

In December 2003, NSC proposed safety goals. The objective of the safety goals is to reasonably limit the public risk posed by nuclear accidents. In addition, NSC proposed performance goals for light water reactor (LWR) which correspond to the safety goals in March 2006.

Risk-Informed Regulation (RIR)

In November 2003, NSC published basic policy statement to introduce RIR concept in the nuclear regulation in Japan, aiming at enhancement of rationality, consistency and transparency of the safety regulation and proper allocation of resources for activities of the safety regulation and improvement of regulation, which is currently based on the conventional engineering judgment and deterministic safety assessment, by utilizing PSA results, while maintaining the deterministic concept, such as defense-in-depth. NSC set up a 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 an interim report on the review results and discussions in December 2005.

In response to the NSC basic policy, NISA, in collaboration with JNES, established Basic Concepts for RIR after receiving the public comments in May 2005. NISA and JNES also issued a Near Term Implementation Plan in May 2005 to embody RIR. NISA established High-Level Guidelines and PSA Quality Guidelines for RIR in collaboration with JNES in April 2006. The Implementation Plan established was revised in January, 2007 mainly because the new inspection system of NPPs adopts risk information in safety preservation activities, safety significance determination and so on.

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

NSC issued a revision of the examination guide for seismic design of nuclear power reactor facilities in September 2006 reflecting significant technical advancements such as advancement of technologies for geological investigation of active faults. The new guidelines are applied to the regulation for the reactors which will be constructed in future, but NISA recommended utilities to make a review on the seismic safety of the existing nuclear facilities based on the new guidelines and to report NISA the results of their reviews, including evaluation of the residual risk of the facilities using seismic PSA.

Maintenance Program

A new inspection system started in April 2008 based on the preservation programs, placing emphasis on inspection of important systems and components from the viewpoint of safety. The risk information is used to determine the importance of systems and components for maintenance and safety significance of findings during inspections.

Revision of Regulatory Guide for Reviewing Classification of Importance of Safety Function for Light Water Nuclear Power Reactor Facilities

Regulatory guide for reviewing classification of importance of safety function of LWRs was partly revised in March 2009. This guide was originally prepared in 1990 to define the importance classification of safety functions for use in the design phase but it had also been referred to in the construction and operation phases because the reliability of safety function should be maintained at all phases according to their importance. The revision clarified that the guide does not prescribe the classification of SSCs but that of safety function and, therefore, the level of maintenance of each SSCs may be determined using available technology and information including risk and operating experiences. Utilization of risk information in the determination of the importance of maintenance activities would enable further effective and individually-targeted maintenance and inspection for SSCs.

3. Numerical safety criteria

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 goals 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, CFF gives more conservative assessment when the same value is taken for CFF as 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.

4. PSA standards and guidance

Guidelines for the risk-informed regulation in Japan

According to the Near-Term Implementation Plan made in May 2005 (See 7.2.12), 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: 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 Risk Technical Committee (RKTC) is one of four technical committees set up in the Standard Committee of AESJ, reorganized in June 2010 in order to issue the standards for nuclear technology from the viewpoint of use of risk information 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 Power Reactor Technical Committee (PRTC), former of RKTC, 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. The revision of this standard has been discussed and is preparing to publish.

Standard for Level 1 PSA for Internal Events during Power Operation: The work on the level 1 PSA standard for internal events during 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 PSA standard including those of the ASME and NSRA with consideration of current practices in Japan.

There are some important differences from the ASME PRA Standard. For example, in the ASME PRA standard, three capability 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. This standard was published in March 2009.

As the PSA Quality Guidelines, issued by NISA and JNES 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 as well as quality assurance procedures, use of expert judgments and 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 Power Operation: The work on level 2 PSA for internal events during power operation was started in April 2004. This standard describes requirements and methodologies to satisfy the requirements for conducting level 2 PSA to obtain the scenarios, frequencies of containment failure and source terms. In its appendices, this standard includes guidance information and examples of the state-of-the-art methodologies of level 2 PSA. This standard was published in March 2009.

PSA Standard of PSA for Seismic Events during 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 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 provide detailed guidance and examples of state-of-the-art methodologies for conducting seismic hazard analyses, fragility analyses and accident sequence analyses. This standard was published in September 2007.

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 was started in November 2004. This standard includes requirements and methodologies to satisfy the requirements to perform level 3 PSA for NPPs. The standard was published in March 2009.

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 parameters (e.g. initiating events frequencies, component failure rates and parameters of common cause failure) and their uncertainties by technique of both Bayes estimate and frequentist estimate. This standard is made as expansion of the level 1 PSA standard, but human reliability is excluded. This standard was published in June 2010.

Risk-Informed Application Guidelines: The work on the risk-informed application guidelines was started in October 2006. These application guidelines describe basic processes, which include allowable risk criteria, for utilities to apply risk information to safety management and ensuring safety in nuclear power plant. These guidelines keep in mind the basic principle of “*High-Level Guidelines for Utilization of ‘Risk Information’ in Safety Regulations for NPPs - Trial Use -*” issued by NISA. This standard was published in October 2010.

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 draft standard was issued in December 2006.

5. Status and scope of PSA programs

Japan Nuclear Energy Safety Organization (JNES), Japan Atomic Energy Agency (JAEA) and utilities have performed PSAs. Objectives, level of PSAs, initiating events included, operational mode studied of each PSA are described below.

PSAs developed by JNES

JNES, as technical support organization, has developed PSA since 1980s’. The purposes of PSA are to develop PSA methodology and data, to make feasibility studies of applications to regulatory framework, to review of AM strategies developed by utilities and to establish basic information for risk-informed regulation. JNES has applied PSA to various areas shown in the section 7 of this report.

As the light water reactors operating in Japan are categorized into following eight types;

- 500 MW class BWR (BWR3)
- 800 MW class BWR (BWR4)
- 1100 MW class BWR (BWR5)
- 1300 MW class BWR (ABWR)
- 500 MW class PWR (2 loop PWR)
- 800 MW class PWR (3 loop PWR)
- 1100 MW class PWR with large dry CV (4 loop PWR)
- 1100 MW class PWR with ice-condenser CV (4 loop PWR)

JNES has performed level 1 through level 3 PSA for internal events during power operation for the representative plants in each category. With regard to shutdown operation, JNES has developed level 1 PSA models for internal events for representative plants except ABWR and PWR with ice-condenser CV.

As the application areas of PSA are expanded, PSA models other than representative plants are required and JNES has, therefore, developed additional PSA models reflecting difference of plant design.

As for external event PSAs, JNES has developed seismic level 1 through level 3 PSA models for eight representative plants, which are same as internal event PSAs. Additional seismic PSA models have been developed to consider the difference of plant design as well. Other external events, such as fire and flooding are in studying phase.

JNES has performed level 1 and level 1.5 PSA which are used to derive core damage frequencies (CDFs), containment failure frequencies (CFFs) and relevant information for internal event during power operation for FBR "Monju" in order to review AM strategies developed by JAEA and to study application of PSA.

PSAs developed by JAEA

JAEA has conducted 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 level 1 and level 2 PSA programs as part of the development of sodium-cooled fast breeder reactor systems. Particularly in order to evaluate the effectiveness of AM measures in FBR "Monju," JAEA performed level 1 and level 1.5 PSA which are used to derive CDFs, CFFs and relevant information for internal event during power operation.

PSAs developed by utilities

Utilities that operate nuclear power plants performed individual plant examinations (IPEs) and established AM strategies. These PSAs cover level 1 and level 1.5 for internal events during power operation. PSA methodologies used in IPEs were developed mainly by their cooperative projects for PWRs and/or BWRs. In addition, they performed level 1 PSAs during shutdown operation as well. The results of both power operation and shutdown operation are presented in PSR reports.

They use risk importance obtained from IPEs during power operation to determine importance of SSCs for maintenance programs in the new inspection system for nuclear power plants which was initiated in 2009.

6. PSA methodology and data

General description: 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 AESJ standard. Specific methodologies used in the PSAs performed by JNES are described in its PSA reports.

Generally, level 1 PSAs for internal events in Japan performed according to the NSRA procedure guide, which was made on the basis of NUREG/CR-2300. The AESJ standard is becoming to be used.

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 analyzed 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 were derived from US ones such as LER and IEEE Std.500 except for fail-to-start of DG. On the other hand, failures of components found in periodic inspection and surveillance test in Japanese NPPs are registered in NUCIA and generic component failure rates and plant specific failure rates can be estimated. NUCIA data being endorsed, PSAs using these data will be utilized in the various areas.

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 using THERP methodology based on the operating manuals at accident and the status of operator training.

7. PSA applications

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.

Utilities conducted 43 level 1 and level 1.5 PSAs in which the scope of PSA is limited to derive containment vessel failure frequency on each of all Japanese operating NPPs. These Individual Plant Examinations (IPEs) cover 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 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 state-of-the-art 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.

NISA²⁰ 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

²⁰ MITI was reorganized to METI in January 2001 and NISA is the regulatory agency belonging to METI.

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 NISA in February 2002. The effectiveness of the AM on CDF and containment failure frequency (CFF) were evaluated through level 1 and level 1.5 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.

NISA reviewed these AM Implementation Reports for eight typical NPPs including the effectiveness of the AM measures on CDF and CFF in an AMWG (Accident Management Working Group). NUPEC has also performed level 1 and level 1.5- PSAs for the above eight NPPs to support technical reviews by NISA. Review Reports by NISA 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 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 and 1.5 PSA for the particular NPPs. The review report will be submitted to NSC in near future.

For the newly constructed NPPs which begin commercial operation in 2002 or later, it is recommended by NSC to establish an AM implementation plan before the first fuel loading to the core and submit the plan to the regulatory body for review. According to this process, AM measures for newly constructed NPPs were investigated and reported to NISA. The results were reviewed by NISA with technical support of JNES and reported to NSC.

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 procedures guide for PSA

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 coincident with the high-pressure coolant injection being unavailable. The reactor was manually shut down immediately after the pipe rupture occurs 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 Electric Power Company, NISA 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 CDF. On May 13, 2002, NISA issued a report that describes the investigation results including the event causes identified, NISA'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.

Evaluation of Allowed Outage Time (AOT) using 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 had 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 level 1.5 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 NISA, had 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 level 1.5 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 of Risk Information in Nuclear Safety Regulations, NISA, in collaboration with JNES, developed Near-Term Implementation Plan for utilization of risk information. The Near-Term Implementation Plan was developed 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 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 shutdown 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.

This Near-Term Implementation Plan was revised in January 2007 reflecting its progress and circumstances.

New Inspection System for NPPs: New inspection system for NPPs started in January 2010. In this new inspection system, three new elements were introduced, i.e.

- New Maintenance Program Framework,
- Root Cause Analyses for Non-conformance Event, and
- Comprehensive Plant Performance Assessment.

In the new maintenance program, risk information obtained from PSA is used to decide importance of systems and functions. Using this importance, maintenance strategy is drawn up. In addition, risk information is used to establish performance criteria which are used to review the efficiency of maintenance program. Utilities decide importance of systems and functions for maintenance activities using risk information obtained from PSA as well as the information obtained from deterministic point of view. The latter is provided in the Examination Guide for Classification of Importance of Safety Systems issued by NSC in Japan. Based on the importance of systems, the utilities decide performance criteria and monitoring plans in order to review efficiency of maintenance plans and reliabilities of systems. NISA and JNES review importance of systems and functions and performance criteria both of which are decided by the utilities.

In the comprehensive plant performance assessment, performance indicators are reviewed and significant determination process (SDP) evaluation is conducted. In SDP, inspection findings discovered in the fitness-for-safety inspection, periodic safety management review and periodic inspection of the plant are reviewed from the view points of safety, exposure of dose and quality assurance. Based on this assessment, importance of the finding is categorized into class 1 to 4 and none class. The results of assessment of SDP are combined with the result of performance indicators to obtain comprehensive plant performance. The results of this comprehensive plant performance assessment is reflected to the next inspection plans of the plant. SDP is now in the trial application phase and this framework is subject to be changed.

7 PSA applications

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.

Utilities conducted 43 level 1 and level 1.5 PSAs in which the scope of PSA is limited to derive containment vessel failure frequency on each of all Japanese operating NPPs. These Individual Plant Examinations (IPEs) cover 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 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 state-of-the-art 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.

NISA²¹ 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.

- f. Implementation system for AM
- g. Facilities and equipment, etc. related to implementation of AM
- h. Knowledge base related to implementation of AM (procedures of actions which are deemed to be effective and appropriate to be studied beforehand)
- i. Notice and communication related to implementation of AM
- j. 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 NISA in February 2002. The effectiveness of the AM on CDF and containment failure frequency (CFF) were evaluated through level 1 and level 1.5 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.

NISA reviewed these AM Implementation Reports for eight typical NPPs including the effectiveness of the AM measures on CDF and CFF in an AMWG (Accident Management Working Group). NUPEC has also

²¹ MITI was reorganized to METI in January 2001 and NISA is the regulatory agency belonging to METI.

performed level 1 and level 1.5- PSAs for the above eight NPPs to support technical reviews by NISA. Review Reports by NISA 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 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 and 1.5 PSA for the particular NPPs. The review report will be submitted to NSC in near future.

For the newly constructed NPPs which begin commercial operation in 2002 or later, it is recommended by NSC to establish an AM implementation plan before the first fuel loading to the core and submit the plan to the regulatory body for review. According to this process, AM measures for newly constructed NPPs were investigated and reported to NISA. The results were reviewed by NISA with technical support of JNES and reported to NSC.

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 procedures guide for PSA 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 coincident with the high-pressure coolant injection being unavailable. The reactor was manually shut down immediately after the pipe rupture occurs 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 Electric Power Company, NISA 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 CDF. On May 13, 2002, NISA issued a report that describes the investigation results including the event causes identified, NISA'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.

Evaluation of Allowed Outage Time (AOT) using 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 had 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 level 1.5 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 NISA, had 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 level 1.5 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 of Risk Information in Nuclear Safety Regulations, NISA, in collaboration with JNES, developed Near-Term Implementation Plan for utilization of risk information. The Near-Term Implementation Plan was developed 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 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.

e. 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

f. 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

g. Accident & Emergency preparedness

- Review the expansion of the scope of AM for shutdown operation
- Evaluation of Accident Sequence Precursors

h. 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.

This Near-Term Implementation Plan was revised in January 2007 reflecting its progress and circumstances.

New Inspection System for NPPs: New inspection system for NPPs started in January 2010. In this new inspection system, three new elements were introduced, i.e.

- New Maintenance Program Framework,
- Root Cause Analyses for Non-conformance Event, and
- Comprehensive Plant Performance Assessment.

In the new maintenance program, risk information obtained from PSA is used to decide importance of systems and functions. Using this importance, maintenance strategy is drawn up. In addition, risk information is used to establish performance criteria which are used to review the efficiency of maintenance program. Utilities decide importance of systems and functions for maintenance activities using risk information obtained from PSA as well as the information obtained from deterministic point of view. The latter is provided in the Examination Guide for Classification of Importance of Safety Systems issued by NSC in Japan. Based on the importance of systems, the utilities decide performance criteria and monitoring plans in order to review efficiency of maintenance plans and reliabilities of systems. NISA and JNES review importance of systems and functions and performance criteria both of which are decided by the utilities.

In the comprehensive plant performance assessment, performance indicators are reviewed and significant determination process (SDP) evaluation is conducted. In SDP, inspection findings discovered in the fitness-for-safety inspection, periodic safety management review and periodic inspection of the plant are reviewed from the view points of safety, exposure of dose and quality assurance. Based on this assessment, importance of the finding is categorized into class 1 to 4 and none class. The results of assessment of SDP are combined with the result of performance indicators to obtain comprehensive plant performance. The results of this comprehensive plant performance assessment is reflected to the next inspection plans of the plant. SDP is now in the trial application phase and this framework is subject to be changed.

8. Results and insights from the PSAs

Industries in Japan implemented AM countermeasures to all of conventional LWRs by the end of February in 2002 under the strong recommendation by NISA. In addition, industries provided PSA results of NPPs 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 containment failure frequencies (CFFs) for 52 NPPs after implementations of AM. PSA results showed CDFs of 52 NPPs are less than 10^{-6} (1/r.y) and CFFs are less than 10^{-7} (1/r.y).

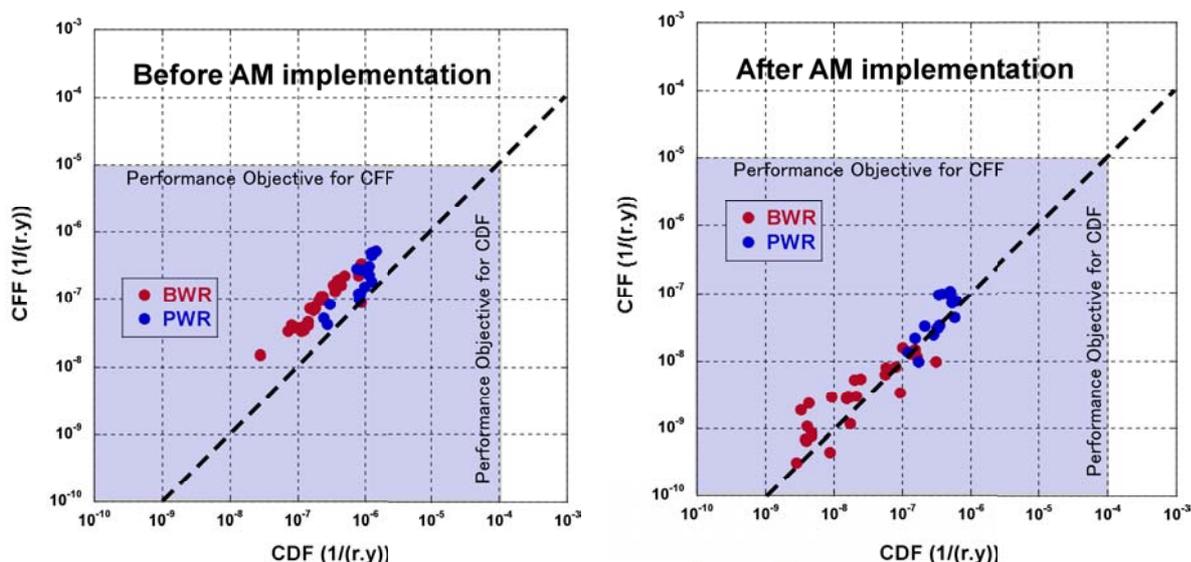


Figure 1. CDF & CFF for Conventional LWRs in Japan after AM Implementation

9. Future developments and research

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.

Reliability Analysis for Passive Safety Features

JAEA addresses development of the reliability evaluation method on passive safety as part of development project of the Japan sodium-cooled fast reactor (JSFR). The passive safety features embedded in JSFR are (1) the rapid reactor shutdown by means of the self-actuated shutdown system (SASS) under anticipated transient without scram events, and (2) the decay heat removal by the natural circulation cooling. In this evaluation method, the failure probability of the passive features is evaluated by combining the sensitivity analysis on plant transient response with evaluation of uncertainty factors of various design parameters such as SASS actuation temperature, coolant flow rate halving time of flow coast down, etc.

Component Reliability Database

Component reliability data for commercial light water reactor plants were collected by the utilities and centralized at CRIEPI, and they were statistically analyzed. A set of component reliability data for PSA developed by CRIEPI, which was 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 system (CORDS) for FBR, JAEA continues to make an effort to collect the operational data and failure data primarily related to FBR-specific components applied to 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.

With regard to sodium-cooled FBRs, JAEA consolidated the analytical methodologies and technical basis for all phases/sequences to be evaluated in level 2 PSA. In addition to the existing computational codes such as SAS4A, SIMMER-III, DEBNET, ARGO and APPLHOS, JAEA newly developed MUTRAN and SIMMER-LT codes in order to evaluate the long term behaviors of the materials relocation in the degraded core. These tools enabled the systematic assessment for the in-vessel accident sequences. For the ex-vessel accident sequences, JAEA also improved CONTAIN/LMR code taking into account the feature of sodium-cooled FBRs and verified the analytical models in CONTAIN/LMR by utilizing the new experiments such as sodium-concrete reaction test. In addition, the technical basis for constructing phenomenological event trees was compiled, in which the dominant factors having significant effects on the event progression were corresponded to the related experiments and analytical 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.

JNES has been promoting the level 3 PSA program. In the program, the MACCS-2 code has been extensively applied to analyze off-site radiological consequences for seismic events at typical BWR and PWR plants in Japan. JNES has been developing the level 3 PSA methodology to estimate average individual risks for multi-unit sites on safety goals considering some plants accidents occurred simultaneously at seismic event.

Seismic Risk Analysis

JAERI and JNC established whole sets of methodologies for seismic risk analysis of LWR and FBR, respectively and those works are succeeded by JAEA. JAERI published a report on its seismic PSA for a generic BWR in 1999. Then, 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. On one hand, JNC carried out a seismic PSA for FBR in order to study the rationalized seismic design, maintaining and/or improving safety during seismic event. JAEA recently addresses a study on fragility evaluation of seismically isolated building as part of development of the JSFR.

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.

10. References

1. Nuclear Safety Commission, “Accident Management as a Measure against Severe Accidents at Power Generating Light Water Reactors,” (1992).
2. Ministry of International Trade and Industry, “Accident Management for Light Water Nuclear Power Reactors,” (1994).
3. Special Committee on Safety Goals, Nuclear Safety Commission, Japan, “Interim Report on Research and Deliberations on Safety Goals,” (2003).
4. Special Committee on Safety Goals, Nuclear Safety Commission, Japan, “Performance Goals for Nuclear Power Plants Equivalent to the Interim Safety Goals,” (2006).
5. Nuclear Safety Commission, Japan, “Basic Policy on Introducing Nuclear Safety Regulations using Risk Information,” (2003)
6. Nuclear Safety Commission, Japan, “Revision of Examination Guide for Seismic Design of Nuclear Power Reactor Facilities,” (2003)
7. Nuclear Safety Commission, Japan, “Interim Report on Taskforce for Introduction of Risk Informed Regulation, Issues and Perspectives” (2005)
8. Nuclear and Industrial Safety Agency, Japan, “Basic Concept to Apply ‘Risk Information’ to Nuclear Safety Regulation,” (2005)
9. Nuclear and Industrial Safety Agency and Japan Nuclear Energy Safety Organization, Japan, “A Near-Term Implementation Plans of Risk-Informed-Regulation,” (2005)
10. Nuclear and Industrial Safety Agency, Japan, “High-Level Guidelines for Utilization of “Risk Information” in Safety Regulations for NPPs – Trial Use -,” (2006)
11. Nuclear and Industrial Safety Agency and Japan Nuclear Energy Safety Organization, Japan, “PSA Quality Guidelines for NPP Applications –Trial Use -,” (2006)
12. NUClear Information Archives, <http://www.nucia.jp/>

13. Atomic Energy Society of Japan, Japan, “A Standard for Procedures of Probabilistic Safety Assessment of Nuclear Power Plants (Level 2 PSA): 2008,” (2009).
14. Atomic Energy Society of Japan, Japan, “A Standard for Procedures of Probabilistic Safety Assessment of Nuclear Power Plants (Level 3 PSA): 2008,” (2009).
15. Nuclear Safety Commission, Japan, “Regulatory Guide for Reviewing Classification of Importance of Safety Function for Light Water Nuclear Power Reactor Facilities,” NSCRG: L-DS-I.01, (2009).

Contact

Technical Support Organisation	Direct Contact
Japan Nuclear Energy Safety Organization (JNES) Nuclear Energy System Safety Division Probabilistic Safety Assessment Group TOKYU REIT Tranomon Bldg., 3-17-1, Toranomon, Minato-ku, Tokyo, 105-0001 Japan	Haruo FUJIMOTO JNES Nuclear Energy System Safety Division Probabilistic Safety Assessment Group Tel:+81-3-4511-1711, Fax:+81-3-4511-1897 E-mail: fujimoto-haruo@jnes.go.jp URL http://www.jnes.go.jp

12. KOREA

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and environment

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 1994, 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. Five regulatory principles are independence, openness, clarity, efficiency, and reliability of regulation. 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 actions, taking into account the possibility of severe accidents. The Korean Nuclear Safety Commission proclaimed the Severe Accident Policy 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 main elements of the policy are as follows:

- (1) Establishing Safety Goals (Quantitative Health Objectives);
- (2) Implementing level-2 PSA for operating NPPs;
- (3) Providing capability for preventing and mitigating features against severe accidents;
- (4) Establishing severe accident management program (SAMP).

In addition, the regulatory body has been working on the development of regulatory guides thereafter to assure the consistency in the regulatory review of PSA. In terms of PSA implementation, the policy states: *"PSAs should be performed in order to determine countermeasures such that the risk from the NPPs is reduced as low as reasonably achievable. For those accident scenarios dominantly contributing to core 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."* In Korea, PSAs have been carried out by several organizations: CRI (Central Research Institute) which is subsidiary research organization of the state-owned utility (Korea Hydro and Nuclear Power Company; KHNP), KAERI (Korea Atomic Energy Research Institute), and KEPSCO E&C (previous KOPEC). Major activities are focused on the development of the PSA models and methods, the use of PSA in design stage, and PSA applications to operational safety and performance improvement such as risk-informed application.

Regulatory reviews are in charge of KINS (Korea Institute of Nuclear Safety) which is a regulatory supporting organization to NSSC (Nuclear Safety and Security Commission), Korea regulatory body. From 2006, a comprehensive risk-informed regulation (RIR) implementation plan was established and has been being implemented since then in order to improve regulatory inspection systems and decision making process utilizing risk insights from PSA.

During the March 2010 to February 2012, KHNP performed the risk-informed application for ILRT (Integrated Leak Rate Test) interval extension of Kori Unit 1, YGN 5&6, and UCN 5&6. For the purpose, KHNP developed a web-based offsite consequence analysis program. As a result, KINS approved the ILRT application for YGN 5&6 in November 2011. In January 2012, KHNP began to start the periodic update of the existing PSA models for the KHNP fleet (Kori Units 1-4, UCN 3&4, and YGN 1-6). Major concern of the update is to reflect the recent reliability data and to revise the existing PSA/RIMS models as-built, as-operated manner. The project will be continued until the end of 2013.

3. Numerical Safety Criteria

In Korea, the performance goals for preventing reactor core damage reactor and limiting radioactive materials release through the containment are being studied by KINS with considerations of reactor types, numbers in a site and operating and constructing conditions.

No quantitative safety criteria in designing plants have been officially used in Korea. However, 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 implement the above goals to NPPs, No quantitative safety criteria for designing plants have been officially used in Korea. However, the (Severe Accident Policy) 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 implement the above goals to NPPs, KINS has been developing quantitative performance goals which are surrogate measures of the high level safety goals. As surrogates for quantitative safety goals, the performance measure should be chosen considering both prevention of core damage and reduction of radioactive material release. Thus the performance measures should be clearly defined, easily quantified, and should represent early and cancer fatalities. Performance measures of CDF and LERF were chosen and the specific values were determined based on the estimation of health risks to the public.

CDF is defined as the frequency of accidents that can cause the fuel in the core to be damaged. In PWR, core damage occurs when a PCT exceeds 2200 °F. And in case of CANDU reactors, it is defined as failure of two or more fuel channels. LERF is defined as the frequency of accidents leading to significant, unmitigated release from containment in a time frame prior to effective evacuation when there is a potential for early health effects. Since the definition of LERF involves with the clarification of “large” and “early”, 4 different cases for definitions of LERF has been studied. The first case is the definition which Korean utility used in their PSA assessment. It includes the containment function failure modes of ECF (Early Containment Failure), containment bypass and containment isolation failure. The second case is the addition of containment failure before reactor vessel break to the definition of the first case. In this definition, whether specific containment function failure is included in LERF or not is determined by the available evacuation time. If the time interval from core uncover to atmospheric release is shorter than 6 hours, the appropriate emergency response plan can't be implemented, and it is included in LERF. The third and fourth cases are involved in the amount of some specific radioactive materials. The third case involves with release of Iodine, Cesium and Tellurium, and the fourth case involves with release of Iodine. Through the case study, the definition for the second case is to be used since it accounts for the evacuation time and it is easier to be clearly defined and easily quantified than other cases.

To determine the specific values for the performance measure, it is necessary to know the risk level of early fatality from other accidents and cancer fatality from other causes since the QHOs were established as 0.1% of risks from other causes. Those risk levels were obtained based on the National Statistics data during the period of years 1983 through 2006. Next, it is needed to determine the conditional probability of prompt and cancer fatality under the conditions of containment failure or core damage. Then, the

performance goals can be determined to satisfy the quantitative safety goals.

Regarding the early fatality from accidents, the average risk was $6.935E-4/\text{yr}$ and the safety goal for early fatality from accident of NPP was determined as $5E-7/\text{yr}$ conservatively. As for the cancer fatality from other causes, the risk level was $1.115E-3/\text{yr}$ and the safety goal for cancer fatality from operation of NPP was determined as $1E-6/\text{yr}$ conservatively. With the similar arguments to those in NUREG-1860, the individual early risk can be derived from summation of products of LERF and conditional probability of early fatality for each accident sequence. The conditional probability of early fatality was estimated by using MACCS2 code calculation result with source term information from level-2 PSA and site-specific meteorological data and population distribution with applicable emergency response plan. Regarding emergency response plan, dose dependent relocation without evacuation was selected after case studies for several different emergency response plans. The safety goal for early fatality was $5E-7$, and the maximum estimated value of CPEF for operating plants in Korea was $1.29E-2$. Thus LERF should be less than $3.87E-5$ to meet the safety goal. The performance goal for LERF is determined as $1E-5/\text{RY}$.

The individual latent risk can be derived from the similar formula to individual early risk. It is a summation of products of CDF and conditional probability of cancer fatality for each accident sequence. Conditional probability of cancer fatality is needed to determine the specific performance goal for CDF. It was also estimated by using MACCS2 code calculation result. With the similar process to determination of LERF, the performance goal for CDF is determined as $1E-4/\text{RY}$.

The performance goals will be used as target or objective values rather than limit values. The reason to use as objective values is the large uncertainties involved in calculating performance measures. It is necessary to do some more studies for addressing several other aspects of applications, which include difference in design between PWR and CANDU plants, effects from several units in a site, different safety level of existing and new plants, and so on.

To have public acceptance for the future reactors, the increase of risk due to addition of new plants should be low as much as possible. So, it is considered the performance goals for future reactors should be one tenth of those for operating plants, namely $1E-5/\text{ry}$ for CDF and $1E-6/\text{ry}$ for LERF. Regarding the scope of analysis, all the initiating events should be considered in principle. But, in reality, risks from external events or shutdown condition have large uncertainties in its analysis. Thus, in the application of performance goals, the applicability should be judged with consideration on the level of analysis technology and uncertainties.

4. PSA standards and guidance

In Korea, regulatory guidelines on PSA and risk-informed applications were developed by the Korean Institute of Nuclear Safety (KINS).

A series of regulatory guidelines for regulatory review of PSA level-1, level-2 and level-3, and external events have been finally issued in 2011. In addition, regulatory guidelines on RIR in general and the specific application of RIR to technical specification changes were also issued by KINS in 2011.

Regulatory Guidance on PSA quality:

Since the issuance of SAP (Severe Accident Policy) which enforced the utility to perform PSA for all operating plants, all kinds of risk information are available for improving current regulatory framework. In addition, with full availability of PSA results for all operating NPPs, it is expected that a series of risk-

informed applications (RIAs) be submitted to the regulatory body for approval.

Usually, risk-informed decision making requires the risk information enough for ensuring the technical adequacy. This information should be provided with the best available PSA elements including sufficient work scope covering the objectives of RIAs. Therefore, there are lots of regulatory concerns associated with the PSA quality for RIA. It is also noted that making general requirements and determining specific check points are essential for the regulatory decision making process. The regulatory guidance for assuring PSA quality is being prepared. Its primary goal is to review all kinds of information related with PSA quality and to identify and correct the limitation or weak points in the RIA submittals. It is also intended that the risk information on RIAs be technically checked for consensus with PSA standards (e.g., ASME standard for internal events), and to satisfy the minimum requirements (e.g., Category 1, 2, or 3) for each item as appropriate for the intended applications.

Regulatory Guide on Maintenance Effectiveness:

To keep adequate operational performance of plant SSCs, their reliable operability for protecting public's health and property against any radiological hazards have to be assured. In addition, one of important regulatory technology for public acceptance is to preserve operational safety related with the maintenance of a lot of active SSCs. As a fundamental of domestic utilization of performance-based regulation, a performance monitoring program to check the impact of risk changes on SSCs is needed. Furthermore, the necessity on the verification of the secondary system performance has also been raised to reduce unplanned plant shutdown. The utility is developing maintenance effectiveness monitoring program, and pilot program was started in 2006. The regulatory guidelines for regulatory review and inspection on this program are under preparation. In 2008, based on the interim guidelines, KINS inspected and reviewed the utility's program to check the adequacy and applicability of both the program and the regulatory guidelines.

5. Status and Scope of PSA Programs

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, APR-1400 which is called evolutionary plant was decided to do full scope (Level 3) PSA for using PSA insights in a standardized design and operation.

In 2007, the utility(KHNP) has completed PSAs and risk monitoring systems for all operating plants as scheduled in the implementation plan to follow SAP. Plant specific PSAs for all operating NPPs consist of Level-1 and Level-2 internal/external events. However, for constructing NPPs, the Level-1 internal event PSA for low power/shutdown operation should be added to the PSA scope of operating plants.

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. 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 for the shutdown stage. In addition, the revisions of their PSAs were completed in 2006 reflecting operating experiences. The revised PSAs for Yonggwang units 3&4 and Ulchin units 3&4 adopted the revised analysis methodologies, 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 construction phase, and Wolsong unit 1 which started the commercial operation in 1983 performed the PSA in 2003 again. These PHWR NPPs revised their PSAs, and made efforts to improve the consistency for success criteria, etc. The seismic event analysis for Wolsong unit 1 was performed using SMA. All PSAs of the above plants were revised with operating experiences by 2007. 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 for the shutdown stages.

Shin-Kori units 1&2 and Shin-Wolsong unit 1&2, advanced KSNP OPR 1000 units, are being constructed by 2011 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 level compared to the core damage frequency (CDF) of the previous KSNPs at the design developing process.

Shin-Kori units 3&4 are the plants based on APR-1400 design which has been developed in Korea with the concept of evolutionary design. In the process of the APR-1400 development, Level-3 PSA during the full power operation and Level-1 PSA during the shutdown operation were also performed for the internal and external events. Through these PSA results, it was verified the plants have lower risk level than the previous OPR-1000 plants.

PSAs for regulatory uses

In any regulatory matters 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 guaranteeing safety, the regulator should provide the measurable 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 regulatory guidelines 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 just depending on the licensee's information. The MPAS model for KSNP (Korean Standard Nuclear Power Plant) was developed with the scope of Level 1 in 2005, which aims at

having the equivalent quality of ASME PSA capability category II. In 2008, the MPAS Level-1 model for Westinghouse 2 loop plant was developed as well. Additionally, the model for Westinghouse 3 loop plant developed in 2010. The MPAS models for evaluating LERF (large early release frequency) are being developed.

6. PSA methodology and data

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 now, but newly constructed plants (APR-1400) should perform Level-3 PSA. 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 modeled 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 analyzed. 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:

FTREX (Fault Tree Reliability Evaluation eXpert) is a tool for generating minimal cut sets (MCSs) by solving Probabilistic Safety Assessment (PSA) fault trees. FTREX is based on a Zero-suppressed Binary Decision Diagram (ZBDD) algorithm. The ZBDD algorithm is an important variation of a Binary Decision Diagram (BDD) algorithm. The ZBDD algorithm can quickly solve a large fault tree and generate numerous MCSs.

A ZBDD is an efficient data structure that encodes MCSs [1]. The ZBDD structure is interpreted as factorized form of MCSs. By optimally choosing the factorization order, that is, a ZBDD variable ordering, the ZBDD size can be minimized significantly. A new ZBDD algorithm was constructed by developing special formulae for Boolean operations for two ZBDDs [2].

FTREX provides a significant improvement in the quantification speed for large PSA models with a small size memory. FTREX has many unique features in fault tree restructuring, gate expansion, subsuming, and data storage. As an independent fault tree solver, FTREX can be used with a number of PSA software packages and online risk monitoring systems. Currently, FTREX has an interface with KIRAP [3] and EPRI R&R Workstation tools [4].

- [1] S. Minato., "Zero-suppressed BDDs for set manipulation in combinatorial problems," Proc. of the 30th Int'l Conf. on Design Automation, pp. 272-277, (1993).
- [2] W.S. Jung, S.H. Han, J.J. Ha, "A Fast BDD Algorithm for Large Coherent Fault Trees Analysis," Reliability Engineering and System Safety, Vol. 83, pp. 369-374, (2004).
- [3] S.H. Han, "PC-workstation based level 1 PRA code package-KIRAP," Reliability Engineering and System Safety, Vol. 30, pp.313-322, (1990).
- [4] Electric Power Research Institute, FTREX User Manual Version 1.4, EPRI, Palo Alto, CA, (2008).

7. PSA applications

Many plant specific PSAs, which were finished according to the 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 allowed outage time (AOT) of reactor protection and engineered safety features actuation system of Kori units 3&4 and Yonggwang units 1&2 which was performed in 1999. After that, several technical specifications

optimization projects were launched and submitted to KINS, which were approved or being still reviewed. The following lists are past and current PSA applications projects:

Relaxation of STI and AOTs:

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 considered both risk insights and system enhancements such as hardware upgrade and circuit card test program.

The topical report for STI relaxation from 1 month to 3 month for RPS/ESFAS of KSNP was submitted to MEST in 2010 and has been under review by KINS. In 2007, a plant got the approval of AOT extension for the inverter of essential power system. In 2010, Westinghouse 2 loop plant obtained approval for STI extension of RPS/ESFAS.

Risk-Informed In-service Inspection for piping of Ulchin unit 4:

- Optimization of in-service inspection points based on risk insights from level 1 and 2 PSA;
- Reduction amount of inspection points is half of previous inspection points;
- KINS approved the topical report on RI-ISI in 2008, and the utility got the approval for the site specific application in 2010.

ILRT (Integrated Leakage Rate Test) Interval Extension

Based on risk insights from level 1, 2 PSA and population dose analysis the applications for the containment ILRT interval extension from 5 years to 10 years were approved. By 2010, over 12 plants already have permission of the test interval extension.

8. Results and Insights from the PSAs

The PSA have several purposes. The important purposes are to verify the safety of NPPs, 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 showed 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

performance goals. Nowadays, Korea has the improved design plants such as OPR1000 (Optimized Power Reactor 1000) or APR1400 (Advanced Power Reactor 1400). Their estimated risk levels are much lower than IAEA recommendation.

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). 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 the 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 coastal 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 1-4, 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 pre-stressed concrete with steel or epoxy liner in all domestic plants except the Kori units 1&2. Kori units 1&2 have a steel containment structure surrounded by a concrete shield structure.

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 recommendation 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.

9. Future Developments and Research

Development of PSA Modeling Methodology and Related S/W

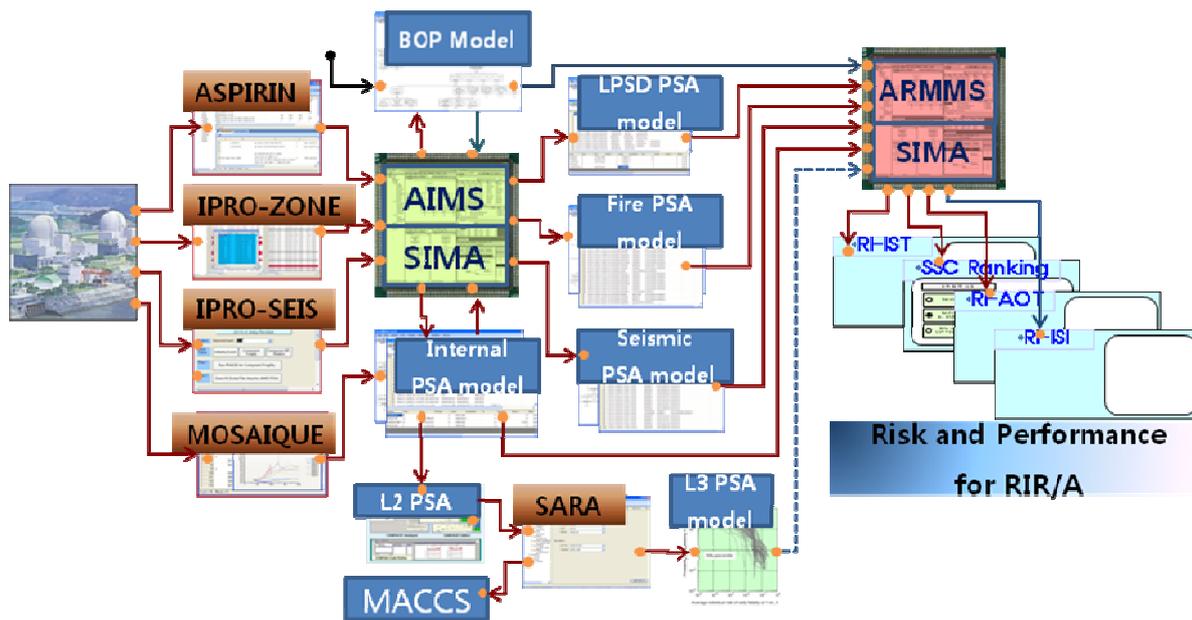
PSAs are widely used in many areas, so we need a lot of analysts. But, performing the PSA needs several skilled experts for following purposes:

- 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 OCEANS (Online Consolidation & Estimation Analyzer for Nuclear System). The targets of OCEANS are:

- Integration of full scope PSA;
- Easy and fast quantification;
- Traceability and reproducibility.

The OCEANS provides a more systematic and efficient framework for the risk assessment of all modes and all hazards. In order to build such a framework, we need to develop new algorithms and techniques. All of these efforts will enhance the PSA and RIA technology. The overall concept of OCEANS is depicted in the following figure with the detailed features of AIMS-PSA given in the following subsections.



Integrated PSA S/W package, OCEANS

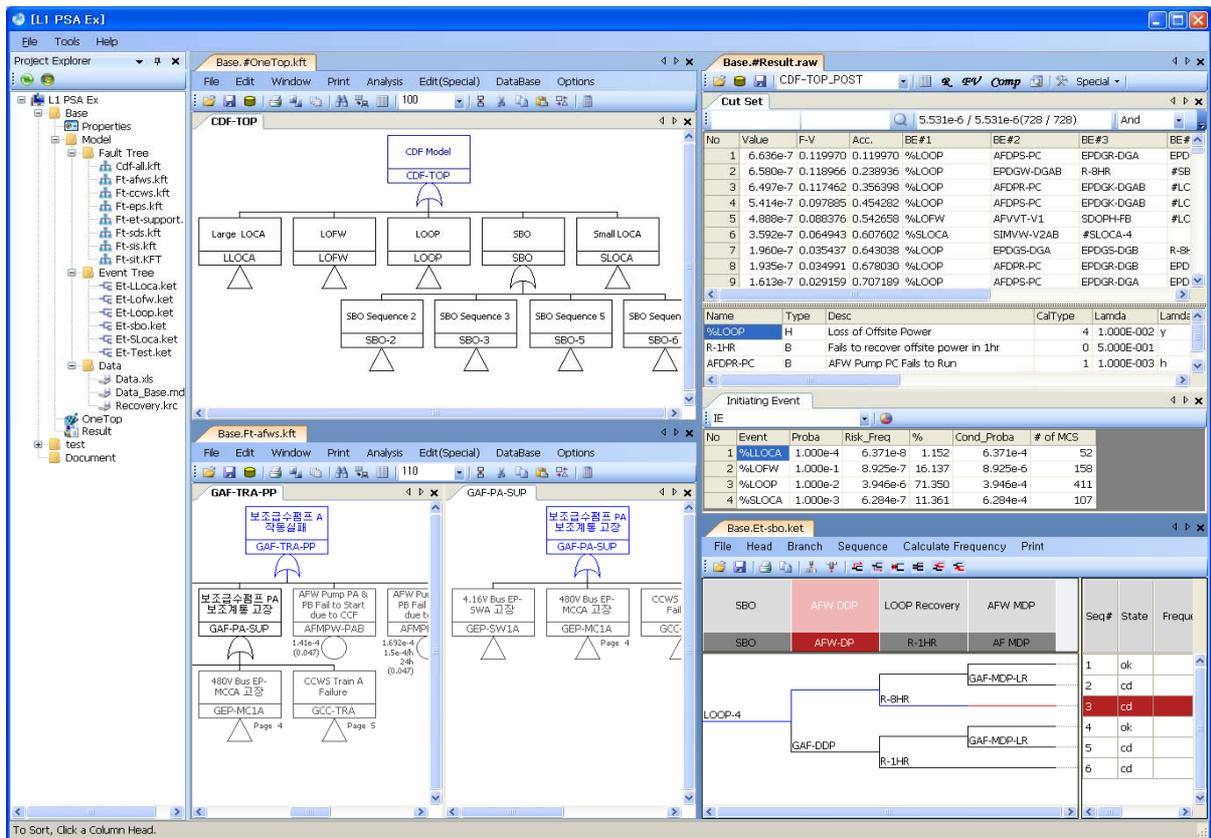
PSA Software AIMS-PSA for Integration of Event Trees and Fault Trees

The AIMS-PSA plays a key role in OCEANS, which takes charge of the event tree and fault tree analysis required in a Level 1 internal PSA. The AIMS-PSA is a fully redeveloped version of the KIRAP using the recent software technology in Windows environment. The project explorer is introduced to provide means to do most works such as browsing each model, quantifying the PSA, and viewing the results. The integrated approach implemented in the AIMS-PSA enables the user to finish the quantification of a PSA by executing just two menus (for integration and quantification of a PSA model) in the project explorer. Thus, the traceability and reproducibility are enhanced greatly.

In the 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 Level-1 PSA model for the UCN 3&4 units with the help of the FTREX quantification engine. The model has about 2800 gate events and 2500 basic events, and has also a lot of circular logics. Note that it takes several minutes to tens of minutes using other PSA software. The following figure shows the example screen of the AIMS-PSA.



PSA software, AIMS-PSA

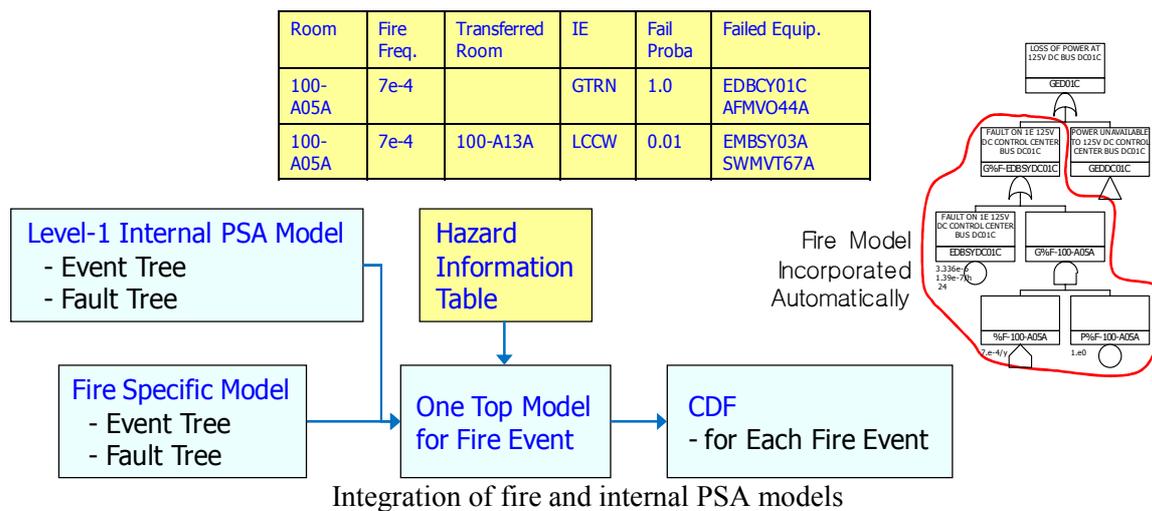
Integration of Level-1 & 2 PSA

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 LRF (LERF and LERF) or CFF (Containment Failure Frequency) for each event sequence are calculated. The information is transferred to the Level-2 PSA software.

Integration of Internal & External PSA

A typical fire PSA consists of modifying the PSA model affected by a fire event, calculating the conditional core damage probability (CCDP), the fire propagation, suppression factors, and the core damage frequency (CDF) for the fire event. This process was repeated for the number of fire zones. If the analysis is not automated, the quantification for fire zones requires a huge amount of manual works as well as a combined knowledge for PSA and fire analysis. In OCEANS, the necessary information is categorized systematically and stored in a database. Then OCEANS generates and quantifies the fire PSA model automatically. The following figure illustrates how OCEANS treats a fire PSA.



The information stored in the database comes from the fire hazard analysis. Because the necessary information is separated between PSA and fire hazard analysis, the basic information can be prepared by an expert of the fire analysis. This kind of approach enables PSA analysts to save time and effort to do the fire PSA. The seismic and flood PSAs can also be automated in similar ways.

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.

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.

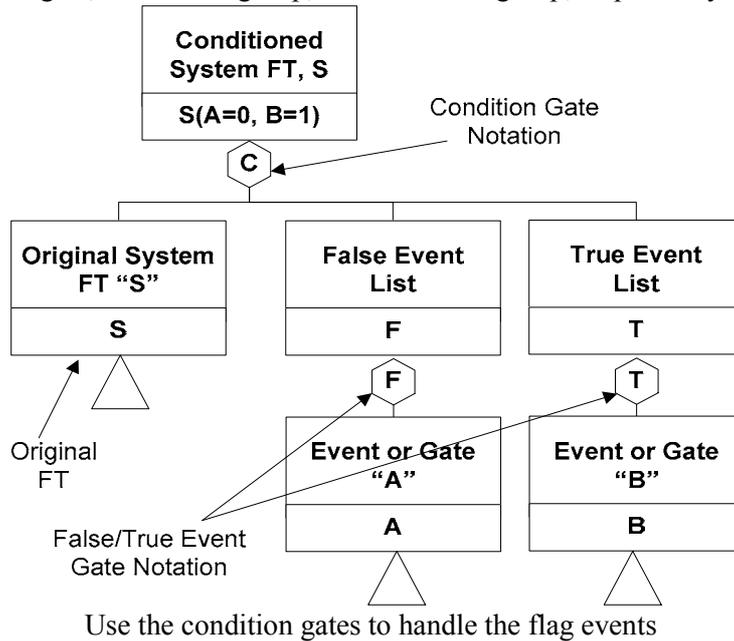
Another approach is to use the flag events in the fault trees. It is the simple way to handle such kind of situation. We can handle most cases via this approach in the one top PSA model which is typically used in a risk monitor. But, there are some cases that we can not model the changed conditions correctly 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:

- $SA[a] = SA(\text{FLAG}[A]-F = \text{False}, \text{FLAG}[A]-T = \text{True})$;
- $SA[b] = SA(\text{FLAG}[B1]-F = \text{False})$.

The following figures illustrate how we use the condition gates to handle the flag events. The gate types C,

F and T denote condition gate, false event group, and true event group, respectively.

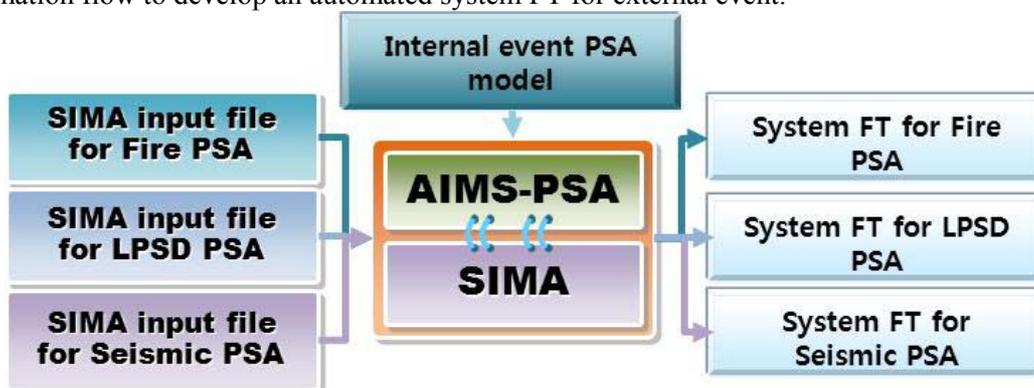


AIMS-PSA takes the fault tree with condition gates. It processes the condition gates, generates a fault tree without the condition gates, and passes the fault tree to the cut set generator. The use of condition gates enables us to build the one top model using the existing event trees and fault trees without excessive effort. It also saves the effort to manage the PSA model.

Common FT information linking module, SIMA

Various methods are used to develop the PSA models for external events such as fire, flooding, and earthquake in addition to LPSD PSA. Especially, when developing system FT for each external event, the conventional method is to use a system FT developed from internal event PSA model as a base. Then, the system FT is modified to reflect the specific condition of each external event. To perform such process, a lot of manual work is needed to modify the original FT and to replace the reliability data in the FT.

To overcome this inefficiency, new information linking module called SIMA (Script Interpreter for Mapping Algorithm) was developed. SIMA was embedded in AIMS-PSA. The information needed to construct a system FT for external event is structured and a database is generated. Using the database, SIMA automatically generates a system FT for an external event PSA model. The following figure shows the information flow to develop an automated system FT for external event.



The concept of system FT generation using SIMA

To automatically generate system FT for each external event including the event in LPSD period, consistent mapping rules are required to transform the original FT into new system FT suitable for external event. SIMA uses the following mapping rules.

Mapping rule of SIMA

Case	Example	Remark
Add+ Add*	Add+ A B Add* A B	Add or multiply event B to A respectively. When implementing this command, new gate called G&-A is generated. Then, event A+B or A*B is attached as child.
Add+	Add+ A B Add+ A D	When multiple events are added to event A, new gate G&-A is generated. Then, event B and event D is added.
Value	Value B 0.1	Assign 0.1 as the probability of event B
Desc	Desc B Desc of an Event	Insert description of event B
Set	Set A C	Replace event A with event C.
Set	Set A True Set E False	Set event A as true event Set event E as false event
Gate	Gate G + I1 I2	Insert Logics to Gate G
Special	DeleteExistingIEs	Set IE(initiating event) value as 0.

SIMA operates with various external event data generation program such as IPRO-ZONE(fire and flooding), PRASSE(seismic event). These external event data generation programs finally generate SIMA input files. Then, using these input files, SIMA generates system FT for external event PSA model. Using SIMA, one can reduce the resource for system FT development dramatically. Also, by automatic generation of FT, manual errors can significantly be eliminated.

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, AiMS-FTREX-CONPAS);

- Assessment of uncertainty bound due to different binning of the Level 1 accident sequences into the Level 2 plant damage states (PDSs);
- Treatment of complementary events in constructing the linked Level 1 and Level 2 fault trees;
- Containment fragility analysis methodology for internal pressure and thermal load under severe accident condition.

Another aspect of the Level 2 PSA R&D has been closely related to uncertainty analysis, including the following items:

- 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;
- Incorporation of the best-estimate and uncertainty analysis results into the plant-specific CET(Containment Event Tree)/DET(Decomposition Event Tree) models to obtain an optimized Level 2 risk metric (LRF): As of 2010, phenomenological uncertainty analysis for two CET/DET models (characterizing (1) pressure and temperature-induced RCS/SG tube creep rupture and (2) early containment failure, respectively) has been made and the resultant uncertainties have been incorporated into the UCN 3&4 LERF model to give the best estimate results for LERF. Both phenomena have been considered dominant contributors to LERF. For the former case, the MELCOR code has been utilized, which makes it to model natural convection phenomena in the RCS boundary. In order to take into account more versatile accident scenarios, the latter was analyzed with the MAAP code. In 2011, a similar approach will be applied to late containment failure model to obtain the best estimate results for LLRF and/or LRF.

Digital I&C PSA

The development of PSA methodology for digital instrumentation and control (I&C) systems has been an important issue since the first application of digital computer systems to safety-critical functions in nuclear power plants. The research activities are performed mainly on the methodology aspect and the model aspect of the digital I&C PSA. The main research activities are:

- Collection and analysis of the operating experience of digital I&C systems;
- Estimating software failure probability by integrating existing software reliability models;
- Estimating the coverage of fault-tolerant features such as watchdog timers;
- Estimating the coverage of automated self-checking algorithms;
- Development of the fault tree models for the digital-based safety-critical I&C systems.

Also, Korea has actively contributed to the OECD/NEA WGRISK Digital I&C Reliability (DIGREL) task group activities by introducing digital I&C PSA models and providing general principles for the development of failure mode taxonomy of digital I&C systems in nuclear power plants. Korea is also actively involved in bilateral research cooperation with other countries in this field.

Human Factors and HRA

As computer-based design features are being adopted in main control rooms (MCR) of nuclear power plants, a human reliability analysis (HRA) method capable of dealing with the effects of these design features on human behavior is needed. HRA is also considered an important element in support of the human factors design of new control rooms, as described in the Human Factors Engineering Program of NUREG-0711, Rev.2. In order to meet this demand, the study was undertaken to develop a new HRA method for computer-based control rooms, which produced the HuRECA method representing Human Reliability Evaluator for Computer-based control room Actions. The HuRECA method is based on the observation of operator behaviors from the human factors verification and validation experiments. Based on the observation of the operator behaviors under the computerized mockup of an advanced control room, several fundamental studies have been conducted for aiming to develop HuRECA, including analysis of

relationship between the operator's cognitive functions and the design features of advanced control rooms, task analysis and task performance analysis, analysis of error types and design-related influencing factors (DIFs). Especially, for the computer-based procedure (CBP), we derived a set of important DIFs for incorporating into HRA by applying the analytic hierarchy process (AHP) to a preliminary list of DIFs identified from the literature survey and the human factors validation experiments, and suggested diversified levels of the designed CBP by task type, and finally, provided graded weighting values for those diversified levels of the CBP determined from expert judgment and comparison with the existing HRA method. For the soft controls (SC), we reflected the complexity of the interface management tasks, which is also called secondary tasks indispensably required to perform primary tasks in controlling the power plant, and newly considered the error recovery possibility given by the information sharing capability between operating crew into the estimation of execution error probability. In addition to these, HuRECA provides necessary rules and judgment aids to help assessors in deciding appropriate levels or degrees regarding performance shaping factors. The HuRECA method is expected to be an effective tool for supporting control room human factors design for new power plants, as well as for conducting HRA of PSA for designed power plants, because it was developed upon the identification of new design features of computer-based control rooms and detailed design-related influencing factors and consideration of their effects on human reliability.

The safety of a nuclear power plant can be ensured through continuous and systematic maintenance work (plan/prevention/prediction) performed on a regular basis and repair work promptly implemented upon the occurrence of a malfunction. In the case of domestic NPPs, detailed procedures have been carried out based on predefined time periods because periodic testing and maintenance is one of the well-known strategies to secure the reliability of critical components. Unfortunately, it is not easy to perform test/maintenance procedures because small number of operating personnel has to manage a huge amount of procedures. For this reason, we developed a software tool called FIXPERTS (fixed and periodic test support system) to manage a lot of maintenance schedule. Human-induced errors such as wrong selection of switch panel in main control room can occur during maintenance operation and affect the plant safety in many ways. To reduce this, it is required to use a supporting tool that assists human operators' correct actions. For this reason, a software system framework called HIRITER (High Risk Inducible Task Evaluator) has been developed in this project. HIRITER calculates human error probability of each step of procedures and also simulates plant risk impact in advance. The HIRITER is aimed at providing information to operators to reduce human errors in maintenance/test activities.

Thermal Hydraulic Uncertainty Analysis Software for PSA (MOSAIQUE)

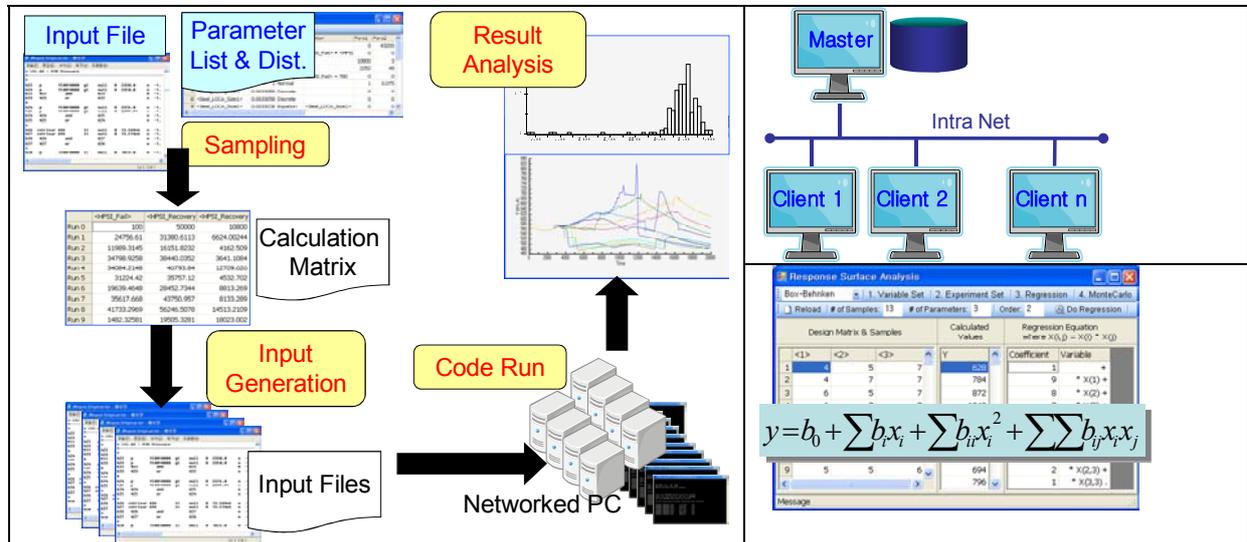
The thermal-hydraulic (T/H) analysis is widely used for the PSA model construction, especially in the development of event tree including success criteria of safety system and an available operator action time for accident mitigation. A best estimate T/H methodology which usually performs sampling calculation based on Monte-Carlo method is needed to enhance overall quality of PSA model. A computational program is required to handle massive calculation loads.

MOSAIQUE was developed to automate all process needed in the best estimate T/H methodology. MOSAIQUE is composed of three modules, named as master unit, client unit, and plot unit. Master unit generates sampling input for T/H simulation code. It uses spread sheet style window to assign information on the sampled parameters. Client unit controls the overall calculations by T/H simulation code. It uses Microsoft Access data base by which a client PC calculate each sampling case independently. Plot unit provide a tool for post processing for the result. It can generate a graph on the key parameters in addition to the generation of some statistical measures.

The unique feature of MOSAIQUE is to use a number of PCs in the intranet to reduce the computing time for a lot of computer code executions. Also the response surface analysis is incorporated. All of these tasks

are automated in Window environment with very few manual works.

MOSAIQUE can work with various safety analysis computer codes such as MARS, RELAP5, TRACE, MAAP4, and GAMMA. It can be also used for the uncertainty analysis of safety margin using the T-H safety analysis.



SW for uncertainty analysis of thermal hydraulic safety analysis, MOSAIQUE

13. MEXICO

1. *Introduction*

Here, no contribution is expected from the participants.

2. *PSA Framework and Environment*

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.

The Mexican Nuclear Regulatory policy establish that the PSA technology should be applied in all regulatory activities, where practical, to complement the deterministic regulation and to support the defence in depth philosophy. Therefore, two regulatory guides SN-01 and SN-02 were developed to be included, adapting the guidelines used in the USNRC RG-1.174 and 1.177, in the Mexican Regulatory Framework. The guides, which can be applied voluntary, establish a methodology to assess the impact on safety of proposals for permanent changes to the licensing basis and also, changes to the technical specifications, supported only by deterministic analysis or by a combination of deterministic and probabilistic analysis. The methodology considers relevant aspects such as safety margins, defence in depth, risk criteria and monitoring performance.

A procedure to link deterministic and probabilistic tools to evaluate operational events and inspection findings was developed looking for an integral decision making process and focus resources in the most relevant event and findings including the risk point of view. Modifications to NRC/SDP were performed to include a flow chart instead of a questionnaire in the first event/finding screening, and the worksheets developed as part of the procedure were automated in order to facilitate their application; the simplified PRA model required by the procedure was validated with the LVNPP IPE model.

Also, a Risk Based Inspection Guides (RBIG) has been developed to incorporate risk information into the inspections activities. The RBIG have been used to prioritize inspections and to optimize resources.

In terms of the PSA studies and their use in the operation of Laguna Verde, after the conclusion of the Individual Plant Examination several safety improvements has been implemented and a Risk monitor is been used to accomplish with the maintenance rule commitment.

3. Numerical Safety Criteria

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.

The Mexican Nuclear Regulatory Commission (CNSNS) has developed an adaptation of the USNRC Significance Determination Process (SDP) to evaluate the risk significance of operational events and inspection findings in Laguna Verde Nuclear Power Plant (LVNPP). The CNSNS developed a plant specific flow chart for preliminary screening instead of the open questionnaire used by the USNRC-SDP, with the aim to improve the accuracy of the screening process. Also, the work sheets and support information tables required by the SDP were built up in an Excel application which allows us to perform the risk evaluation in an automatic way, focusing the regulator staff efforts in the risk significance analysis

instead of the risk calculation tasks. In order to construct this tool a simplified Probabilistic Risk Assessment (PRA) model was developed and their results validated with those obtained using the full PSA model of the Individual Plant Examination.

The evaluation result by mean of this tool determines the corresponding risk level in accordance with the increase in Core Damage Frequency, and the result of the compute is boxed in one of four colors, which will tell us how severe the event/finding was, according with the next criteria:

- Green: Very low safety significance: Increase minor or equal to 10^{-6} /year.
- White: Moderate safety significance: Increase between 10^{-6} /year and 10^{-5} /year.
- Yellow: Substantial safety significance: Increase between 10^{-5} /year and 10^{-4} /year
- Red: High safety significance: Increase greater than 10^{-4} /year.

Risk monitor criteria:

The Laguna Verde Nuclear Power Plant (LVNPP) evaluates and manages the risk prior to taking out one or more structures, systems or components (SSC), to perform maintenance (preventive or corrective), which disables its function during operating condition 1 and 2 by mean of the Risk Monitor.

The result of the quantitative evaluation by mean of the Risk Monitor is based on the worst risk indicator (CDF or LERF); according to the resulting color will be defined risk management actions:

Color (Risk indicator)	Mining	Actions
Green $1.0 \leq \text{CDF}$ or $\text{LERF} < 2.0$	Minimal risk, the work is performed normally (not actions are required)	the work is performed normally.
Yellow $2.0 \leq \text{CDF}$ or $\text{LERF} < 10.0$	Moderated risk, take compensatory actions to not increase the risk level (orange or red).	Necessary measures should be taking to ensure that maintenance work does not increase the level of risk.
Orange $10.0 \leq \text{CDF}$ or $\text{LERF} < 20.0$	High risk, you need the authorization and approval to perform the work in this condition.	It is required the authorization of the operation chief and approval of the operation general manager to work in this condition. Take compensatory measures and contingency plans.
Red CDF or $\text{LERF} \geq 20.0$	Unacceptable risk, you should not perform any planned work in this condition.	Do not work planned in this condition voluntarily. If this condition is a result of emerging work, you must return inoperable or unavailable equipment is required, fig carry the plant to a safe shutdown condition. The shift supervisor must immediately notify the manager of the GCN, the deputy general manager of operations, and to all levels of the CLV, to take necessary steps and out of this condition.

4. *PSA standards and guidance*

Two regulatory guides SN-01 and SN-02 were developed adapting the USNR CRG-1.174 and 1.177 to be included in the Mexican Regulatory Framework. The guides establish a methodology to assess the impact on safety of proposals for permanent changes to the licensing basis and also, changes to the technical specifications, supported just by deterministic analysis or by a combination of deterministic and probabilistic analysis. The methodology considers relevant aspects such as safety margins, defense in depth, risk criteria and monitoring performance.

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.

The National Commission for Nuclear Safety and Safeguards (CNSNS) has initiated a program to incorporate risk-information into the Mexican regulatory framework. This emphasizes the need to expand the scope of the probabilistic safety analyses (PSA) of Laguna Verde Nuclear Power Plant (LVNPP) to cover accidents initiated by fire, external events and low power and shutdown operating modes.

Based in our experience during the review process of the Individual Plant Examination (IPE), we considered very useful the development of a process for the review and approval of the not in attendance PSA scope. The development of the review and approval process allow us to both teams, developers and reviewers, to be agree in advance in the level of detail and necessary technical quality of the PSA study. Therefore, we start the development of a review process for the LVNPP Fire-PSA.

The guideline set were developed to cover the state-of-the-art in the Fire-PSA methodologies that was public available, like the NUREG/CR-6850.

The detailed review process will be made on line, in which were reviewed the most significant aspects of the PRA that can be useful in the decisions of the CNSNS.

5. *Status and Scope of PSA Programs*

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 warranted 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 developed 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 according with the updating of the PSA used to support such tool, in the beginning the updating was performed on each refuelling, looking for introduce plant specific data. Actually the updating is performed each 5 years or when an important change in the plant is developed. For example, recently, the Comisión Federal de Electricidad (CFE) has requested to the CNSNS the approval of the Extended Power Uprate Project (EPU) of the LVNPP to increase the power to 2317 MWt. For this purpose, the CFE has been submitted, among others, the safety analysis report for its evaluation by CNSNS. The aforementioned report includes the results of security assessments carried out to justify the increased power of the plant. As part of the activities evolve in the Power Uprate, an updating of the PSA models needs to be developed.

Currently the CNSNS is updating the PSA level 1 for internal events taking into consideration the uprating of Laguna Verde NPP (20%), at the same time the PSA level 1, internal events, for low power and shutdown conditions for four operational stages has been started. In the same way the PSA level 2 is being updated and an uncertainty analysis is being developed.

6. *PSA methodology and data*

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, internal 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 SAPHIRE 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.

In fact, the APS level 2 developed by the regulatory authority is being updated by using a better model input and version of the code to simulate de severe accidents (MELCOR).

7. *PSA applications*

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 2.87×10^{-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 two regulatory guides SN-01 and SN-02, 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 were agreed on their trial use through the evaluation of one Operational Technical Specification modification. The evaluation included meetings to discuss the principal issues derived from the process as well as comments about the guidelines clarification and understanding as well as the role played by deterministic and probabilistic safety analysis into the decision making process.

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 and the worksheet were automated; 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.

Actually the PSA has also been used to plan the emergency scenario for the evaluation of the External Radiological Emergency Procedures (PERE).

Evaluation of operational events and inspection findings:

The Mexican Nuclear Regulatory Commission (CNSNS) has developed a Risk Evaluations System for Operational Events and Inspection Findings named SERHE, by its acronyms in Spanish. This tool is an adaptation of the USNRC Significance Determination Process (SDP). The SERHE has a plant specific flow chart for preliminary screening instead of the open questionnaire used by the USNRC-SDP, with the aim to improve the accuracy of the screening process. Also, the work sheets and support information tables required by the SERHE were built up in an Excel application which allows us to perform the risk evaluation in an automatic way, focusing the regulator staff efforts in the risk significance analysis instead of the risk calculation tasks. In order to construct this tool a simplified Probabilistic Risk Assessment (PRA) model was developed and their results validated with those obtained using the full PSA model of the Individual Plant Examination.

The PSA has also been used to evaluate the important changes in the plant, for example, recently, the Comisión Federal de Electricidad (CFE) has requested to the CNSNS the approval of the Extended Power Uprate Project (EPU) of the LVNPP to increase the power to 2317 MWt. For this purpose, the CFE has been submitted, among others, the safety analysis report for its evaluation by CNSNS. The aforementioned report includes the results of security assessments carried out to justify the increased power of the plant. As part of the activities evolves in the Power Uprate, a PSA evaluation was developed and re-evaluated.

8. Results and Insights from the PSAs

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 5.6×10^{-5} per year which is 10% less than the figure obtained in the IPE (6.18×10^{-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 5.25×10^{-5} compared with 2.59×10^{-5} 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.

9. Future Developments and Research

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 like the NUREG/CR-6850.

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.

10. References

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.

14. SPAIN

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

- In 1986 Spain started The PSA development. The “Integrated Programme on Performance and Use of PSA in Spain” (IP) was the conductive document of the activities that CSN and Spain in general, carried out in relation to the PSA in eighties and nineties. The IP was revised in 1998, and the second edition was issued by the CSN.

- In the years of experience with the IP first edition, the activities in the country went more along the line of PSA performance, first of the objectives indicated in the title of the IP. The second great objective was related to the use of PSA, the activities in relation to this objective had been more sporadic and, in general, carried out in an exploratory way.

- The second edition of the Integrated Program (1998) proposed the same general objectives, although the emphasis was directed towards the needed activities to apply the PSA to different fields. The second edition also included the CSN activities on PSA review and acceptance, it established the need of utility activities to revise and update the previous PSA projects. The second edition also discussed the activities to reach to a final and common scope of all the Spanish PSA. These types of activities were the basis for the development of PSA applications. Utilities developed their PSA projects which have been thorough reviewed by the CSN.

- On the other hand, all the Spanish NPPs have to renew their operation permits each ten years. In the operation permits issued in the eighties a Periodical Safety Review (PSR) and an updated PSA were required for NPPs, in this context all the Spanish NPPs have update their PSA not only updating data and design modifications but also since the methodological point of view.

- Finally as part of the Spanish Action Plan in the framework of the WENRA RHWG (Reactor Harmonisation Working Group), CSN has developed a legal framework for covering PSA Program. So in 2010 CSN issued a mandatory Instruction (IS 25): “Criteria and requirements on the performance of probabilistic safety assessments and their applications for nuclear power plants”.

- Thus, this Instruction is aimed at the Nuclear Power Plant (NPP) licensees, who must perform a probabilistic safety analysis in order to verify that all potential risk scenarios - including multiple failures, common-cause failures and human errors - have been properly weighed up in accordance with their expected frequency and estimated significance and that there are adequate and balanced preventive or mitigative measures to face up to those situations.

- The Instruction also requires the PSAs be updated by the licensee in a continuous manner or after every refuelling outage such that they reflect the reality of the plant at all times. As an essential part of PSA updating processes, NPP licensees have to keep appropriate databases to continuously collect the statistical experience needed for a better quantification of the frequency and probability parameters of the events included in the models of the PSAs. Also the instruction establishes bases for PSA applications.

- In 2004 CSN has already issued the guide GS 1.15: “PSA Actualization and Maintenance”. In this guide CSN established the frequency and scope for the process which is linked with the use in PSA applications. As a minimum specific data analysis must be completed for each outage shutdown.

3. Numerical Safety Criteria

- 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.
- Nevertheless, since some PSA applications need of some kind of quantitative acceptance criteria or guidelines CSN issued de guide “GS 1.14 Basic criteria for carrying out PSA Applications”. In this guide some quantitative goals are established. These goals are based at US RG guide 1.174 “An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis”.

4. PSA Standards and Guidance

- There are not national standards in the area of PSA for performance. In the eighties and nineties the CSN review and PSAs development was done under CSN and Utilities collaboration, PSA scope was being increased at the same time that experience was doing. For the main PSA tasks (accident sequence delineation, human reliability analysis, CCF modelling, quantification, etc.) methodologies had been defined within the PSA projects. Several reference documents (NUREG, other previous PSAs, etc.) were considered for this purpose.
- Currently, new standard for fire PSA is being required, by CSN, for the PSA actualization which is required for the authorization renew.
- As it is said in the previous section there are specific guides for the actualization and maintenance process (GS 1.15) and for carrying out PSA applications (GS 1.14).
- In addition between years 2000 and 2005 several PSA applications projects were developed in which CSN and Utilities collaborated as a result of them specific applications guides were also developed.

5. Status and Scope of PSA Programmes

- The common scope established by the PSA Integrated Programme second edition for the Spanish NPP PSA was that of Level 1 and 2 analyses, including all reactor operating modes and fires and internal floods. As it was described in previous yearly reports, the original scopes of the plant specific PSA was progressively increased.
- In 2010 with the IS 25 Instruction, the global scope for PSAs was increased. This is a mandatory requirement for all Spanish NPP which are encouraged to perform: Level 1 and Level 2 PSA, including internal and external events, both at power operation and low power operation and shutdown, also taking into account other sources of radioactivity that might give rise to source terms similar to the reactor core, in particular the spent fuel pool.
- Currently, all NPP operators have programs in order to develop and complete these analyses in the next 4 -5 years. Common scope required by IS 25 will be Level 2 of internal events at low power and shutdown, Level 1 and Level 2 PSAs for fires and floods at low power and shutdown, and Level 2 PSA for fires and floods at Power.
- Current status can be summarised as follows:

Spanish nuclear fleet in operation currently comprises 6 sites and a total 8 units. Spanish nuclear power plants currently have Probabilistic Safety Assessments (PSAs), which are kept updated and whose scope includes:

Trillo Nuclear Power Plant (KWU-3 loops):

Level-1 PSA of internal events at power.
 Level-1 PSA of internal events at low power and shutdown.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Vandellós II Nuclear Power Plant (Westinghouse-3 loops):
 Level-1 PSA of internal events at power.
 Level-1 PSA of internal events at low power and shutdown.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Cofrentes Nuclear Power Plant (GE-BWR6).
 Level-1 PSA of internal events at power.
 Level-1 PSA of internal events in other operating modes.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Ascó Nuclear Power Plant (Westinghouse-3 loops, 2 units):
 Level-1 PSA of internal events at power.
 Level-1 PSA of internal events at low power and shutdown.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Almaraz Nuclear Power Plant (Westinghouse-3 loops, 2 units).
 Level-1 PSA of internal events at power.
 Level-1 PSA of internal events at low power and shutdown.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Santa María de Garoña Nuclear Power Plant (GE-BWR3):
 Level-1 PSA of internal events at power.
 Level-1 PSA of internal events at low power and shutdown.
 Level-1 PSA of internal flooding at power.
 Level-1 PSA of internal fires at power.
 Level-2 PSA of internal events at power.

Additionally, Almaraz, Trillo, Santa María de Garoña and Cofrentes have conducted probabilistic assessments of the spent fuel pool with the unit at shutdown conditions.

- At same time assessments of other external events (IPEEE Individual Plant Examinations for External Events) have been completed for all NPP. The IPEEE analyses are oriented towards the identification of plant vulnerabilities to external events. In accordance with the seismic margin methodologies applied (EPRI and US-NRC), the aim is to determine the seismic capacity of the plant known as the “high confidence of low probability of failure” (HCLPF): GL 88-20 SUP. 4 -> NUREG-1407 -> GL 88-20 SUP. 5
- Appendix A gives an overview of the time schedule of the different PSA projects.

6. PSA Methodology and Data

- For the level 1 PSA, the small event tree - large fault tree methodology (using fault tree linking) is used. All models are managed with the RiskSpectrum or CAFTA codes.
- Following methodologies are used in data analysis:
 - Initiating event frequencies: Some of them are generic (LOCA, SGTR. etc), specific events for the NPP are based in specific fault tree models (Lost of instrumentation air systems, ISLOCA, etc), plant specific data for frequent events (turbine trip, lost of outside power, etc.) and finally in some cases plant specific data are used for bayesian combination of generic and specific data when the feed back of experience is not sufficient to be used alone.
 - Unavailabilities of system components or trains (programmed or non-programmed) are based on plant operating experience.
 - Plant specific data failures are collected for the majority of components failures and they are used for estimation of component failure rates. In those cases where plant specific data are not sufficient to be used alone they are used for bayesian combination of generic and specific data. Very few component failure rates are based on a generic data base for Spanish NPP (it takes data mainly from NUREG/CR 6928).
 - The CCF-modelling is based on the Alpha factors and uses generic CCF-parameter data. However NPP analyze collated data looking for common cause failures.
- “Human reliability analyses in the Spanish NPPs are mainly based on SHARP methodology. These analyses have been conducted for internal events, covering at power and the other operational modes, and for external events (fires and floodings). So, pre and post initiating event human actions have been identified and modeled. Regarding quantification techniques, THERP for pre initiating event human actions (test, maintenance, calibrations, etc.), and a combination of THERP plus HCR (or THERP plus TRC) for post initiating event human actions have been used mainly. Dependency analyses are included. These methodologies have been complemented with some additional specific human reliability criteria and considerations as far as the PSA scope depart from an standard level 1 PSA for internal events at power. Some new methods are currently under consideration for human reliability in external events in order to better inform PSA applications”
- The level 2 Spanish PSA involves the three classical aspects: Interface, Containment Event Tree and Source Terms Calculation. The grouping done at the Interface incorporate the back end systems and enlarge the level 1 event trees when necessary. The Plant Damage States are identified by a short number of attributes, which includes the pressure in the Reactor Cooling System and plant systems status at the beginning of the core damage. Short Containment Event trees are used, being every point brunch the result of a Decomposition Event Tree (DET). The Source Term Analysis sets up the source term categories and identifies its representative scenarios. MAAP code is the system code used and the studies do not include uncertainties analysis. LERF is the result of the measure of the risk, which includes the frequencies of all the releases greater than 3% in iodines before 12 hours from the reactor trip.

7. PSA Applications

- In the origin of PSA Program one of the main goals was to develop PSA applications. In Spain, PSA insights are used for the Utilities and CSN for several activities, some examples of these are given below:
 - Design evaluation
 - Since first stages in PSA developments a big quantity of design modifications has been implemented. Modifications were directed to reduce the risk in the operation for NPPs and to enhance safety. PSAs have been consider as a useful tool to identify important contributions to the risk (core melt

and early radioactive release). At the same time PSAs are used as a part of the safety analysis in the framework of the periodic safety review.

- This use has been done not only by NPPs but also by CSN. In some cases CSN has required design modifications based on a high contribution to the risk.

- Risk Monitor

- All Spanish NPP use the risk monitor to manage maintenance activities under Maintenance Rule requirements during at power operation.

- During shutdown refuelling activities they use procedures that have developed to manage safety based in some cases in shutdown PSA models.

- PSA based event analysis

- CSN has the analysis of operational events by using PSA as a part integrated in the operational experience feedback process. CSN staff makes the determination of the quantitative importance of a few well-selected operational events per year.

- Ranking of safety critical components

- CSN has developed a Systematic Oversight Program for NPP based on USA reactor oversight process (ROP) for supervising activities. Some of the inspections are focused in the most risk significant components and inspection findings and categorized by their risk impact.

- Evaluation of Technical Specifications

- In 2011 CSN issued a new Technical Specification Instruction. In this Instruction new limited condition are required for risk significant components or systems. Currently NPP are adapting their Technical Specification to this new requirement. In 2006 Cofrentes NPP had already adopted this criterion, new operational conditions were included for equipment not previously required in Standard Technical Specifications (venting valves, fire pumps for injecting vessel in case of SBO etc).

- RI-ISI / RI-IST

- Some Spanish NPPs have performed these applications:

- Cofrentes NPP has implemented RI-ISI for class 1 and class 2 pipings and RI-IST for valves (motorized, air, solenoid and check) and motor pumps.

- Almaraz NPP has implemented RI-ISI for class 1 pipings.

- Ascó NPP has implemented RI-ISI for class 1 pipings and RI-IST for check valves.

-

- Use of PSA insights for training

- Spanish NPP are including the use of PSA insights for training purposes but there are not any CSN requirement to follow.

-

8. Results and Insights from the PSAs

- Some quantitative information on the currently Level 1 results is given in the following tables.

	Trillo NPP	Vadellós 2 NPP	Cofrentes NPP	Ascó I y II NPP	Almaraz I y II NPP	Garroña NPP
Contribution CDF L1 Power	8%	15%	43%	40%	12%	14%
Contribution CDF L1 L&S	62%	62%	22%	14%	14%	7%

Contribution CDF L1 Fire	25%	12%	11%	32%	53%	75%
Contribution CDF L1 flood	5%	11%	23%	15%	21%	4%

-
- The initiating events with highest CDF contribution are:
-

NPP	for power states	for non power and shutdown states
Trillo	LOCAs (40%), generic transients (36%), loss of auxiliary electricity supply or LOOP (16%)	Loss of auxiliary electricity supply with the primary system at 3/4 loop open (37.92%) and closed (19.48%), Residual Heat Removal (RHR) rupturing or leakage with the cavity full (13.83%) and rupturing or leakage outside containment with the Reactor Coolant System (RCS) at 3/4 loop open (11.37%)
Vandellós	Reactor and turbine trip (30.84%) and loss of off-site 400 kV feed (14.68%)	the main contributor to the risk of the facility being reduced vessel inventory situations (“half nozzle”)
Ascó I y II	Reactor and turbine trip (25.73%), small-break LOCA (18.31%), steam generator tube rupture (12.81%) and loss of main feedwater (10.42%)	Overpressurisation and loss of off-site power in operating mode 4 (hot shutdown) and overpressurisation and small-break LOCA in RHR in mode 5 (cold shutdown)
Almaraz I y II	Small-break LOCA's (22.29%) generic transients (19.59%), Interface LOCA's (11.30%) and Loss of the Component Cooling Water System (11.28%), SBO (7.99%)	Losses of the Residual Heat Removal System (RHR) due to failure of its support systems with the RCS partially filled, Loss of Off-Site Power with the RCS full and partially full, and losses of RCS inventory under reduced inventory conditions.
Cofrentes	ATWS (60.75%), followed by LOCA sequences (11.04%), SBO (10.87%) and transients (10.56%)	Reactor subcritical with vessel head in place in Operating Condition 4 (cold shutdown). Reactor subcritical with temperature below 100°C and vessel head in place in Operating Condition 4 (cold shutdown). Vessel head removed and water level higher than 7 meters above the vessel flange. Operating Condition 5 (refueling).

NPP	for power states	for non power and shutdown states
Sta. M ^a de Garoña	ATWS 47%, Transients including losses of off-site power and losses of service water (47%)	The highest contribution in this case (70%) is due to a scenario in which there are minor breaks in the recirculation lines or inventory losses as a result of maintenance activities with the cavity full and connected to the spent fuel pools

- For the level 2 PSA results are bellow:

NPP	Level 2 for power states
Trillo	The contribution is governed fundamentally by Steam Generator Tube Rupture scenarios, secondary pipes rupture and induced generator tube rupture and to a lesser extent, by scenarios Interface LOCA
Vandellós	Frequency of Major Releases (FMR): accidents involving off-site releases of volatiles amounting to more than 3% of the inventory of the core over the 24 hours following the start of the accident: The main contributors to the risk of the facility are sequences involving penetration of the foundation slab and rupturing of the containment as a result of overpressure
Ascó I y II	Frequency of Major Releases (FMR): The main contributors to the risk of the facility are sequences involving penetration of the foundation slab and interface LOCA's (containment bypass).
Almaraz I y II	The overall results obtained point to a frequency of major early releases from containment (LERF): accident with off-site volatile emissions exceeding 3% of the core inventory during the first 12 hours into the accident. The release categories that most contribute to this frequency are those associated with interface LOCA initiating events and, to a much lesser extent, those associated with containment isolation failures and early failures of the containment.
Cofrentes	Annual frequency of Major Early Releases (LERF): the most important contributors being early failure of the vessel and containment and bypassing of the Drywell (DW) and sequences involving containment bypass and early failure of the vessel and containment and DW bypass. Annual frequency of major releases (FMR): the major contributors being failure of the vessel with early failure of containment and delayed DW bypass, as well as those described previously for LERF.
Sta. M ^a de Garoña	The overall results obtained for the Frequency of Major Early Releases (LERF): This result comes from 7 sequences 4 ATWS, 3 Interface LOCA Major contributor Frequency of Major Releases (FMR)

9. Future Developments

- In 2010 CSN issued a new Instruction with the IS 25 Instruction, the global scope for PSAs was increased. This is a mandatory requirement for all Spanish NPP which are encouraged to perform: Level 1 and Level 2 PSA, including internal and external events, both at power operation and other modes of operation, also taking into account other sources of radioactivity that might give rise to source terms similar to the reactor core, in particular the spent fuel pool.
- Currently, all NPP operators have programs in order to develop and to complete these analyses in the next 4 -5 years.
 - Level 2 PSA for fires and floods at Power,
 - Level 2 of internal events at low power and shutdown,
 - Level 1 and Level 2 PSAs for fires and floods at low power and shutdown.
- PSA Insights are used as a part for de Safety Analysis in the Periodic Safe Review (PSR), in order to get updated results for de PSAs, a methodological review in some part of the PSAs is required. In this framework fire PSA for all Spanish NPP are being completed in accordance with NUREG/CR 6850 “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities”.

10. References

- [8] “Integrated Programme on Performance and Use of PSA in Spain” (IP). Ed. 1 (1986).
- [9] “Integrated Programme on Performance and Use of PSA in Spain” (IP). Ed.2 (1998).
- [10] Safety Instruction: “Criteria and requirements on the performance of probabilistic safety assessments and their applications for nuclear power plants”. IS-25 (2010).
- [11] Guía de Seguridad: GS 1.15. “Actualización y mantenimiento de los Análisis Probabilistas de Seguridad” (Safety Guide: PSA Actualization and Maintenance) (2004)
- [12] Guía de Seguridad: GS 1.14 "Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad" rev. 1. (2007) (Safety Guide: “Basic criteria for carrying out PSA Applications”.

Appendix B – Contact Information

Regulatory Authority Nuclear Safety Council CSN	Direct Contact
C./ Pedro Justo Dorado Dellmans 11 28400 Madrid Spain Tel: +34 91 346 01 00 Fax: +34 91 346 05 88 Website Address: www.csn.es	M ^a Teresa Vázquez Mateos Head of PSA Branch Nuclear Technology Department C./ Pedro Justo Dorado Dellmans nº 11 28400 Madrid Spain Tel: +34 91 346 02 60 Fax: +34 91 346 04 96 Email: tvm@csn.es

15. SWEDEN

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

During the 80ies and 90ies 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 weak 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.

3. Numerical safety criteria

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 good 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.

4. PSA standards and guidance

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 not 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.

5. Status and scope of PSA programs

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.

6. PSA methodology and data

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.

- 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 be treated, covered in the PSA models. CCF:s are treated in the Swedish 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 access to as wide and QA dependency and CCF data as possible.

Human reliability: Method descriptions exist 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 address: HE:s that can lead to faulty system configuration, 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 recent 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 themselves 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.

7. PSA applications

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.

8. Results and insights from the PSAs

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.

9. Future developments and research

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 be 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 adjoining 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 traditional 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 2004:1 regulation 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.

10. References

References – 2

1. Description of the regulatory framework in Sweden, the PSA environment, *The Nuclear Activities Act (1984:3)*, DOCSOPEN #10491 v1

References – 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 – 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].

Contact

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		

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 in 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 Probabilistic 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

16. SWITZERLAND

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Framework and Environment

Regulatory Framework:

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, today ENSI) required the utilities to perform full power Level 1 and Level 2 PSAs for all Swiss nuclear power plants. Four years later, the Inspectorate additionally required the licensees to develop plant-specific low power and shutdown PSAs, including external events.

PSAs for all Swiss nuclear power plants were developed by licensees and independently assessed by ENSI. 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 ENSI by the licensees.

After the initial phase of development and review, the implementation of a plant-specific “living PSA” was required, 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 Act and an accompanying ordinance were enacted in Switzerland. Since this ordinance requires a full-scope, plant-specific Level 1 and Level 2 PSA for all relevant operational modes, the low power and shutdown PSAs are currently extended to Level 2 and are reviewed by ENSI following submission by licensees. This work has been conducted for most of the Swiss NPPs.

Another major task was the update of the probabilistic seismic hazard analysis. The corresponding large-scale project PEGASOS (a German acronym for “Probabilistic Assessment of Seismic Hazards for Swiss Nuclear Power Plant Sites”) was carried out by Swiss licensees in response to a requirement that was issued by ENSI’s PSA review process. In order to achieve a thorough quantification of the uncertainty of seismic-hazard estimates, licensees conducted an extensive expert elicitation process involving individual technical experts, scientific institutions and engineering organisations from Europe and the USA. The project was conducted in full compliance with the Senior Seismic Hazard Analysis Committee (SSHAC) Level 4 methodology. The complete project report was released in 2006 at an OECD specialists’ meeting in Korea. A summary report in German can be downloaded from www.ensi.ch.

In 2008, Swiss licensees initiated a follow-up project, the “PEGASOS Refinement Project” (PRP). The project takes advantage of the most recent findings in earth sciences and new geological and geophysical investigations at Swiss NPP sites. A particular objective is to reduce the uncertainty range of the PEGASOS results. In 2009 the scope of the PRP was extended to include the sites for the proposed new Swiss NPPs. The Inspectorate is following the study closely through a system of continuous peer reviews similar to that for PEGASOS. In the PRP full compliance with the SSHAC Level 4 methodology is maintained.

Based on PEGASOS insights, ENSI has increased the seismic hazard levels to be used for plant-specific PSA studies. In response, the licensees invested considerable effort to update and refine their seismic

PSAs. Higher hazard levels are also used for the design of new safety-related structures and components. Furthermore, various structures and components have been seismically backfitted.

The ordinance also anchors a number of PSA applications in the law, including:

- For the construction permit of a new nuclear power plant (NPP), applicants need to demonstrate that the core damage frequency is below 10^{-5} per year. This risk criterion is also expected to be fulfilled by the existing plants, to the extent that is reasonably achievable.
- 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, ENSI follows an integrated regulatory safety oversight process. Plant-specific PSA insights are only one element of the integrated regulatory safety oversight process.

The ordinance introduced in February 2005 authorizes ENSI to issue the following PSA guidelines:

- Guideline ENSI-A05: PSA quality and scope
- Guideline ENSI-A06: PSA applications

These guidelines are available for download from <http://www.ensi.ch/index.php?id=146&L=2>.

Requirement for a PSA to Be Produced:

The initial applications of PSA focused 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.

Further applications are on the assessment of the risk impact of power uprate, the risk implication of accident management alternatives, and the risk implication of plant modifications (including changes to technical specifications). The identification of risk-significant components is used to complement the scope of the ageing surveillance programme as well as to complement the method for classifying the safety significance of a structure, system or component.

PSA is also used to assess the operational experience. On the one hand PSA is applied to assess every reportable event involving a PSA component. On the other hand the annual operational experience (including the impact of planned and unplanned maintenance) is analysed by two risk-based safety indicators.

Who Has Carried Out the PSAs:

The licensees conduct the PSA studies, which are then submitted to ENSI. 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 20 years. As a part of this periodic review process, ENSI has developed independent plant-specific regulatory PSA models. These regulatory PSA models enable ENSI to perform independent confirmatory analyses, and to assess the risk implication of various safety issues and regulatory actions.

3. Numerical Safety Criteria

The nuclear ordinance, the ordinance on “hazard assumptions and evaluation of protection measures against accidents in nuclear installations,” and in particular the regulatory guideline ENSI-A06 define risk criteria in the following areas:

- Probabilistic evaluation of the safety level
- Evaluation of the balance of the risk contribution
- Probabilistic evaluation of the technical specification

- Probabilistic evaluation of change to structures and systems
- Risk signification of components
- Probabilistic evaluation of operational experience

Details can be found in the regulatory guideline ENSI-A06 electronically available at: <http://www.ensi.ch/index.php?id=146&L=2>

4. PSA Standards and Guidance

The nuclear ordinance introduced in February 2005 requires a full-scope, plant-specific Level 1 and Level 2 PSA for all relevant operational modes. It also anchors a number of PSA applications in the law.

Furthermore, the ordinance authorized ENSI to issue the following PSA guidelines:

- Guideline ENSI-A05: PSA quality and scope
- Guideline ENSI-A06: PSA applications

These guidelines are electronically available for download at: <http://www.ensi.ch/index.php?id=146&L=2>

5. Status and Scope of PSA Programmes

Historical Development:

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, today ENSI) required the utilities to perform full power Level 1 and Level 2 PSAs for all Swiss nuclear power plants. Four years later, the Inspectorate additionally required the licensees to develop plant-specific low power and shutdown PSAs, including external events.

PSAs for all Swiss nuclear power plants were developed by licensees and independently assessed by ENSI. 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 low-power and 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 ENSI by the licensees.

After the initial phase of development and review, the implementation of plant-specific “living PSA” was required, 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 Act and an accompanying ordinance were enacted in Switzerland. Since this ordinance requires a full-scope, plant-specific Level 1 and Level 2 PSA for all relevant operational modes, the low power and shutdown PSAs are currently extended to Level 2 and are reviewed by ENSI following submission by licensees. This work has been conducted for most of the Swiss NPPs.

Another major task was the update of the probabilistic seismic hazard analysis. The corresponding large-scale project PEGASOS (a German acronym for “Probabilistic Assessment of Seismic Hazards for Swiss Nuclear Power Plant Sites”) was carried out by Swiss licensees in response to a requirement that was issued by ENSI’s PSA review process. In order to achieve a thorough quantification of the uncertainty of seismic-hazard estimates, licensees conducted an extensive expert elicitation process involving individual technical experts, scientific institutions and engineering organisations from Europe and the USA. The project was conducted in full compliance with the Senior Seismic Hazard Analysis Committee (SSHAC) Level 4 methodology. The complete project report was released in 2006 at an OECD specialists’ meeting in Korea. A summary report in German can be downloaded from www.ensi.ch.

In 2008, Swiss licensees initiated a follow-up project, the “PEGASOS Refinement Project” (PRP). The project takes advantage of the most recent findings in earth sciences and new geological and geophysical investigations at Swiss NPP sites. A particular objective is to reduce the uncertainty range of the PEGASOS results. In 2009 the scope of the PRP was extended to include the sites for the proposed new Swiss NPPs. The Inspectorate is following the study closely through a system of continuous peer reviews similar to that for PEGASOS. In the PRP full compliance with the SSHAC Level 4 methodology is maintained.

Based on PEGASOS insights, ENSI has increased the seismic hazard levels to be used for plant-specific PSA studies. In response, the licensees invested considerable effort to update and refine their seismic PSAs. Higher hazard levels are also used for the design of new safety-related structures and components. Furthermore, various structures and components have been seismically backfitted.

Level of PSA:

The nuclear ordinance introduced in February 2005 requires a full-scope, plant-specific Level 1 and Level 2 PSA for all relevant operational modes. All Swiss licensee PSAs are full-scope Level 1 and Level 2 studies for full power operation. Low-power and shutdown Level 2 has been performed by most of the plants. 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, 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 (which is conducted at least 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.

6. PSA Methodology and Data

The requirements on the quality and scope of the PSA are defined in the regulatory guideline ENSI-A05.

Overall Methodology:

In Switzerland, the linked event tree as well as the linked fault tree methodology have been used for Level 1 PSA. Both methods are 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 in Switzerland.

Common Cause Failure (CCF):

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 (HRA):

Pre-initiator Human Errors (HEs) (category A actions), HEs causing initiating events (category B actions) as well as post-initiator HEs (category C actions) are 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 ENSI, THERP (technique for human error prediction), and ASEP (accident sequence evaluation program). 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.

7. PSA Applications

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. The main requirements on the PSA applications are described the regulatory guideline ENSI-A06.

Probabilistic Evaluation of the Safety Level

An important application of the PSA is the evaluation of the safety level and the identification of potential plant-specific vulnerabilities. Corresponding evaluation criteria are given in the regulatory guideline ENSI-A06. This evaluation is performed 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 8.

Evaluation of the Balance of the Risk Contribution

The balance among the risk contributions from initiating event categories, accident sequences, components and human actions shall be evaluated. If any of the initiating event category accident sequences, components or human actions are found by PSA to have a remarkably high contribution, measures to reduce the risk shall be identified and – to the extent appropriate – implemented. The regulatory guideline ENSI-A06 provides criteria for the evaluation of the balance of the risk contribution of the various initiating event categories.

Contribution to the Design Criteria for External Hazards

According to the Ordinance on "Hazard Assumptions and Evaluation of Protection Measures against Accidents in Nuclear Installations," the plant shall be designed against natural hazards such as earthquakes,

flooding and extreme weather conditions. In particular, sufficient protection against natural hazards with a frequency greater than or equal to $1\text{E-}4$ per year shall be demonstrated. The corresponding hazard curves are taken from the PSA.

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, 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.

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, ENSI 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, ENSI 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-year²²).

Risk-significant Components

A component is regarded as significant to safety from the PSA point of view if the following – in terms of CDF (core damage frequency) or FDF (fuel damage frequency) or LERF (large early release frequency) – applies:

$$FV \geq 1\text{E-}3 \text{ or } RAW \geq 2$$

where FV is the Fussell-Vesely and RAW the Risk Achievement Worth importance. Further instructions on the computation of the criteria are given in the regulatory guideline ENSI-A06. Components identified to be significant to safety from the PSA point of view

- shall be included into the ageing surveillance programme,
- need an approval by the Inspectorate in case such a component is modified, and
- shall be at least classified into safety class 4 (and correspondingly for electrical components).

²² Excluding earthquakes.

Probabilistic Evaluation of Plant Modifications

The impact of a plant modification on the risk shall be assessed. This applies to all PSA-relevant structural or system-related plant modifications as well as to changes of the technical specification involving PSA-relevant components. Criteria are given in the regulatory guideline ENSI-A06.

Evaluation of Technical Specifications

In defining the allowed outage times, it shall be ensured that components shown to be significant to safety from the PSA point of view (see above) are considered in the technical specifications (completeness), and assigned to correspondingly short allowed outage time categories (balance). Based on the risk measures CDF and LERF, it is foreseen to conduct a review of the completeness and the balance of the allowed outage times shall be carried out in the course of the periodic safety review.

In addition to the deterministic requirements for the maintenance of components, the following probabilistic requirements shall be satisfied during power operation:

- Maintenance work shall be planned in such a way that a) no component unavailability configuration resulting from maintenance will result in a Conditional Core Damage Frequency (CCDF) greater than $1E-4$ per year, and b) the total planned cumulative maintenance time for components shall be limited such that the portion of the Incremental Cumulative Core Damage Probability (ICumCDP) resulting from maintenance is less than $5E-7$.
- Compliance with the above mentioned requirements shall be demonstrated either by a previous enveloping analysis along with an additional probabilistic evaluation of operational experience or assessed with the help of a risk monitor. Any deviations from the requirements on maintenance planning mentioned above shall be justified.

Assessment of the Operational Experience

The operational experience is assessed by the PSA in two ways.

- *Annual Evaluation of Operational Experience*: At the beginning of every year, the licensees submit to ENSI a probabilistic evaluation of the operational experience of the previous year. In this study initiating events as well as component unavailabilities due to planned or unplanned maintenance or tests are considered. The study involves among other things the determination of the probabilistic safety indicators (the maximum annual risk peak and the incremental cumulative core damage probability) and the risk contribution of the online maintenance. ENSI incorporates all the data into a databank in order to review the study.
- *Event Analysis*: PSA is one element in the integrated decision-making. Therefore, PSA is also used to classify reportable events (provided the event affects a PSA-relevant structure, system, component or operator action). Since ENSI classifies all reportable events by the INES-Scale, regulatory guideline ENSI-A06 provides a relationship between the cumulative conditional risk of an event and the INES-Scale.

8. Results and Insights from the PSAs

PSA-based modifications and backfits have often been introduced in the Swiss nuclear power plants and are listed below.

Beznau Plant

Backfits of 1980s:

Beznau I and II are Westinghouse PWRs. They have been 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 during the late 1980s 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 total CDF of the plant was reduced by about a factor of two by these cost effective measures.

Optimization of a large backfitting project by using PSA results:

During the late 1970's, the HSK (today ENSI) required that the Beznau plant be upgraded to meet more recent safety standards. The aim of the backfit called NANO ("Nachrüsten Notstandssysteme") 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 in 1992/93, 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.

Backfits of late 1990s:

The Beznau PSA was also used to evaluate the optimal configuration for the feedwater upgrade project installed in 1999. This investigation resulted in the decision to install one additional emergency feedwater train.

In addition, a new fourth battery train was implemented as part of the project to replace the Reactor Protection System (RPS).

Backfits after 2000:

Passive autocatalytic recombiners have been installed in order to minimize the risk of a containment failure due to hydrogen explosions during a severe accident

After a seismic walkdown of the Inspectorate, additional measures to improve the anchorage of electrical cabinets and mechanical equipment were performed after 2000.

Based on PEGASOS insights, the Inspectorate increased the seismic hazard levels to be assumed for the PSA studies. In response, the licensee put a lot of effort into the updating and refinement of its seismic PSAs. Based on recent PSA results, the licensee identified risk-effective seismic backfits that are currently implemented, especially in the area of containment isolation. These improvements will notably reduce the LERF.

Optimization of new EPS Configuration:

The Beznau PSA was also used to evaluate the planned reconfiguration of the emergency electrical power system. In the related project, called AUTANOVE (“Autarke Notstromversorgung”), the emergency power supply from the hydro plant will be replaced by newly installed diesel powered systems. Each unit will receive two new diesels generators that are fully redundant and located in separate buildings. The new systems will be protected against external events including earthquakes. PSA calculations show that the new configuration will significantly reduce the CDF.

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 (today ENSI) 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.

Based on PEGASOS insights, the ENSI increased the seismic hazard levels to be assumed for the PSA studies. In response, licensee invested considerable resources in updating and refining its seismic PSA. Using PSA, the licensee identified and implemented a seismic back-fit in the 380-V switchgear.

Leibstadt Plant

Leibstadt nuclear power plant is a General Electric BWR/6 with a Mark III containment. The plant has an additional bunkered 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 the water level in the reactor pressure vessel 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. On the other hand, lowering RPV water level is desirable following the postulated ATWS because the low water level reduces power generation. It is therefore important to inhibit opening of the ADS Safety Relief Valves and initiate a feedwater runback 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 line-up of geodetic reservoir water) and the manual opening of SRVs.
- KKL developed a new concept aiming at improving – in case of earthquake – the automatic shut-off of the containment drain lines leading out of the containment. As an effective and easy-to-implement action, KKL identified the back-fitting of the shut-off through a battery-powered electric motor. As an interim solution, an administrative measure was introduced to manually close the drain lines.
- In order to sustain in station blackout scenarios the long-term DC power supply required to maintain the operation of gravity-driven or steam-driven core cooling, KKL has acquired a mobile emergency diesel generator to be aligned by the operators according to accident management procedures. Since the annual revision 2010, the emergency diesel generator has been able to feed the related electrical divisions through a temporary connection. The final connection will be made during the annual revision 2011.

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 relief 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.

Based on PEGASOS insights, ENSI increased the seismic hazard levels to be assumed for the PSA studies. In response, licensee invested considerable resources in updating and refining its seismic PSAs. Based on the recent PSA results, the licensee identified risk-effective seismic backfits that are currently implemented.

9. Future Developments and Research

The main development of the PSA is currently the extension of Level 2 PSA to low-power and shutdown operation. This work will be completed in the next years. Furthermore, ENSI focuses on the harmonization of the PSAs in order to make the PSA results more comparable. The various research projects are aiming to reduce the uncertainty in some selected fields.

Switzerland supports research and development in the following fields:

- *Data Collection*: ENSI 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).
- *Human Reliability Analysis (HRA)*: ENSI supports 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 (EOCs). 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 previous work, PSI developed the CESA method for EOC identification and performed a pilot application. CESA has been used so far to identify potential EOC opportunities for two Swiss NPPs.

Furthermore, the development of guidance on the application of simulator data for HRA methods and the collection data of seismic events relevant for seismic HRA is envisaged.

- *Severe Accidents*: ENSI 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 ENSI supports the international OECD project on Melt Coolability and Concrete Interaction (MCCI). This project provided 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; e.g. ablation rates for two different concrete types were obtained and the successful ex-vessel cooling of the molten debris in case of early containment flooding has been demonstrated in one large-scale experiment.

MELCOR – Air Oxidation Modelling: ENSI supports the development of a new MELCOR model at the Paul Scherrer Institute (PSI). The computer program models the oxidation process of fuel elements in case of air ingress during severe accident scenarios. It will help to calculate the consequences, i.e. release of fission products within the framework of PSA Level 2 studies, more accurate. The advanced model considers also new future cladding materials.

- *ADAM System*: A much faster than real-time accident diagnostics and prognostics system has been developed by Energy Research, Inc. (ERI) for ENSI and has been implemented at the ENSI 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.

In addition a source term program for application to emergency conditions has been added to ADAM (STEP module). This module can be used to predict the radiological release fractions in case of a severe accident.

17. SLOVAK REPUBLIC

1. Introduction

Here, no contribution is expected from the participants.

2. PSA Environment

The Slovak Republic has four units equipped with WWER440/213 type reactors in operation. At the nuclear site of J. Bohunice there are three nuclear power plants: A1, V1 and V2 plant. The A1 plant, equipped with a heavy water moderated and gas cooled reactor is shutdown, its operation was terminated after a severe accident. The plant is under decommissioning from 1979. Two units with WWER440/V230 type reactors in the V1 plant are also shutdown; operation of the unit 1 was terminated in 2006 and operation of the unit 2 was terminated in 2008. Two units (unit 3 and 4) with WWER440/V213 type reactors are in operation in the V2 plant. At the Mochovce nuclear site two units (unit 1 and 2) with WWER440/V213 type reactors are in operation and another two units (unit 3 and 4) are under construction. They will be given into operation in 2013.

The plant 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 SR) as the 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 fulfil an important role in this process because they 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.

The regulatory authority issued a guidance for requirements for PSA studies (BNS I.4.2/2006). The guidance is not intended to be a procedural guide for performing a PSA. Such procedures have been developed by IAEA and other organizations. This guideline is intended to define the requirement for PSA and supporting documentation. Thereby, providing a more useful and effective tool for operational and regulatory safety enhancement.

UJD SR requires performing the internal event level 1 and level 2 PSA study (including internal fires and floods) for full power operation, low power operation and shutdown operating modes for any nuclear power plant on the site. In addition, external hazards (as seismic event, extreme meteorological conditions, aircraft crash, impact of neighbouring industry, etc.) must be incorporated into 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 SR requires a 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 plant are performed by RELKO Ltd. and VÚJE, Inc. UJD SR performs review of the PSA studies. In addition, IPSART type review is performed by the experts of IAEA.

3. Quantitative Safety Goals

PSA acceptance criteria are defined 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 $1.0E-3$. In case of reactor protection system the failure probability is unacceptable if it is higher than $1.0E-5$.

The baseline values of CDF and LERF are calculated from PSA models. The safety goal for plants in operation is $CDF \leq 1.0E-4/y$ resp. $LERF \leq 1.0E-5/y$. The safety goal for new plants is $CDF \leq 1.0E-5/y$ resp. $LERF \leq 1.0E-6/y$.

The changes in CDF are considered non-risk significant if the changes:

- in CDF are less than $1.0E-4/y$ and their cumulative effect do not cause the safety goals to be exceeded; changes in the CDF greater than $1.0E-4/y$ are considered unacceptable,
- in LERF are less than $1.0E-5/y$ and their cumulative effect do not cause the safety goals to be exceeded; changes in the LERF greater than $1.0E-5/y$ are considered unacceptable.

4. Status of PSA Programmes

The status of PSA for the Slovak operating plants is as follows:

- The J. Bohunice V2 NPP: Level 1 and level 2 full power, low power and shutdown PSA is performed for the plant.
- The Mochovce NPP: Level 1 and level 2 full power, low power and shutdown PSA is performed for the plant.

In addition, PSA is used to support:

- the decommissioning of the A1 and V1 plants on J. Bohunice site,
- construction of the unit 3 and 4 on the Mochovce site.

5. PSA Applications

Based on the PSA model of the plants the risk monitors are developed, precursor analyses are performed, plant modifications are supported and other PSA applications are performed.

The risk monitors

The status of risk monitors for the Slovak plants is as follows:

The J. Bohunice V2 NPP: Level 1 and level 2 full power, low power and shutdown EOOS (Equipment Out Of Service) risk monitor is developed to monitor the CDF and LERF. The monitor is used to evaluate the risk profile for the plant in operation and for preventive maintenance planning.

The Mochovce NPP: Level 1 and Level 2 full power, low power and shutdown SM (Safety Monitor) monitor is developed to monitor the CDF and LERF. The monitor is used to evaluate the risk profile of the plant in operation and for preventive maintenance planning.

Precursor analyses

The precursor analyses are carried out on the safety significant events that occurred at the plants using the PSA model. The objective of the analyses is to get quantitative measure of risk importance of the events. The results from precursor analyses are also used to prioritize areas for safety improvement and to support the regulatory work.

Improvement plant safety

Modernization of the J. Bohunice V2 plant was performed during the last years. The PSA provided strong support in the following areas:

- Identification of the systems, components, initiating events and accident sequences which are the most important from the risk point of view.
- Prioritisation of the safety upgrading measures.
- Evaluation of alternative proposals for the upgrading.
- Evaluation of the proposed design changes for the systems.
- Support for the designers to achieve the probabilistic goals.
- Identification of additional possibilities to decrease the risk.
- Saving investment.

Other applications:

- optimization of the technical specification,
- implementation of the reliability centred maintenance,
- in service inspection, etc.
-

6. PSA Related Research and Development

The PSA studies were updated for the plants after power uprate to 107% of the nominal power (uprated power of the unit by 7% of nominal power, i.e. $1\,375\text{ MW} \times 1.07 = 1\,471.3\text{ MW}$). Power uprates of the plants are a way to increase generating capacity in an economical way. The risk increase in the form of CDF and LERF is negligible, less than 1%.

In the future more enriched uranium fuel will be used in the reactors of the plant. It will require the PSA update of the plants due to the changed core inventory.

High cost of long outages caused that preventive maintenance activities during refuelling were changed in the plants of EU and US to on-line maintenance during the plant full power operation. The preventive maintenance of all safety systems of WWER440/213 units is performed during shutdown for refuelling. However, on-line preventive maintenance is planned for the future. It reduces the duration of annual overhaul but leads to small risk increase. PSA will be used to evaluate and minimise the risk deriving from on-line preventive maintenance. For this purpose the methodology will be developed in the future and it will be applied for the plants.

Z. Kovács, RELKO Ltd

J. Husárček, UJD SR

18. SLOVENIA

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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 guidelines.
- to perform PSA level 2 analyses on the basis of IAEA and US NRC 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 performed 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 performed 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.

In 2009 the new regulation was adopted which also explicitly addresses the PSA. It includes and determines PSA scope, quality and applicability. It also gives principles, commitments, requests and conditions for using PSA. Also the criteria for assessment of changes, uncertainty assessment, reporting requests and on-line maintenance requirements are included.

3. Numerical safety criteria

In Slovenia the numerical safety criteria is set by the regulation which sets the design and operation requirements.

The design of a NPP must assure that the total core damage frequency (CDF) including all internal and external events, for all modes of operation is less than $1 \cdot 10^{-5}$ per year and that the total large early release frequency (LERF) including all internal and external events, for all modes of operation must be less than $1 \cdot 10^{-6}$ per year.

In the case that the core damage frequency is less than 10^{-5} per year but more than 10^{-6} per year or the large release frequency is less than 10^{-6} per year but more than 10^{-7} , the investor or facility operator shall provide substantiated proof that any further reduction of the level of frequency is either impossible or not reasonable.

For the existing NPP Krško these numbers are $1 \cdot 10^{-4}$ and $5 \cdot 10^{-6}$ per year respectively.

The plant can use the PSA for the on-line maintenance (OLM) planning. The risk due to OLM must be assessed before and after the implementation of maintenance. The limits for risk increase are $5 \cdot 10^{-7}$ for CDF and $1 \cdot 10^{-8}$ for LERF per year. Likewise the risk of any configuration due to maintenance of the plant must be lower than $1 \cdot 10^{-4}$. Again, these numbers are lower for the existing plant, i.e. $4 \cdot 10^{-6}$, $2 \cdot 10^{-7}$ and $1 \cdot 10^{-3}$ respectively.

In general the changes that would increase the risk are not allowed, except when the benefits would substantially surpass the increase in risk. Still the limits for the increase in risk are $5 \cdot 10^{-7}$ for CDF and $1 \cdot 10^{-8}$ for LERF per year. For the existing NPP these numbers are $1 \cdot 10^{-6}$ and $1 \cdot 10^{-7}$ per year respectively.

4. PSA standards and guidance

The scope and the quality of the PSA in general are set by the new regulation. Except for the regulation there are no other national standards or guidance. It is expected that the PSAs are done in accordance with international standards and best practice.

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.

5. Status and scope of PSA programs

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 performed 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. The last update also includes the risk

evaluations due to high energy line breaks (HELB), which includes steam generator blow down break and chemical and volume control system letdown line break.

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 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.

6. PSA methodology and data

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 unavailability.

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 modeled 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 modeling of CCFs were distinguished:

- The modeling 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 CCFs 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-modeling of the existing CCF representation in the Krško NPP baseline PSA was performed by employing (RiskSpectrum) built-in CCF modeling capabilities. The focus of the work done was on re-modeling 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-modeling 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, modeling 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 modeled 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.

7. PSA applications

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 a 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 Paragon (before 2007 it was ORAM), 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;
- Performance indicators – Mitigating Systems Performance Index (NEI 99-02 Appendix G, MSPI Basis Document Development).

Applications at the SNSA

The SNSA uses PSA for its applications such as plant systems configuration impact on safety, plant vulnerabilities evaluations, etc. The most important application is a PSA based event analysis. The SNSA developed a procedure for event analysis. The main goal of evaluation and assessment regarding operational events is:

- identification of safety issues, appearing during the Krško NPP operation with intent to maintain and upgrade nuclear safety,
- allocation of acceptable solutions regarding unresolved safety issues,
- 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),
- upgrade of 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.

The SNSA also uses PSA for planning of plant outage oversight, for assessment of inspection findings and for performance indicators trending.

8. Results and insights from the PSAs

Results and insights are based on the valid NEK PSA model “NEKC22L2” and 2004 seismic PSA are given.

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 CDF and LERF for the valid NEK PSA model

Initiator Category	CDF [1/rcryr]	LERF [1/rcryr]
Internal initiating events	3.21E-5	8.07E-7
Seismic events	2.50E-5	1.53E-6
Internal fires	1.28E-5	2.77E-8
Internal floods	5.61E-6	6.67E-11
HELB	1,97E-6	2,29E-5
Other external events	6.50E-6	1.35E-7
Total	8.96E-5	2.50E-6

In Table 2 and Figure 1 the release categories and their frequencies are given. Note that LERF is calculated as the sum of release categories number 6 to 8.

Table 2: The release categories and their frequencies

RC no.	Release Category Definition	Release frequency [1/yr]
1	Core recovered in-vessel, no containment failure	0
2	No containment failure	1,34E-05
3A	Late containment failure, no molten core-concrete attack	1,14E-06
3B	Late containment failure, molten core-concrete attack	2,23E-05
4	Basemat penetration (no overpressure failure)	2,63E-06
5A	Intermediate containment failure, no molten core-concrete attack	2,77E-05
5B	Intermediate containment failure, molten core-concrete attack	5,53E-07
6	Early containment failure	4,90E-08
7A	Isolation failure, no molten core-concrete attack	7,44E-08
7B	Isolation failure, molten core-concrete attack	6,18E-08
8A	Bypass, scrubbed	6,53E-08
8B	Bypass, unscrubbed	1,60E-06

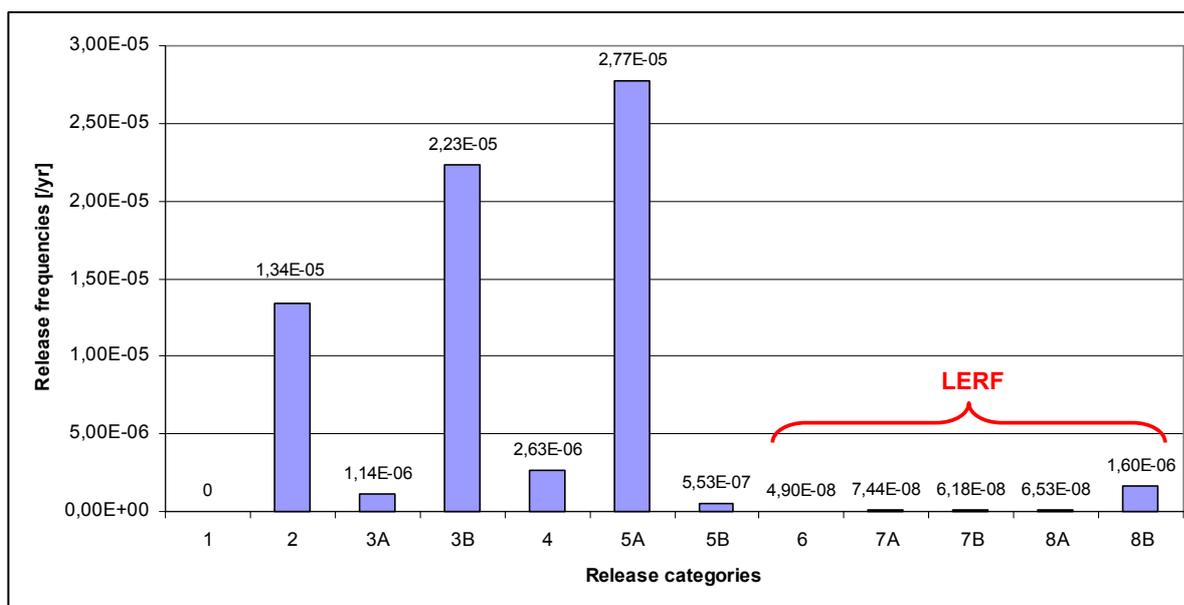


Figure 1: The distribution of releases by release categories and their frequencies

Important sequences

The event trees representing the plant response to Internal Initiating Events in the Baseline of the Krško NPP PSA Model “NEKC22L2” contain 176 event sequences that lead to core damage. The most important sequences are: Loss of Offsite Power ($3.34 \cdot 10^{-6}$ /rcryr), Station Blackout ($3.08 \cdot 10^{-6}$ /rcryr), Transient without MFW Available ($2.47 \cdot 10^{-6}$ /rcryr), Medium Loss of Coolant Accident ($1.93 \cdot 10^{-6}$ /rcryr). There are 9 sequences, which have frequency above the value of 10^{-6} /rcryr. They contribute roughly 53% to the IIE CDF.

Important Internal Initiating Events

The internal initiating events (IIE) in the Krško NPP baseline PSA Model contain 16 IIE categories. A group of the three most important single initiators is comprised of initiators categories Station Blackout (SBO), Loss of Component Cooling (CCW) and Loss of Offsite Power (LSP). These three categories contribute cumulatively somewhat more than 58% 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), as well as the emergency diesel generators.

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 $1 \cdot 10^{-10}/\text{rcryr}$ 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 performed 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 uncover 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 performed 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 Annunciator;
 - 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.

9. Future developments and research

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:

- Incorporation of complete PSA Level 2 into RiskSpectrum,
- next year a third diesel generator will be installed; this will also be reflected in the NEK PSA,
- the plant is following the developments of new fire PSA standards (NFPA standards), as well as shutdown PSA standards, so new studies are possible in these areas,
- plant data update.

At the SNSA

The SNSA has developed a set of Safety Indicators. These are 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.

10. References

- [1] Evaluation of New RS PSAP NEK Baseline Model “NEKC22”, NEK ESD-TR-15/08, Rev. 0
- [2] Implementation of Level 2 PSA for Internal Events Into RS PSAP Model, NEK ESD-TR-08/09, Rev. 0
- [3] 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] NEK Paragon Model NEK2007, NEK ESD-TR-03/07, Rev. 0
- [5] Seismic Probabilistic Safety Assessment of Krško Nuclear Power Plant, Level 1 and Level 2, SPSA-ABS-NEK-2004-003 Rev. 2, 2004.
- [6] Probabilistic Safety Assessment of Nuclear Power Plant Krško Level 1 Report, Volume 1, January 1994.

Appendix B – Contact Information

Ministry of the Environment and Spatial Planning	Železna cesta 16
Slovenian Nuclear Safety Administration	P.O. Box: 5759
Djordje Vojnovič	SI-1001 Ljubljana
	SLOVENIA
	e-mail: Djordje.Vojnovic@gov.si
	webpage: www.ursjv.gov.si

19. THE NETHERLANDS

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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 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 Sciencetech 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

3. Numerical safety criteria

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:

<i>Frequency of event (per year)</i>	<i>Effective dose (H_{eff}, 50 years)</i>	
	<i>Adult</i>	<i>Child (1 year old)</i>
$F \geq 10^{-1}$	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, 2006-2007 session, 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 $<2\%$.
- ²The 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 5×10^{-8} for Δ TCDF x AOT and Δ TCDF always $<10^{-4}$ /year.

4. PSA standards and guidance

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.

5. Status and scope of PSA programs

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)

6. PSA methodology and data

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 Bayesian 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 U₃Al_x fuel (High Enriched Uranium) respectively U₃Si₂ fuel (Low Enriched Uranium).

7. PSA applications

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 5.6×10^{-5} /year to 2.8×10^{-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 = $1 \times 10^{-2} ((1 + 10^{-2})/2) = 5 \times 10^{-3}$.

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 = 1.1×10^{-6} /year

CDF Power POS + TE unavailable = 1.6×10^{-6} /year

CDF Power POS + alternate pump with 10 times higher failure rate = 1.15×10^{-6} /year

CDF cold shutdown POS = 1.0×10^{-5}

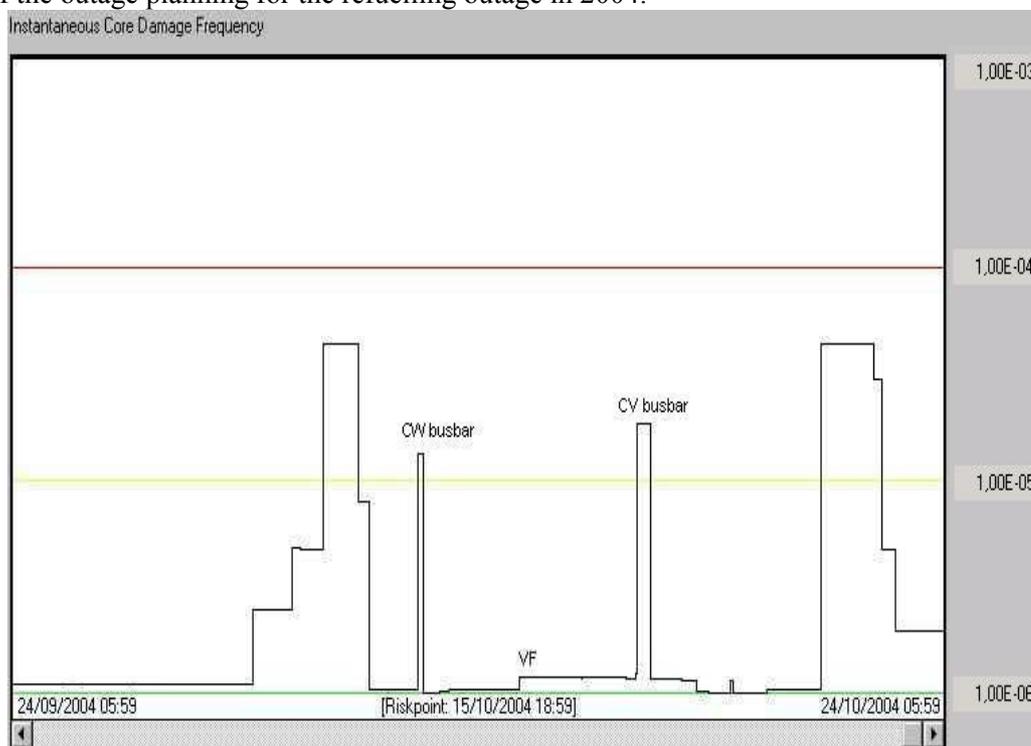
CDF cold shutdown + alternate pump with 10 times higher failure rate = 9.9×10^{-6} /year

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 MAAAP4 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 1×10^{-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 5×10^{-8} for $\Delta\text{TCDF} \times \text{AOT}$ and ΔTCDF shall always $< 1 \times 10^{-4}$ /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 serious 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 significantly larger. Therefore, a more realistic and Borssele Specific source term will be developed.

8. Results and insights from the PSAs

Borssele

Level 1 results:

TCDF all Plant Operating States = $2.65 \text{ E-}6$ /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 uncover 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 uncover occurs at 4 hours. In late phases (after refuelling), core uncover 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%):

- Fire: 1.9 E-5/year (27%)
- Large LOCA outside pool on pressure side of pumps: 1.8 E-5/year (26%)
- Drop of heavy load above spent fuel pool, thereby damaging primary piping below pool: 8E-5/year (26%)
- 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.

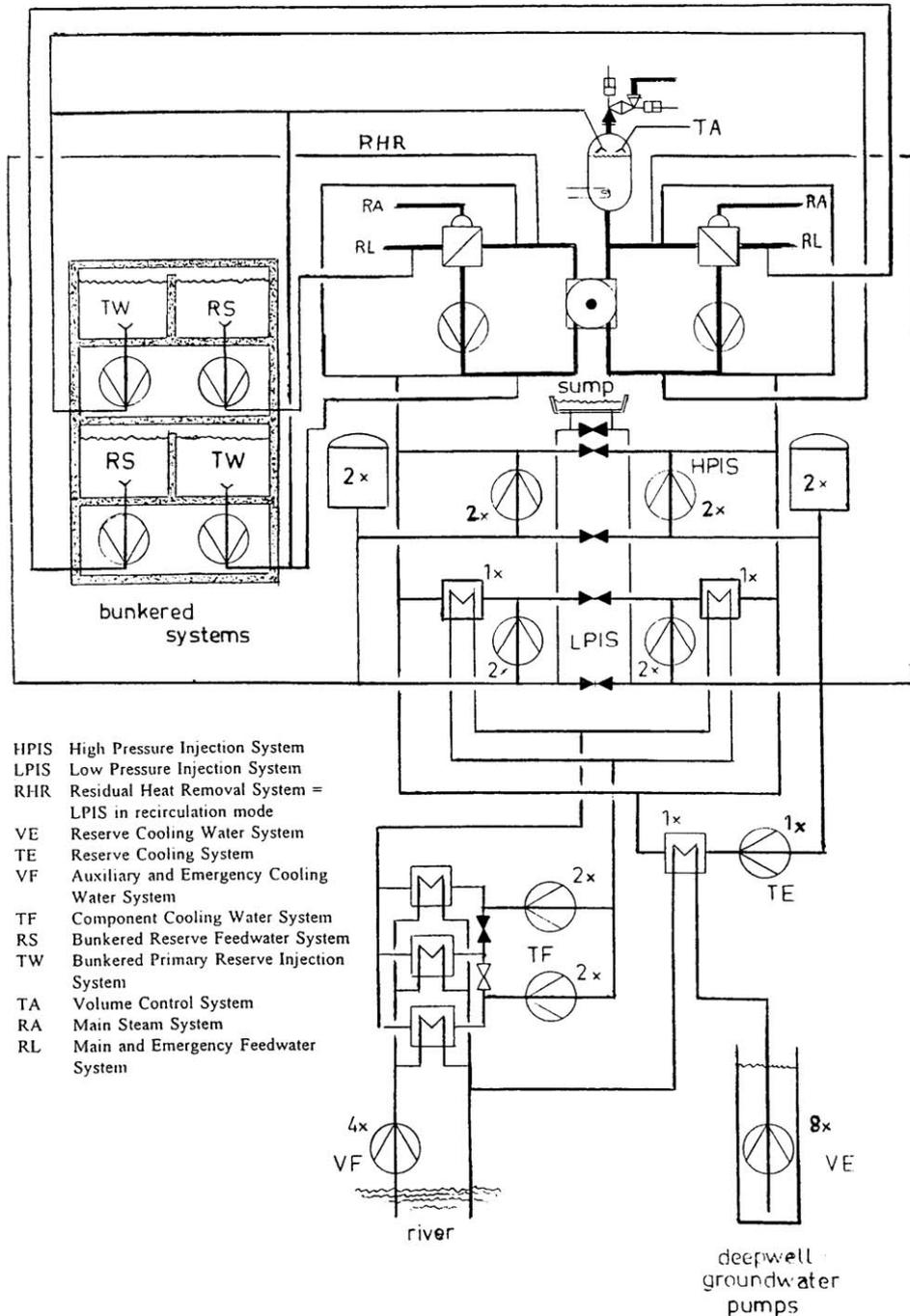
After several modifications (e.g., installation of additional vacuum breakers on the primary system to avoid that the core would be emptied due to the siphon effect, as well as limitation of portal crane movement above the pool during power operation) the CDF changed from 6.9 E-5/year to 2.4 E-6/year:

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

- Fire: 1.2 E-6/year (49%)
- Medium LOCA outside pool in inlet: 3.1 E-7/year (13%)
- Medium LOCA outside pool in outlet: 3.1 E7/year (13%)
- Loss Of Offsite Power: 2.6 E-7/year



○ (11%)

9. Future developments and research

As described in chapter 2 the development taking place is in the field of a transition towards Risk Informed Regulation. There are 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).

10. References

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, 2006-2007 session, 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 Decisions 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.

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
---	--

20. UNITED KINGDOM

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

2.1 PSA in the UK - Background

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 numerical safety criteria.

Probabilistic techniques and numerical safety criteria 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 Reviews (PSRs) which are now carried out every 10 years for all nuclear facilities. One of the requirements of the regulatory body, the Office for Nuclear Regulation (ONR)²³ is that the PSR includes a plant specific PSA.

Currently Generic Design Assessments (GDA) are being carried out by the regulatory organizations in the UK for new reactor designs that might be introduced into the UK – namely the AP1000 designed by Westinghouse and the EPR designed by AREVA. The GDA process allows the safety, security and environmental implications of new nuclear power plant designs to be assessed before an application is made for the permissions required to build that design at a particular site.

²³ The Office for Nuclear Regulation (ONR) is an Agency of the UK’s Health and Safety Executive (HSE) and was formerly known as the Nuclear Installations Inspectorate (NII).

If the design is judged to be satisfactory, a Design Acceptance Confirmation will be issued. Any remaining nuclear safety concerns or shortfalls in the information provided will be identified in the form of exclusions or caveats and these will be addressed when an application has been made for a nuclear site licence.

The GDA process includes an assessment of the PSA which is carried out by ONR. Step 3 of the GDA has been to: reviewed the methods, techniques and scope of the PSA; carry out some in-depth spot checks of the models and data; and review the identification of internal initiating events during operation at power in detail. This has now been completed and the reports have been published – see References [14] and [15] for the main reports and [16] and [17] for the reports on the assessment of the PSA. Step 4 of the GDA includes a more detailed review of the PSA. To take account of relevant recommendations from the head of ONR, Mike Weightman’s interim assessment report of the implications of the nuclear crisis in Japan for the UK nuclear industry, published in May 2011 (Ref. 22) and his final report expected in September 2011, ONR will not now draw conclusions from the GDA assessments in June 2011 as planned.

2.2 Requirement for a PSA

PSAs are performed for all nuclear installations in the UK to evaluate the design of the plant and to provide one of the inputs to determine whether the risk to workers and members of the public is both tolerable and ALARP. The PSAs need to address the numerical safety criteria given in the Safety Assessment Principles for Nuclear Plants (SAPs) published by ONR.

The following numerical safety criteria were defined in the 1992 version of the SAPs (see Reference [2]) and have been used in the assessment of the PSAs for the currently operating nuclear facilities:

- P42: Doses to the public
- P43: Risk to workers
- P44: Large release
- P45: Plant damage
- P46: Criticality incidents

These have been replaced by the numerical safety criteria given in the 2006 version of the SAPs (see Reference [3]) and these criteria are being used in the Generic Design Assessments (GDAs) of the PSAs produced for the new designs of nuclear power plants which could be built in the UK:

- Target 4: Design basis fault sequences – any person
- Target 5: Individual risk of death from on-site accidents – any person on the site
- Target 6: Frequency dose targets for any single accident – any person on the site
- Target 7: Individual risk to people off the site from accidents
- Target 8: Frequency dose targets for accidents on an individual facility – any person off the site
- Target 9: Total risk of 100 or more fatalities

The surrogate measures of risk (such as core damage and a release of radioactive material greater than specified quantities of I_{131} and Cs_{137}) given in the earlier version of the SAPs have been replaced by criteria that relate to the harm to people (death of a worker or a member of the public, and a release of radioactivity that would lead to 100 or more fatalities). Hence the requirement for a PSA has advanced from a Level 1+ PSA required by the old SAPs to a Level 3 PSA required by the new SAPs.

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 (PSR) 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. ONR 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 ONR who 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 ONR assessors in carrying out an assessment of a PSA is given in the SAPs and the Technical Assessment Guides (TAGs) which relates to the interpretation of the SAPs and the specific topics that an assessor may need to address. One of the TAGs relates to the assessment of PSAs and PSA related submissions and this has been updated so that it is consistent with the 2006 version of the SAPs (see Reference [7]). This provides an interpretation of the SAPs related to PSA and gives specific guidance to ONR inspectors in the assessment of a PSA. However, the TAG does not give formal acceptance criteria for safety case/ PSA issues and does not provide detailed information on how to judge the technical adequacy of the various PSA aspects assessed. In the UK, this relies heavily on the judgement, knowledge and experience of the ONR inspectors 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, EDF Energy²⁴ and Magnox Sites North²⁵ 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.

3. Numerical safety criteria

3.1 Tolerability of Risk from Nuclear Power Stations

One of the recommendations that came out of the Sizewell B Public Inquiry was 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”.

To address this recommendation, a document entitled “**The Tolerability of Risk from Nuclear Power Stations**” (referred to as TOR) was produced (see Reference [1]). This was issued for comment in February 1988 and the updated the final version was issued in October 1992.

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

1. unacceptably high where the risk is regarded as intolerable and cannot be justified in any ordinary circumstances;

²⁴ EDF Energy was formerly known as British Energy Generation Limited (BEGL).

²⁵ Magnox Sites North was formerly known as the British Nuclear Group (BNG).

2. 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
3. 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.

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

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

TOR also discussed the effects on society of a major accident and suggested that an event leading to one hundred to several hundred immediate and eventual deaths should not be more frequent than one in 100,000 years, allowing for the influence on the consequences of weather conditions – see Reference [1].

The guidance given in TOR was updated in 2001 in the publication “Reducing Risks, Protecting People; HSE’s Decision-Making Process” (referred to as R2P2) – see Reference [5]. This sets out an overall framework for decision taking by the Health and Safety Executive (HSE) which would ensure consistency and coherence across the full range of risks falling within the scope of the Health and Safety at Work (HSW) Act.

The risk management framework proposed in R2P2 is based on the approach described in TOR for nuclear power plants. R2P2 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.

R2P2 proposed the following criteria for the risk of death for workers and members of the public from the activities on a site:

7. 10^{-3} pa as the boundary between the ‘tolerable’ and ‘unacceptable’ regions for a worker;
8. 10^{-4} pa as the boundary between the ‘tolerable’ and ‘unacceptable’ regions for a member of the public; and
9. 10^{-6} pa boundary between the ‘broadly acceptable’ and ‘tolerable’ regions for both workers and members of the public.

This risk framework and the reference levels given in TOR and R2P2 have been used as the basis for defining the numerical criteria given in the SAPs.

3.2 Risk assessment framework

The way that the numerical targets have been structured is based on the TOR framework which has been extended in R2P2. This framework has been translated into targets by defining Basic Safety Levels and Basic Safety Objectives.

Basic Safety Limit (BSL): This is the boundary between the “tolerable” and “unacceptable” regions and represents the limit of tolerability. The ONR policy is that the level of risk from a new nuclear facility should at least be lower than the BSL. For existing facilities that have been designed and constructed to different safety standards and may have deteriorated with the passage of time, it is expected that additional improvements to safety can be made that are reasonably practicable. If this is not the case then consideration would be given to recommending regulatory action to shut down the facility.

Basic Safety Objective (BSO): This is the boundary between the “broadly acceptable” and “tolerable” regions. The BSO reflects modern safety standards and is the point beyond which the risk is so small that ONR inspectors need not seek further safety improvements. However, the licensee of the plant is still legally required to make further improvements where reasonably practicable.

The numerical values assigned to the BSOs and BSLs are used in judging whether the risks for nuclear facilities have been adequately controlled and reduced to a level that are ALARP. The numerical targets relate directly to the effects on people of normal operation and accidents including severe accidents and are used by ONR inspectors to give guidance to indicate where there is the need for consideration of additional safety measures.

3.3 Numerical criteria defined in the 1992 version of the SAPs

The 1992 revision of the SAPs chose to address the risks discussed in TOR supplemented by the consideration of the 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.

Numerical criteria were defined that related to the following measures of risk:

P42 – doses to the public:	total predicted frequencies of accidents on the plant which would give rise to doses to a person outside the site;
P43 – risk to workers:	total predicted individual risk of death (early or delayed) to a worker on the plant from doses of radiation arising from accidents
P44 – large release:	total predicted frequency of accidents on the plant with the potential to give a release to the environment greater than specified quantities of I_{131} or Cs_{137} .
P45 – plant damage:	predicted frequency of a degraded core for a nuclear reactor.
P46 – criticality incidents:	predicted frequency of an accidental criticality excursion on a plant other than a nuclear reactor

In the revision of the SAPs published in 2006, the numerical targets P42 - doses to the public and P43 - risk to workers have been retained and appear as Targets 8 and 5 respectively. The numerical target P44 - large release defined in terms of a release greater than a specified quantity of I_{131} or Cs_{137} has been changed to a societal risk criterion defined as the total risk of 100 or more fatalities. The numerical targets P45 – plant damage (interpreted as a degraded core for a nuclear reactor) and P46 – criticality incidents have not been retained.

Following the publications of the 1992 revision of the SAPs, the nuclear power plant operators updated their own Nuclear Safety Principles for Gas Cooled Reactors which are now formal company standards. They include numerical accident frequency criteria which are broadly equivalent to those defined in the SAPs.

3.4 Numerical criteria defined in the 2006 version of the SAPs

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 ONR 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 following numerical criteria have been defined:

Target 4: Design basis fault sequences – any person

Target 5: Individual risk of death from on-site accidents – any person on the site

Target 6: Frequency dose targets for any single accident – any person on the site

Target 7: Individual risk to people off the site from accidents

Target 8: Frequency dose targets for accidents on an individual facility – any person off the site

Target 9: Total risk of 100 or more fatalities

These targets defined relate to normal operations, design basis analysis, individual risk and societal risk. The numerical criteria are not legal limits and hence not mandatory. They are indicative figures that are intended to guide ONR inspectors in judging whether risks have been reduced to a level that meets the ALARP requirement.

Targets 4, 6 and 8 present dose-frequency ladders that are based on the premise that the larger the potential consequences of an accident, the smaller should be its frequency. More detail on the rationale behind the numerical targets is found in an explanatory note – see Reference [4].

Target 4: Design basis fault sequences – any person

The targets for the effective dose received by any person arising from design basis fault sequence have been specified as a function of the initiating fault frequency for people on-site and off-site as follows:

	Target effective dose		Initiating fault frequency
	On-site	Off-site	
BSL:	20 mSv	1 mSv	$>10^{-3}$ pa
	200 mSv	10 mSv	10^{-3} to 10^{-4} pa

	500 mSv	100 mSv	$<10^{-4}$ pa
BSO:	0.1 mSv	0.01 mSv	

In addressing this target, the radiological analysis to determine the maximum dose should be performed on a conservative basis. In particular, for off-site releases, it should be assumed that:

- a) the person remains at the point of greatest dose for the maximum duration, although for extended faults a more realistic occupancy may be assumed after a suitable interval;
- b) the conditions under which the fault is analysed has characteristics which produce the highest dose to that person; and
- c) no emergency countermeasures are implemented, other than those whose implementation is shown to be highly likely.

Target 5: Individual risk of death from on-site accidents – any person on the site

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

BSL: 1×10^{-4} pa

BSO: 1×10^{-6} pa

The BSL has been set at 10^{-4} pa (rather than 10^{-3} pa given in R2P2) since the majority of the risk to people on the site is from normal operation. The BSO has been set at 10^{-6} pa which is consistent with R2P2.

Target 6: Frequency dose targets for any single accident – any person on the site

The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are:

Effective dose, mSv	Predicted frequency per annum	
	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}

The maximum effective dose to the worker who is most exposed to the ionising radiation needs to be calculated using a best estimate approach or, where this is not practicable, reasonably conservative assumptions can be made. The effects of any mitigating action can also be taken into account if a

satisfactory case has been made for them. This target is not intended to include the risks associated with personnel returning to perform recovery actions after a radiation accident or emergency.

Target 7: Individual risk to people off the site from accidents

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

$$\text{BSL: } 1 \times 10^{-4} \text{ pa}$$

$$\text{BSO: } 1 \times 10^{-6} \text{ pa}$$

The BSL has been set at 10^{-4} pa since the majority of the risk to people off the site is from accidents. The BSO has been set at 10^{-6} pa and this is consistent with R2P2.

The calculation of the risk of death to a person outside the site needs 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 wind and weather conditions and the effect of countermeasures. A particular issue is the physical position of the hypothetical person.

Target 8: Frequency dose targets for accidents on an individual facility – any person off the site

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	Predicted frequency per annum	
	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}

A single facility which just met the BSLs/BSOs in the dose ladder, allowing for variability of wind direction, would give a maximum individual risk of death to a person outside the site of about $10^{-5}/10^{-7}$ pa, ignoring countermeasures which are lower than the targets given in TOR and R2P2.

The facility safety should be balanced so that no single class of accident should make a disproportionate contribution to the overall risk – that is, of the order of one tenth of the frequency in each dose band.

For accidents that lead to doses of >1000 mSv, the risk of prompt death should be considered and the analysis should also be assessed against the societal risk levels in Target 9.

In addressing this criterion, the calculation of the risks and frequencies should, as far as possible, be realistic estimates for the specified accidents occurring on the facility. The radiological analysis to evaluate maximum effective dose should be carried out for a hypothetical person located at the distance of the nearest habitation (that is, any place with significant daily occupancy), or one kilometre from the facility, whichever is nearer, or at the point of greatest dose if that is further away. The person should be assumed to remain directly downwind of the release point for the duration of the release. The best estimate dose should be calculated as the expected value over the possible weather conditions.

The dose bands that have been defined relate, in an approximate fashion, to the off-site actions that could be expected following an accident, namely:

0.1-1 mSv	10. additional off-site radiation and contamination surveys 11. possibility of advice being given to restrict the use of foodstuffs produced close to the site
1-10 mSv	12. increased off-site surveys; restrictions on the use of foodstuffs likely to be implemented 13. sheltering or issue of stable iodine may be considered in areas very close to the site
10-100 mSv	14. restrictions on foodstuffs likely to be implemented many kilometres from the site 15. sheltering or issue of stable iodine likely to be implemented 16. evacuation may be considered in areas immediately adjacent to the site
100-1000 mSv	17. restrictions on foodstuffs likely to be extensive 18. sheltering or issue of stable iodine likely to be implemented to several kilometres from the site 19. evacuation of nearby population likely to be implemented

These demonstrate that the dose bands are a suitable surrogate for a range of events, including risk of death, which could affect the individual from different levels of accident.

Target 9: Total risk of 100 or more fatalities

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

$$\text{BSL: } 1 \times 10^{-5} \text{ pa}$$

$$\text{BSO: } 1 \times 10^{-7} \text{ pa}$$

The BSL has been based the consideration of societal risk given in TOR.

This includes fatalities both on and off the site. A significant proportion of the fatalities would be expected to occur from the stochastic effects of the exposure of very large populations, which are typically estimated using collective dose calculations. Based on studies carried out by the Health Protection Agency (HPA), the integration of these effects should be over 100 years and restricted to the UK population.

The total risk should be calculated taking account of the frequency distribution of the source terms together with probabilistic weather conditions. The weather conditions should be based on meteorological data appropriate to the site and the population data should be based on current demography. The ability to

implement off-site countermeasures should be based on current UK and relevant international advice and should be demonstrated in the safety case.

Accidents where the consequences are less than 100 deaths should also be considered in the overall ALARP demonstration if their frequency is above the BSO. This target does not cover all the factors related to societal concerns and, in making an ALARP demonstration, the consequences in terms of other societal effects must also be considered.

3.5 Dealing with time at risk situations

The numerical targets relate to annual average risks. However, it is recognised that higher levels of risk will exist for short periods of time. The overall requirement is that there should be sufficient control of radiological hazards at all times and decisions need to be made as to whether additional safety measures are needed to meet the ALARP requirement. The consideration of Short Term Risks and Time at Risk considerations are a new addition to 2006 version of the SAPs, neither having been explicitly mentioned in the 1992 version.

An important factor in assessing short-term risks is the degree of independence between the reason for the risk being only present for a short period and the fault or hazard causing the risk. In particular, consideration should be given to:

- a) independence between the initiating event and the activity or operation being undertaken;
- b) the degree of control that the duty-holder has over the initiating event and the activity or operations; and
- c) the degree to which the risk only arises due to the activity being undertaken – for example, lifting operations.

Any period in which the risk is elevated (for example, due to equipment unavailability or occupancy of hazardous areas) must be subject to a specific demonstration that risks are controlled ALARP and the period of elevated risk should be as short as reasonably practicable.

The safety case should not rely solely on numerical risk estimates or on averaging risk over a longer period of time. Good engineering and operational practices should be prominent in the case.

Sufficient protection based on engineering and operational considerations should be retained. If this is not reasonably practicable, adequate substitution arrangements should be considered. The extent of protection should 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 radiological hazard should normally be taken even though the time at risk may be short.

During operations which impose a planned short term risk, means for monitoring the actual facility state should be in place to ensure that the mode of operation and the time during which it persists meet the assumptions in the safety case. Where possible, means to reverse the process should be in place in the event that it becomes apparent that the safety case is not being met.

Where reasonably practicable, contingency measures should be identified that could cope if the situation deteriorates further, including accident management arrangements.

High risks that would exceed BSLs if evaluated as continuous risks should be avoided except in special circumstances. These circumstances should be 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 should not be the sole argument for acceptability that a situation is ALARP.

4. PSA standards and guidance

4.1 UK industry guidance on PSA

There are no UK specific PSA standard or guidance for the production of a PSA for a nuclear facility. The current raft of UK PSAs have been developed based on the international practices that each licensee considers to be fit for purpose for the PSA 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.

Participants from the UK have been involved in the development of the IAEA Safety Standards and Guides. In particular, there was involvement in the development of the early procedures for the production of Level 1, 2 and 3 PSAs for nuclear power plants developed by IAEA in the 1990s – see References [9], [10] and [11] respectively. This was used as guidance in producing the PSAs that have been developed for all the nuclear power plants currently operating in the UK. There has also been UK involvement in the development of the Specific Safety Guides for Level 1 and 2 PSA – see References [12] and [13]. This has been taken into account in the development of the parts of the Safety Assessment Principles (SAPs) and the Technical Assessment Guide (TAG) related to PSA.

Since 2002, ONR has been making an important effort to assess the PSAs for the Gas Cooled Reactors in the UK against modern standards and international practices. For this purpose an approach has been adopted that is based, to some extent, on the IAEA IPSART (International PSA Review Team) Service.

4.2 ONR Safety Assessment Principles and Technical Assessment Guides

In the assessment of the PSAs, ONR inspectors use 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 in the interpretation and application of the SAPs and form an integrated suite of guidance to ONR inspectors. They are being progressively updated to reflect the version of the SAPs published in 2006. The TAG most relevant to the assessment of PSA is T/AST/030 on “Probabilistic Safety Analysis”.

General Fault Analysis SAPs

- FA.1 Fault analysis should be carried out comprising design basis analysis, suitable and sufficient PSA, and suitable and sufficient severe accident analysis
- FA.2 Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement
- FA.3 Fault sequences should be developed from the initiating faults and their potential consequences analysed

FA.4 – Relate to the design basis analysis
FA.9

FA.2 requires that a systematic process should be carried out for identifying initiating faults and this should be auditable and comprehensive. This should include all significant inventories of radioactive material, all planned operating modes and activities, and all internal and external faults and hazards.

SAPs relating to the PSA

- FA.10 Suitable and sufficient PSA should be performed as part of the fault analysis and design development and analysis
- FA.11 PSA should reflect the current design and operation of the facility or site
- FA.12 PSA should cover all significant sources of radioactivity and all types of initiating faults identified at the facility or site
- FA.13 The PSA model should provide an adequate representation of the site and its facilities
- FA.14 PSA should be used to inform the design process and help ensure the safe operation of the site and its facilities

FA.10 requires that the PSA should be able to be used in determining whether the numerical targets given in the SAPs have been met; the design is balanced; and the risks are ALARP. This requires that a comprehensive PSA is produced that meets modern standards.

FA.11 requires that the PSA should be directly related to existing plant and site information, data and documentation. In addition, the PSA should be kept living – that is, it should be periodically updated to reflect: the current design and operation; operational experience; improved understanding of physical processes or accident progression; and advances in modelling techniques.

FA.12 requires that the scope of the PSA needs to cover all sources of radioactivity at the facility (fuel ponds, fuel handling facilities, waste storage tanks, radioactive sources, reactor core, etc), all types of initiating faults (internal faults, internal hazards and external hazards) and all operational modes (full power, low power, shutdown, start-up, refuelling and maintenance outages).

FA.13 relates to the technical adequacy of the PSA and requires that it should have a robust technical basis and identify all the contributors to the risk. The analysis should systematically and comprehensively identify the complete range of sequences leading to the undesired consequences that may occur.

The PSA should account for all contributions to the risk including: random component failures; components failed by the initiating fault; common cause failures; unavailabilities due to testing and maintenance; pre-initiating fault human errors; human errors that lead to initiating faults; and human errors during the course of the accident sequences. The analysis should take account of the dependencies between separate human activities.

The level of detail of the PSA should be sufficient to ensure that it is realistic, the logic is correct, the dependencies are captured and the data used is applicable to the basic events in the model. Model simplifications should be clearly described and justified.

The frequency of occurrence and consequences of each of the fault sequences identified should be estimated. Justification should be provided for any screening or grouping used in the PSA and care should be taken to avoid the introduction of gross conservatism that would distort the conclusions drawn from the analysis and limit its usefulness.

Best-estimate methods and data should be used throughout the PSA. If this is not possible, reasonably conservative assumptions should be made and the sensitivity of the risk to these assumptions should be established.

The PSA should use plant specific data wherever possible. If this data is not sufficient, it should be combined with applicable generic data using Bayesian techniques. The use of generic data or judgements should be justified.

When models are used for the calculation of probabilities in the PSA, the methodologies used should be justified and should account for all the key influencing factors. This is the case for the probabilities of: personnel error and the potential dependencies between separate human activities (see T/AST/012); common cause failure (see T/AST/036); structural failures (see T/AST/016 and T/AST/017); computer-based systems and software reliability (see T/AST/046); passive systems; and the probability of occurrence of phenomena following a severe accident.

The results of the PSA should be comprehensively documented and this should include the numerical results, lists of minimal cutsets, importance measures, the justifications for any assumptions made, and the results of sensitivity studies and uncertainty analysis.

FA.14 defines the uses that should be made of the PSA which includes its use in: the initial design of a new plant; making changes to the design or operation during the life of the plant; safety classification of structures, systems and components; testing, inspection and maintenance planning and daily management of plant configuration; changes to operating procedures, limits and conditions; off-site emergency planning and response; and the evaluation of the risk significant events. The PSA should also be used by ONR inspectors to understand the significance of safety issues and inspection findings, and to target inspection activities on those areas with the highest safety significance.

FA.14 also requires that that PSA should be used in an appropriate way for any applications. This requires that: the issue to be evaluated should be defined together with the type of results required from the PSA; all aspects of the PSA model should be suitable for the application; and the PSA should be extended and/or enhanced to address the issue. Sensitivity studies and uncertainty analysis should be carried out to inform the decision-making process.

SAPs relating to severe accident analysis

FA.15 Fault sequences beyond the design basis that have the potential to lead to a severe accident should be analysed

FA.16 The severe accident analysis should be used in the consideration of further risk-reducing measures

Severe accidents are defined as those fault sequences that lead to: a radiological dose of 500mSv for a worker or 100mSv for a member of the public (which are the BSLs of Target 4 of the SAPs); or a substantial unintended relocation of radioactive material within the facility.

The aim of the severe accident analysis should be to: determine the magnitude and characteristics of their radiological consequences; and demonstrate that there is no sudden escalation of consequences just beyond the design basis. As well as supporting the PSA, the analysis should provide an input into: the identification of further preventative or mitigating measures; accident management strategies; and emergency planning.

SAPs relating to the assurance of validity of the data and models used in the fault analysis

- FA.17 Theoretical models should adequately represent the facility and site
- FA.18 Calculation methods used for the analysis should adequately represent the physical and chemical processes taking place
- FA.19 The data used in the analysis of safety related aspects of plant performance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means
- FA.20 Computer models and datasets used in support of the analysis should be developed, maintained and applied in accordance with appropriate quality assurance procedures
- FA.21 Documentation should be provided to facilitate review of the adequacy of the analytical models and data
- FA.22 Studies should be carried out to determine the sensitivity of the fault analysis (and the conclusions drawn from it) to the assumptions made, the data used and the methods of calculation
- FA.23 Data should be collected by the licensee throughout the operating life of the facility to check or update the fault analysis
- FA.24 The fault analysis should be updated where necessary and reviewed periodically

Many theoretical models and calculational methods are used in the PSA including: reliability models for common cause failure and human error; thermal-hydraulic analysis; accident progression and fission product transport analysis; and structural integrity analysis. In addition, the PSA software uses a calculation algorithm to quantify the PSA models and to obtain the list of cutsets. These should adequately represent the real processes taking place in the facility and that the calculations are done as intended by the analysts.

The duty-holders should have put in place adequate procedures to develop, maintain and apply computer models and databases. These procedures should cover verification, validation or qualification of computer codes for the specific design of the plant and that the codes are only used within their limit of applicability by trained users.

PSAs should be documented in such a way as to ensure that each aspect of the PSA can be directly related to existing facility information, facility documentation or the analysts' assumptions in the absence of such information.

Data should be collected by the duty-holders relating to the initiating fault frequencies, component failure probabilities, unavailabilities, etc, used in the PSA and this should be used when the PSA is updated.

The updating of the PSA to maintain it as a living PSA should be done as part of the Periodic Safety Reviews (PSRs) normally carried out every ten years or on a shorter timescale if a high number of changes have been made to the plant or the safety case.

5. Status and scope of PSA programmes

5.1 PSA for the Sizewell B Pressurised Water Reactor (PWR)

Background

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 RiskSpectrum 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 conservatism which were in the licensing PSA and will be used by the licensee to provide advice 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 ALARP.

Current model developments include: simplification of the Level 2 PSA, updating generic data with Sizewell B specific data, further increasing the scope of the electrical modelling to support station activities and more detailed analysis of mid-loop operation.

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

20. increasing the enrichment of the fuel used in the reactor,
21. increasing the time given in the Technical Specifications for the period between refuelling outages from 18 months to 2 years,
22. 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,
23. optimization of the in-service testing intervals for Motor Operated Valves, and
24. safety case support.

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

Recent developments

The Sizewell B Living PSA has been updated 5 times in the last 10 years and the main changes introduced are as follows

- (1) Extensive refinements have been made to the scope of the modelling of faults at shutdown as follows:

Mode 4: this is now considered explicitly and has been split into operating states covering decay heat removal via the residual heat removal system (RHRS) or the steam generators (SGs).

Mode 5: this has been split into operation in a number of sub-states as follows:

25. steam bubble present,

26. water solid,

27. reactor coolant system (RCS) drained down to just below flange level (RCS intact with isolatable and non-isolatable vents present),

28. mid-loop (RCS intact and not intact),

29. RCS not intact (flange level and above), and

30. at least one reactor coolant pump (RCP) in operation (boron dilution fault related).

Mode 6: this has been split into operating states covering RCS drained down to just below flange level (reactor pressure vessel head on and off), refuelling pool filled

Cold overpressure fault, the safeguards requirements have been revised and the analysis updated.

(2) A method of Bayesian updating for data has been developed, independently peer reviewed and used for component failure rates and initiating fault frequencies;

(3) Uncertainty analysis now undertaken.

(4) Extensive updating to electrical modelling undertaken - used as an input to support justification for maintaining an essential electrical separation group at power.

(5) Consequential RCP seal LOCA modelling revised based on US operating experience.

(6) Incorporation of IAEA IPSART recommendations including: the modelling of LOCA and consequential LOCA (including SG tube rupture) accident sequences has been updated to provide a better estimate and make the analysis more realistic; and the representation of latent errors that lead to safeguards equipment being unavailable has been increased.

(7) Updated fuel storage pond faults modelling.

Recent uses of the Sizewell B PSA

Extensive use has been made of the Living PSA that has been developed for Sizewell B which includes the following:

31. as the basis for the Risk Monitor PSA model used with the RiskWatcher software;

32. in support of maintenance and outage planning;

33. continued use in refining Limiting Conditions of Operation and the Action Completion Times given in the Technical Specifications;

- 34.support for hardware modifications;
- 35.support in response to emergent issues at power and shutdown e.g. pressuriser heaters issue; and
- 36.as an input into operator training.

In addition, the CCF research into a replacement for the UPM method used in the AGR PSAs will have an impact on Sizewell B in terms of how to take CCF modelling in the Living PSA forward.

5.2 PSA for the Advanced Gas-cooled Reactors (AGRs)

PSAs for the Periodic Safety Reviews for the AGRs

PSAs have been produced for all the AGRs as part of the Periodic Safety Reviews (PSR) that are carried out every 10 years. The aim of these PSAs is to address the frequency-dose criterion for any person off the site from accidents. This criterion, which was defined as SAP P42 in the 1992 version of the Safety Assessment Principles (see Reference [2]) is now given as Target 8 in the 2006 version of the SAPs (see Reference [3]).

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 of areas including:

- 37.increasing the time given between refuelling outages from 2 to 3 years, and
- 38.extending the duration of shifts at Hinkley Point B from 8 to 12 hours, and
- 39.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.

In 2002 and 2003 respectively, the Hinkley and Hunterston PSAs were subjected to ONR-led international reviews that adopted an approach based, to some extent, on the IAEA International PSA Review Team (IPSART) Service. Follow-up reviews were carried out in 2006/07. Similar reviews have also been undertaken for the Dungeness, Hartlepool/Heysham 1 and Heysham 2/Torness PSAs. As part of PSR2, EDF Energy performed a self-assessment of the Heysham 2/Torness PSAs.

The PSAs for the AGRs have more recently been updated for PSR2, with completion on the 10 year timescale from PSR1. The opportunity has been taken to incorporate many of the recommendations arising from the ONR-led reviews, in particular to include increased usage of site specific data together with Bayesian updating methods and uncertainty analysis. In addition, the updated models include enhanced coverage of internal and external hazards and a more detailed approach to human reliability analysis. Work is also ongoing to identify a preferred methodology for the derivation of CCF probabilities, noting that the current UPM (partial beta factor) method is conservative.

Note: The PSAs are also updated between the PSRs to reflect major changes thereby ensuring that an understanding of the station risk can always be inferred. In addition, reviews are carried out on a 3-yearly basis to update the PSAs as required to reflect plant configuration and any less significant changes.

Fire PSA for Hinkley Point B

A fire PSA has been produced for Hinkley Point B. The starting point for the analysis was the PSA model developed for the second Periodic Safety Review (PSR2). The methodology used was based on the guidance given in the IAEA Safety Reports Series No. 10 on the treatment of internal fires in PSA and NUREG/CR-6850 on the methodology for a fire PRA.

The plant was subdivided into compartments; 166 were identified and these were characterised in terms of the potential for a fire to occur, the fire protection provided and the equipment in the compartment related to post trip cooling. These compartments were screened by impact and those that could lead to an automatic reactor trip, require a controlled reactor shutdown or damage equipment required for post trip cooling were retained along with the compartments with a significant fire loading.

The remaining fire compartments were screened by frequency. The frequencies of fires from fixed ignition sources were derived using station specific data and data from all the gas cooled reactors in the UK and those from transient fires have been allocated to specific fire compartments based on the approach defined in NUREG/CR-6850.

In the initial screening, the probabilities of loss of PTC have been calculated using the event trees from the internal events PSA and the assumption was made that all the components and cables in the compartment were damaged by the fire. In most cases, the spurious trip event tree was used but in some cases another event tree (such as loss of grid) was used since this provided a more accurate model. For fires in the Central Control Room (CCR) no credit has been taken for operator actions carried out in the CCR.

The screening analysis also addressed inter compartment/ multi compartment fires which models fires that spread from the fire compartment that it starts in to adjacent compartments. This takes account of the fire detection and suppression systems in the compartment where the fire initiates and the fire barriers between adjacent compartments. In the screening analysis it has been assumed that all equipment located in the affected compartment will be lost.

This was followed by a refined screening where some of the conservatism in the initial screening were removed. This included: the fire frequencies were recalculated by a Bayesian updating process using station specific data; pipework was assumed not to fail due to a fire; credit was taken for automatic fire detection and suppression for cable fires; credit was taken for fires not spreading between cabinets; and the layout of the compartment.

Within the scope of the fire PSA, a systematic analysis was carried out to identify the hot shorts that could occur in fire damaged cables leading to initiating events or to spurious operation of any component involved in post trip cooling. A systematic analysis was carried out to identify the hot shorts that could occur and the safety components that would be affected. The screening analysis was reviewed to determine whether any of the fire compartments screened out needed to be included because of the contribution to the DB5 PTC frequency from hot shorts.

Of the 166 fire compartments identified, 68 were screened out by impact, 76 were screened out by the initial frequency screening and 16 were screened out by the refined screening leaving 6 to be taken forward for detailed analysis.

The aim of the detailed analysis was to calculate a more realistic DB5 PTC frequency from fire that takes account of all the relevant factors including: the relative locations of ignition sources, combustible materials and safety components and cables; the protection provided within compartments (such as equipment cabinets); the rate of fire propagation; fire detection and suppression; and additional operator actions.

In the detailed analysis, specific event trees were drawn for some of the fire compartments to model the fire scenarios more accurately.

The overall frequency of loss of PTC following a fire leading to a DB5 release was found to be small compared with the overall frequency of loss of PTC from internal faults. An uncertainty analysis has also been carried out that addresses the statistical uncertainties in the component failure data and initiating event frequencies.

Fuel route PSA

The AGRs currently provide a quantification of the risk associated with fuel route operations independent of the reactor PSAs. This approach reflects the separate and independent plant and protection provisions for fuel route activities. However, as part of PSR2, reviews have been carried out against modern standards with a view to identifying potential improvements that could be made to the quantification methods. A revised approach using fault and event trees has been trialled for some AGRs and improvement work is currently ongoing.

A pilot study has been carried out for the PSA for the refuelling and fuel handling operations for the Heysham 1 and Hartlepool AGRs. These reactors are currently refuelled off-load with the primary circuit depressurised.

A review was carried out to determine the current international standards and methodologies being used to produce PSAs for refuelling and fuel handling operations for other types of nuclear power plants and nuclear facilities worldwide. The review included IAEA standards on PSA, guidance on PSA for low power and shutdown states, PSA for non-reactor nuclear facilities, and the analysis for the lifting equipment used to handle irradiated fuel assemblies and other components.

The pilot study was carried out for the group of initiating events where a heavy item (irradiated fuel stringer, irradiated part assembly, control rod, new fuel assembly or outage equipment) is dropped during the refuelling operations carried out at the reactor. The methods used for the internal events, at-power PSA were used for the pilot study and the PSA model was developed using RiskSpectrum. Events trees were drawn which included failure of the protection provided (which includes mechanical/ electrical interlocks and administrative controls), the mitigation factors identified (such as the drop height) and the factors that influence the magnitude of the off-site release (which include the consequential failures that could occur such as failure of the support plates for reactor assemblies or failure of the reactor containment). Fault trees were developed for the mechanical and electrical interlocks which included the weight sensing system that trips the fuelling machine hoist and applies the brakes following an indication of a high load due to the snag of a fuel element. The fault trees that have been developed are different from those in the internal events PSA due to the design of the protection provided. The off-site consequences of the fault sequences identified were categorised into the five dose bands defined for the numerical safety criteria. The pilot study has indicated that the approach used for the internal events, at-power PSA can be used for the fuel route PSAs.

Level 2 PSA for the AGRs

The AGR design, which does not include an outer containment building, is not readily amenable to Level 2 PSA modelling. A pilot study has been carried out to ascertain the feasibility of carrying out Level 2 PSA for AGRs. It takes a limited number of sequences from the existing Hinkley Point B PSA, allocates them to Sequence Classes and then assesses the consequences of each class with a view to making a more refined estimate of the frequency of the associated radiological releases. Acceptably for a pilot study, a large number of simplifying assumptions are made in demonstrating how such refinement could be carried out. However, the consequence is that the lack of available information and analysis for detailed accident progression mean that the results of the pilot study directly reflect the simplifying assumptions made.

In order to carry out a meaningful study, the uncertainties associated with accident progression and the expected timeline would have to be reduced to enable realistic success probabilities to be assigned to each strategy. Whilst it can be concluded that it is possible to carry out a full Level 2 PSA for the AGRs, the overall benefits and reasonable practicability of this work remain under review.

5.3 Review of the AGR PSAs

A series of reviews of the PSAs for the AGRs has been commissioned by ONR. They were started in 2003 and have been carried out by a team of three independent, experienced PSA practitioners who have followed the concept of the IAEA IPSART process. So far the reviews have addressed the PSAs for Hinkley Point B, Hunterston B, Dungeness B, Hartlepool and Heysham 2. The overall conclusion is that many aspects of the PSA were consistent with current practice for a full-scope PSA but some detailed points were identified as described below. EDF Energy has carried out additional analysis or put programmes of work in place to address the findings of these reviews and this is also indicated below.

Initiating faults/ fault schedule: the process used to identify initiating faults is systematic, complete and well organised. The completeness and level of specificity in the fault schedules are consistent with current practice. In addition, the fault grouping into Bounding Faults is generally well justified. However, it was noted that a number of initiating event frequencies have been calculated using the zero event approximation (where, for initiating events with no recorded failures, the frequency is taken to be $0.55/T$). This does not correspond to the current practice and means that a large number of different initiating faults have the same frequency. However, this is being addressed by EDF Energy.

Component failure data: the way that the component failure data is assigned generally conforms to current practice. It was noted that a substantial effort has been made to collect plant specific failure data from the plant and to derive failure parameters for selected PSA equipment. Where the zero event approximation has been used, it was recommended that this should be replaced by a Bayesian process using generic and plant specific data. EDF Energy have now implemented a Bayesian approach.

Accident sequence analysis/ event trees: the scope of the accident sequence analyses, the level of detail in the event tree function events and the detailed logic structure correspond to good practice. No major technical issues were identified.

Systems analysis/ fault trees: the structure, completeness and resolution of the fault trees and the modelling of dependencies from support and supply systems follow current practice. However, it was noted that condensed (single) events have been used for some of the reactor trip and shutdown systems and there was a concern that the dependencies due to support systems may not be explicitly modelled. It was considered that this might limit the ability of the PSA models to be used to examine the risk impacts from proposed changes to the design or operation of the plant.

Human reliability analysis: a recognised, mature approach is used consistently to derive the human error probabilities – namely the Human Error Assessment and Reduction Technique (HEART). The review concluded that the models for each primary function generally contain a good treatment of the cognitive responses for that function and implementation actions for each respective system.

EDF Energy are currently making further improvements in this aspect of the PSAs by developing the Nuclear Action Reliability Assessment (NARA) method which is based on the HEART approach but takes account of recent research and operating experience data and is more applicable to the tasks carried out at nuclear power plants.

Common cause failure (CCF): CCF is modelled using the β -factor method and the CCF probabilities have been derived using the Unified Partial Method (UPM). However, the reviewers consider that there are problems with this approach in that it has not been calibrated and is vulnerable to a systematic bias in the results where single analysts have been used. This approach does not meet current practice and the reviewers recommended that further use of it should not be made in its current form.

EDF Energy are addressing this issue and have been investigating the use of one of the more detailed parametric methods (the α -factor or Multiple Greek Letter method) for modelling CCF with the parameters being derived from operating experience data and a pilot study has been carried out.

Consequence analysis: the aim of the consequence analysis carried out is to allocate the fault sequences identified in the event trees to Dose Bands (DBs) 1 to 5 as defined in the numerical safety criteria. This explicitly takes account of fault sequences that result in partial fuel damage and is different from the PSAs for light water reactors where the focus is on large scale fuel damage. However, it was noted that the sequences that have been allocated to DB5 (defined as an off-site dose of >1000 mSv to a member of the public) have not been analysed in detail. There is no realistic, quantitative evaluation of accident progression and radiological releases and hence the analysis is not consistent with current practice.

EDF Energy are addressing this issue and are carrying out work to investigate core degradation and (large) radiological release processes associated with fault sequences currently allocated to DB5. This will allow a quantitative assessment of the AGRs against ONR's Safety Assessment Principals for societal risk.

Hazards: the current PSA do not contain an integrated analysis of the risk from internal and external hazards. It was noted that an analysis has been carried out for a few specific hazards. However, it was considered that these analyses had been performed to confirm the validity of specific design criteria and licensing-based assumptions, rather than to evaluate the actual risk from the hazard.

EDF Energy is addressing this issue and has carried out a detailed fire PSA for Hinkley Point B.

Uncertainties: it was noted that an uncertainty analysis has not been carried out for the AGRs. The reviewers consider that uncertainties represent central information in PSAs and the current practice is to carry out such an analysis. EDF Energy are now carrying out uncertainty analysis.

Risk Monitor: the review of the PSAs to be used in the new Risk Monitors at Heysham 2 and Torness concluded that the methods used were generally very thorough and quite sophisticated and the modified fault trees had been configured to account for the actual status of individual components (running, standby or out of service for maintenance). However, it was noted that ESOP only quantifies the frequency of DB 5 releases for each maintenance state and questioned whether it should also address DBs 1 to 4. EDF Energy consider that the PSA model for BD5 provides complete coverage of fault sequences and bounds those in lower dose bands.

5.4 PSA for the Magnox reactors

Long Term Safety Reviews (LTSRs)/ Periodic Safety Reviews (PSRs) 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 to a member of the public 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 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:

40. 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),
41. 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),
42. to inform on the benefits of modifications in terms of reductions in expected accident cost, and
43. to check that operating rules related to plant unavailability deliver satisfactory control of risk.

Currently only two Magnox reactors remain operational; Oldbury and Wylfa. A revision of the PSA as part of the PSR has been completed in the past few years and at this time the Wylfa PSA was enhanced to include a more detailed consideration of the risks from internal fires. In 2004 the Wylfa PSA was subjected to an ONR-led international review that adopted an approach based, to some extent, on the IAEA IPSART Service.

Fire PSA for Wylfa

A fire PSA has been carried out for the Wylfa Magnox nuclear power plant. The methodology used for the fire PSA was based on the guidance given in the IAEA Safety Reports Series No. 10 on the treatment of internal fires in PSA and NUREG/CR-6850 on the fire PSA methodology.

The fire PSA was based on the Fire Consequence Assessments (FCAs) that were carried out for the significant rooms in the plant to identify which fires have the potential to damage the post-trip cooling (PTC) capability. The FCAs contain all the information required for each of the rooms which includes: ignition sources; inventories of fixed and transient combustible materials; fire detection systems; automatic

and manual fire suppression systems; fire barriers, doors and penetrations; safety components and cables that could be damaged by the fire; and the layout of the fire compartment. This information was confirmed by plant walk-downs by the PSA analysts.

The surveys carried out to produce the FCA reports included the following systems which are credited in the PSA: the Emergency Boiler Feed Pumps (EBFPs), AC Gas Circulator Pony Motors, the Electrical Overlay System (EOS), the Circulator Auxiliary Cooling System (CACs) and the cable routes for the power supplies, switchgear supplies and essential control/ interlock cables associated with these systems. In addition, there are a number of systems that would not be affected by fire which include: Back-Up Feed System (BUFS), Tertiary Feed System (TFS), TFS boiler vents valves, and the boiler Safety Relief Valves (SRVs). A number of systems have not been surveyed and no credit has been taken for them in the PSA including: Main Boiler Feed (MBF) system, Gas Circulator Main Motors and DC Gas Circulator Pony Motors.

A fire fault schedule was drawn up for each of the rooms that identified: the fires that could occur; the essential supplies PTC plant challenged; the ignition sources and combustible materials present; the fire protection measures available such as fire detection, suppression and fire barriers; the essential supplies PTC plant available; the post-trip cooling claimed; and any operator actions required after the fire.

The frequency of fires from fixed ignition sources was calculated as the sum over all the ignition sources in the room. Fire frequency data from the following data sets was used: Wylfa; all the Magnox plants; all the UK nuclear plants; and generic data from available fire PSAs. The frequency of transient fires was calculated using the approach defined in NUREG/CR-6850 which takes account of: the maintenance and repair activities; the occupancy; and the quantity of combustible material that can be stored in the room.

In the screening analysis, it was assumed that all the safety components and cables in the room were damaged by the fire and no credit was taken for fire detection and suppression. The failure of PTC was calculated using the updated PSA for the plant which included the BUFS. A two stage quantitative screening approach was carried out and rooms were screened out if: the probability of failure of PTC following the fire was $<10^{-6}$; or, for the rooms remaining, the frequency of the loss of PTC was less than 1% of the total for all the rooms. Of the 26 rooms identified as “high significance” in the qualitative screening carried out in the preparation of the FCA reports, 8 met the quantitative screening criteria and were taken forward for detailed analysis.

Fire detection and suppression was modelled using fire propagation event trees. Since UK data was not readily accessible, the failure probabilities used were derived using generic data.

The fire scenarios modelled included: intra-room fires; inter-room fires and fires with “widespread consequences”.

Intra-room fires: this addressed the fires scenarios that can occur within any of the 8 rooms included in the analysis. A qualitative screening process was carried out to identify the scenarios that would lead to the unavailability of 1 or more EBFPs or 2 or more AC Pony Motors.

Inter-room fires; this addressed the potential for fires to spread from one room into another through penetrations such as doors, electrical cables, pipes, ventilation ducts, etc. A simplified, conservative analysis has been carried out – for example, it has been assumed that a fire that spreads into an adjacent room will lead to a full room burnout. Three cases were identified where the spread of the fire between rooms increased the consequences of the fire.

Widespread consequences: these are fires that can cause hot-shorts in cables or cabinets leading to spurious operation of equipment or to incorrect indications to the operators. These were identified using a structured

approach based on plant information on the design of control systems and the layout of the control cables. The widespread consequences were screened based on the potential for it to: affect the availability of PTC plant; cause a reactor depressurisation; or required additional operator actions. Of the 38 fault scenarios identified, five were taken forward for inclusion in the PSA.

The fire scenarios have been listed in the Fire PSA Fault Schedule (FPFS) and an event tree has been developed for each of them. These start from the initiating fire and graphically represent the successes and failures of the individual systems that are available for PTC which includes boiler feed, gas circulation and boiler blowdown. The human error probabilities (HEPs) included in the internal events PSA model have been reviewed for each of the fire scenarios identified in the FPFS and they were changed where necessary to take account of the consequences of the fire – for example, where breathing apparatus needed to be worn. The fire scenario event trees have been quantified taking account of the damage to safety components and cables and the effect of the fire on the HEPs.

A wide range of sensitivity studies were carried out which included: the assumptions made on the failure of PTC plant following a fire; the fire PSA input data; the provision of feed to reactor 1 using the EBFs on reactor 2; and the effectiveness of fire detection and suppression.

5.5 Generic Design Assessment

ONR is carrying out a pre-licensing process known as the Generic Design Assessment (GDA) to evaluate new reactor designs in advance of an application for a nuclear site license being made. If the design is judged to be satisfactory, a Design Acceptance Confirmation will be issued. The following designs are currently under evaluation:

44. UK AP1000 which is a PWR with passive systems designed by Westinghouse (WEC), and

45. UK EPR which is an evolutionary PWR designed by AREVA.

For the pre-licensing GDA process the Generic PCSR should include a full scope Level 1 and Level 2 PSA. A Level 3 PSA is also required but as details are site specific a high level outline analysis is acceptable.

UK AP1000 PSA and UK EPR PSA submitted for GDA are currently under review against ONR's expectations that can be found in the Safety Assessment Principles (SAPs) (see Reference [3]) and in the Technical Assessment Guide (TAG) on PSA (see Reference [7]).

The PSA Step 3 assessment strategy (see Reference [19]) identified SAPs FA.10 to FA.14 and Numerical Targets 7 to 9 as the relevant parts of that document. Attention has also been paid to relevant parts of the International Atomic Energy Agency (IAEA) standards (see Reference [20]) and the Western European Nuclear Regulators' Association (WENRA) reference levels (see Reference [21]). These PSA related SAPs, IAEA standards and WENRA reference levels are embodied and enlarged in ONR's TAG on PSA (see Reference [7]) and it is this guide that provides the principal means for assessing the PSA in practice (Level 1, 2 and 3 and the use of PSA to support decision-making).

Where numerical targets are given in the SAPs, ONR is seeking sufficient information for it to judge that the target is likely to be achieved and the overall risk is as low as reasonably practicable (ALARP). GDA is following a "Claims – Arguments – Evidence" structure as follows:

46. Step 2 was "claims" and for the PSA these were interpreted as approach, outline scope, criteria and output of the PSA.

47. Step 3 was “arguments” which were broadly interpreted as being the methods, techniques and detailed scope.

48. Step 4 has concentrated on the “evidence” and for the PSA this is the detailed implementation of the methods and techniques, and the data and parameters used to quantify the PSA.

Step 3 of the GDA has been completed and the reports have been published – see References [14] and [15] for the main reports, and [16] and [17] for the reports on the assessment of the PSA.

Following on from the GDA Step 3 review, Step 4 is currently looking at the application of the methods and techniques, and the data and parameters used to quantify the PSA. As well as the detailed review of all the technical areas of the PSA, a Risk Gap Analysis (RGA) has been undertaken that was designed to meet the following objectives:

49. Support to GDA conclusion whether the EPR or AP1000 are reactors that can be built and operated safely in the UK.

50. Evaluation of the importance of the findings of the GDA review in the various PSA technical areas.

51. Evaluation of the overall gap between the plant design risk claimed by designers and the risk contributors that may have been underestimated or omitted.

Following the unprecedented events in Japan, Chris Huhne (Secretary of State for Energy and Climate Change), has asked Mike Weightman (HM Chief Inspector of Nuclear Installations), to provide reports to the Government on the implications and any lessons to be learned for the UK. The reports will draw on similar work being undertaken by others, both nationally and internationally, and will be put in the public domain. As well as considering any implications for the UK’s existing nuclear sites, the reports will also inform the UK regulators’ assessments for the new nuclear build programme. Both industry and the regulators will need to take account of Mike Weightman’s recommendations. To take account of relevant recommendations from Mike Weightman’s interim report published in May 2011 (Ref. 22) and his final report expected in September 2011, ONR will not now draw conclusions from the GDA assessments in June 2011 as planned.

6. PSA methodology and data

In the UK, there are no specific PSA standards or guidelines and hence there are no prescribed methods for carrying out a PSA. However, much of the methodology used for the PSAs for the UK nuclear power plants has been derived from available international standards and guidelines. Much of this relates to light water reactors, so that it is not all applicable to the gas cooled reactors operated in the UK. An example of this is the methodology for carrying out a Level 2 PSA which is not applicable to gas cooled reactors. The methods used for the gas cooled reactor PSAs has used those aspects of current practice that are considered by the licensees to be applicable to their particular design of reactor.

6.1 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 – see References [9], [10] and [11] respectively. 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 used as references. More recent PSA guidance and standards are also being taken into account such as the IAEA Specific Safety Guides on Level 1 and 2 PSA – see References [12] and [13].

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 PSA considers quantitatively 170 Initiating Internal Faults and 6 Hazards (Seismic, Extreme Wind, Flooding, Fire, Aircraft Crash and Turbine Disintegration.)

The Level 2 PSA for Sizewell B includes containment event trees, thermal hydraulic analyses and source term analyses. Its phenomenological event trees consider steam explosions, hydrogen burns, direct containment heating, debris coolability, molten core-coolant interaction, natural circulation induced RCS failures, etc. The thermal hydraulic and source term analyses have been performed using MAAP 3B.

6.2 Common cause failure

Current approach

The current approach to modelling Common Cause Failure (CCF) in the PSAs for the nuclear power plants in the UK is to use the β -factor method. In this approach, the CCF of a set of redundant components is modelled using a single basic event that represents failure of all the redundant trains. The β -factors are derived using the Unified Partial Method (UPM) which is a structured expert judgment technique that takes account of a complete range of important influencing and conditioning factors regarding CCF events. In addition, CCF 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.

This method is relatively simple to implement since the CCF of a redundant system is modelled using a single basic event and is generally considered to be conservative since it assumes that all CCF events lead to failure of all the redundant components or trains of the system.

Although the safety systems in the UK NPPs have high levels of redundancy (generally four-fold redundancy) CCF makes a significant contribution to the frequency of Dose Band 5 (which corresponds to a release of radioactivity that leads to a dose of >1000 mSv at 1 km or at the nearest habitation if that is closer) and there is the concern that this approach could unduly influence the results of the PSA.

The UPM approach used to derive the β -factors is relatively easy to apply since the same framework can be used for all redundant safety systems and this provides an auditable trail for the derivation of the β -factors used in the PSA. However, the β -factor/UPM approach has a number of shortcomings as follows: judgements need to be made about the relative weighting of the CCF influencing factors; the numerical values provided by the UPM have not been calibrated to provide the justification that they are realistic; and the level of conservatism introduced is not known and could be very large for safety systems with a high level of redundancy.

To provide a more realistic model of CCF in the PSAs and to reduce the level of conservatism in the analysis, consideration is being given to moving towards one of the parametric models such as the α -factor model or the Multiple Greek Letter (MGL) model and work is being carried out to determine the feasibility of doing this as described below.

Work carried out on the use of detailed parametric models for CCF

Phase 1 - pilot study: A pilot study has been carried out where the β -factor/UPM approach was replaced by the MGL approach. The analysis was carried out for the boiler depressurization systems which carry out two functions: depressurisation of the boilers to allow low pressure feed from the LP Feed System and the Back-up Cooling System (BUCS); and vessel overpressure protection following a boiler tube failure. This

function is carried out by the Diverse Boiler Vent (DBV) and the Low Pressure Vent (LPV) valves. These are relatively simple systems with four-fold redundancy.

The basic events representing CCF were replaced by basic events for failure of any two, any three or all four trains of the system. The parameters used to quantify the MGL model have been derived from the Idaho National Laboratory (INL) CCF database which is derived from operating experience of light water reactors (LWRs) in the USA – see Reference [18].

The conclusions of the pilot study were that modelling CCF using the MGL approach gives a significant reduction in the failure probability of the boiler depressurisation function compared to the β -factor /UPM approach since this removes much of the conservatism inherent in the β -factor /UPM approach.

Phase 2 - review of current practice: A review has been carried out to determine what current practice is in modelling CCF in PSAs. This was done using a questionnaire, a literature review and discussions with PSA analysts.

The conclusion was that, for the majority of the PSAs included in the review, the current practice is to model CCF using one of the parametric models such as the α -factor or MGL methods. In most cases, the same approach is being used for all the CCF groups in the PSA; however, in some cases the α -factor or MGL model is being used for the most risk significant CCF groups combined with a simpler model (such as the β -factor model) for the less risk significant CCF groups. The most common way of including CCF in the PSA model is to define the CCF groups/ parameters and use the facility in current PSA software to define the equivalent fault tree model and to derive the CCF basic event probabilities. No specific difficulties were identified in the survey relating to the application of the α -factor or MGL model in a PSA, the quantification of the PSA or the interpretation of the results.

Operating experience data is being used to quantify the CCF parameters for the α -factor or MGL models. The most common sources of data are the data provided by NRC from the operation of LWRs in the USA. However, in some countries, operating experience data is being collected and used in the PSAs. In addition, the CCF data collected by ICDE is increasingly being used.

There are a number of ways of analysing the operating experience data to generate the parameters required for the α -factor or MGL models. The most common way is to use an impact vector approach. Many PSAs have used a Bayesian updating approach and many have taken account of the component testing regime.

At present, the α -factor model is the best to use if an uncertainty analysis is to be carried out for the PSA since performing an uncertainty analysis using the MGL model is considered to be problematic (if not impossible).

Phase 3 – use of RiskSpectrum for CCF modelling: The aim of the study was to use the automatic CCF modelling facility in RiskSpectrum PSA.NET to carry out the analysis for boiler depressurization/ vessel overpressure protection for the α -factor and MGL methods and compare the results obtained for the two analyses and with the results of the analysis carried out in the Phase 1 study.

The main conclusion reached was that the use of the automatic CCF modelling facility is relatively easy, transparent and allows the model to be easily updated when compared with putting CCF basic events into the model manually. This would be particularly efficient when modelling CCF in the large AGR models.

However, a problem was identified in that there were differences in the results of the analyses that, at the present time, have not been fully explained. It appeared that the INL data is not compatible with the way that the CCF probabilities being generated by RiskSpectrum and the reasons for this are being investigated.

Future work

Further work will be carried out on CCF modelling for the AGRs which presents a particular problem since there are components in the AGR designs that are not found in LWRs. The work to be carried out will: determine the extent to which the INL data can be used to model CCFs for the AGRs; consider the applicability of the INL data to UK plants; consider the extent to which ICDE data can be used; and set up a process to collect and analyse UK data on CCF.

6.3 Human reliability

Human Error Assessment and Reduction Technique (HEART)

The main techniques to quantify the Human Error Probabilities (HEPs) used in the PSAs for nuclear power plants (NPPs) in the UK has been HEART which was originally developed by J.C. Williams in 1985 as a structured approach that can be used to rapidly determine HEPs for tasks carried out in a range of industries. It was updated in the early '90s so that it provided a better fit for the range of tasks carried out at NPPs and has been successfully validated a number of times. HEART defines:

Generic Task Types (GTTs) - these are a set of pre-defined tasks with an associated HEP which would apply if the task was carried out under 'ideal' conditions;

Error Producing Conditions (EPCs) - these are aspects of the operating conditions which would lead to an increase in the probability of failure compared to the GTT; and

Assessed Proportion of Affects (APOAs) which relate to the proportion of the effect of the EPCs that applies for this specific task.

There are three steps in applying HEART: (i) select the appropriate GTT for the operator action being addressed; (ii) identify the EPCs and the APOAs; and (iii) calculate the HEP/ document the analysis.

Improvements proposed for HEART

A number of improvements to HEART have been proposed which aim to: provide greater transparency in the derivation of the GTT and EPC data; provide a better match between the assessment factors and those applicable to nuclear power plants; address the effects on human performance in situations where there are extended timescales; and provide better guidance on how to address dependencies.

In addition, it was intended to use the data on human error that has been collected since HEART was developed – in particular, the Computerised Operator Reliability and Error Database (CORE-DATA). This was set up in 1992 and has been maintained and updated continuously since then and is considered to be a mature human error database. It now contains more than 400 records of human error data from a range of industries including the nuclear industry. This was supplemented with relevant data from other sources.

Nuclear Action Reliability Assessment technique (NARA)

The aim has been to update HEART so that its strengths and ease of use are maintained, and to provide better underpinning using the human error data now available. This update is referred to as NARA.

Existing PSAs were examined to identify the HEP assessment needs of typical PSAs so that the technique could be tailored more to the nuclear industry. A re-defined set of GTTs was identified and re-quantified HEPs were produced based on the extended human error database. In addition, a new set of EPCs were produced for the updated technique, together with improved guidance for the assessed proportion of the

EPC to be applied. These EPCs have been quantified mainly by reviewing the original HEART data and carrying out an extensive literature review to extract relevant data.

Additional functionality was incorporated into NARA relating to accident sequences that occurred over long timescales since, for the UK gas cooled reactors, the fault sequences where there is a loss of decay heat removal after a reactor trip are characterized by long timescales for the restoration of core cooling. There is almost no data available relating to such scenarios. However, extensive research has been carried out in the UK based on expert judgement and this has been used to provide a basis for a method of quantification of the HEPs. Clear qualitative usage guidelines have been included in NARA so that the additional benefit of extra time could be applied consistently and not optimistically.

NARA defines an **Extended Time Factor** (ETF) where, if an operator action is initially unsuccessful, there may be ample time to detect the initial failure and try it again hence reducing the overall HEP. Four ETF bands have been defined with probabilities of 0.3, 0.1, 0.03 and 0.01. Determining the ETF is a three step process as follows: (i) determine the feasibility of an action being carried out in the longer timescale; (ii) determine the time available; and (iii) determine if the minimum requirements have been met for any of the ETF bands. These minimum requirements relate to five factors: the information available to carry out the required action; the scenario characteristics in terms of the time available and environmental conditions; the guidance and procedures available; the level of stress related to the environmental conditions and the consequences of actions to be carried out; and the training of plant operators and teams. The minimum requirement for all five factors for an ETF level need to be met before it can be claimed.

NARA also gives guidance on the identification of dependencies for the operator action being addressed which need to be taken into account in the quantification of the PSA model. However, this is not an integral part of the method).

NARA has undergone a series of reviews, which have been commissioned by ONR. However, in light of the on-going review process, ONR do not currently have a regulatory position on the suitability of NARA for application to nuclear risk assessment.

6.4 Availability assumptions

For the original Magnox and AGR PSAs the models considered that all plant is available – that is, 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 AGR PSA models have been enhanced as part of the PSR2 updates to include plant unavailability modelling, including 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 has always included unavailabilities due to maintenance.

6.5 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.

7. PSA applications

7.1 Risk Monitors

Risk Monitors at Heysham 2 and Torness

Risk Monitors have been in operation at Heysham 2 and Torness since 1986. These were based on the 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 rules covering safety system availability and a probabilistic analysis which is done using a fault tree model of the PSA that is solved for each plant configuration entered.

At Torness, compliance with the deterministic rules is assessed using the Essential Systems Outage Program (ESOP1) and a separate probabilistic assessment is carried out using LINKITT which contains the pre-solved cut-sets from the 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.

EDF Energy has more recently developed a more advanced tool called ESOP to replace the existing Risk Monitors. ESOP assists the operator by indicating whether or not the current plant configuration is compliant with the predetermined permissible plant configurations and, in parallel, carries out a risk evaluation using the Living PSA. It has a user-friendly interface and presents risk in a way that can be appreciated by the operators. ESOP retains a log of all changes in plant configuration and the results of operating rule compliance which is periodically reviewed to confirm satisfactory operation.

ESOP uses the updated PSAs which have been developed into four-quadrant models which correctly represent initiating events arising in each of the four quadrants (as required for a Risk Monitor application). These four-quadrant models are being maintained as Living PSAs. ESOP calculates risk using a full re-quantification of the PSA by RiskSpectrum which was the software used to develop the PSA model. However, the ESOP software has the same functionality as the earlier Risk Monitors so that it does not provide the wide range of functions that are available in current Risk Monitor software.

Risk Monitor at Sizewell B

A Risk Monitor is being used at Sizewell B which is based on Scandpower's RiskWatcher software and version V3.30 of the Living PSA.

The Risk Monitor is mainly used off-line by the work-week manager for maintenance planning purposes. A RiskWatcher run is undertaken to identify if there any high peaks in the risk for the outage plan for the coming week. In addition, RiskWatcher is updated the week prior to implementation of the plan with any unplanned outages to determine whether the plan requires amendment. If any issues are identified, the plan is reviewed in an ALARP manner using RiskWatcher.

All maintenance work is planned so that the plant is within the Tech Spec limits. RiskWatcher is used to identify the combinations of plant outages which, although within the Tech Specs, would result in a higher risk so that these combinations can be avoided. In addition, contingencies can be put in place to ensure that risk significant components can be identified and protected. It has also been used to risk inform the outage plan during the pre-outage planning process.

At present, the Risk Monitor is not used in the Control Room (CR), but there is interest from CR staff in implementing this.

RiskWatcher V1.22 can use a four band colour scheme to identify component outage combinations of increasing risk. However Sizewell B are still using the original three band structure (traffic lights), but have plans to move to a four band structure in the future (by addition of an orange band).

The RiskWatcher PSA model contains all six Tech Spec plant operating modes and these in turn are subdivided into further sub-modes depending on factors such as whether steam generators can be used or not.

The Risk Monitor is currently being updated with the latest version of the Living PSA (V3.40) which, amongst other developments, has removed some of the pessimisms associated with shutdown modelling and this is currently going through its validation process. In addition, the latest version of RiskWatcher software (V1.24) is being validated for use with the updated version of the Living PSA.

7.2 Risk Informed Technical Specifications

The original approach in the UK was to define Operating Rules and a Maintenance, Inspection and Test Schedule which are derived from the deterministic safety case to define the operational envelope of the plant. More recently all AGRs have implemented Technical Specifications for which the deterministic considerations have been supported by limited use of PSA insights.

Sizewell B has always had Tech Specs, 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 Sizewell B 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.

8. Results and insights from the PSAs

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.

8.1 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), a reactor pressure vessel (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:

- 52.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),
- 53.a Level 3 PSA for a range of internal initiators at power which forms part of the evidence presented to the Public Inquiry,
- 54.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, and
- 55.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 than 10^{-7} per year and the sum of all such fault sequences should be less than 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:

$$[\text{initiating event frequency}] \times [\text{safety system failure probability}] < 10^{-7} \text{ per year}$$

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 increase diversity:

- 56.a Secondary Protection System (SPS) using magnetic logic devices (LADDICS) which was diverse from the computer based Primary Protection System (PPS),
- 57.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,
- 58.the auxiliary feedwater system was replaced by two diverse systems one using electrical motor driven pumps and one using steam turbine driven pumps,
- 59.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
- 60.a seismically qualified air-cooled Reserve Ultimate Heat Sink (RUHS) to provide diversity from the seawater cooling system.

The PSA related design work led support to further changes to the SNUPPS design to increase reliability and segregation:

61.4 x 100% Essential Diesel Generators,

62.4 High Head Safety Injection (HHSI) pumps,

63.interchangeable Residual Heat Removal (RHR) and Containment Spray pumps - 4 Low Head Safety Injection (LHSI) pumps in total,

64.automatic switchover to recirculation mode for all safety injection pumps (HHSI+LHSI) on depletion of the Refuelling Water Storage Tanks (RWST),

65.4 x 100% Component Cooling Water System (CCWS) pumps, and

66.SEBIM valves to replace the pressuriser's Power Operated Relief Valves (PORVs) plus 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:

67.the provision of two battery charging diesels to give long term DC power for control and instrumentation following an extended loss of all AC power,

68.additional, diverse provisions for isolation of the containment mini-purge system,

69.changes to provide a Cavity Flooding System to provide better protection (basemat protection/ debris coolability) for the containment following a severe accident,

70.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

71.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 that would arise if the reactor coolant level was reduced to mid-loop level. The LPSA is regular updated to ensure that it correctly reflects the operational plant.

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	60%
- Mode 4 - Cooldown (SG or RHR)	2%
- Mode 5 - RCS intact (includes several operating states)	19%
- Mode 5 - RCS open-refuelling pool not filled	19%
- Mode 6 - Refuelling pool filled	0.1%

With the major contributors to the Core Damage Frequency being:

Major contributors to Core Damage Frequency	% Contribution
Design basis initiating faults	64% ⁽ⁱ⁾
Hazards	28% ⁽ⁱⁱ⁾
Beyond design basis initiating faults	8%

- (i) No initiating fault contributes >10% of Core Damage Frequency
- (ii) Seismic event is the most significant hazard

Currently the LPSA is being utilised by station support and operational staff to provide support to:

72.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);

73.the maintenance strategies, primarily for:

- battery maintenance,
- mid-loop operations, and
- RPV head seal replacement/repairs;

74.hardware modifications; and

75.the Surveillance Programme for Category 1 Motor Operated Valves (MOV).

8.2 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:

76.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,

77.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

78.the 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, and

79.the 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:

80.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),

81.provision of a Vessel Overpressure Protection Equipment (VOPE) 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),

82.enhancement to the fire hydrant system to provide an alternative heat sink for the Pressure Vessel Cooling Water (PVCW) system and installation of backup diesels for the PVCW pumps to provide diversity following loss of grid faults (Hinkley Point B),

83.installation of an Additional Feed System to provide increased post-trip cooling reliability, particularly following loss of grid faults and hazards (Dungeness B),

84.installation of an Electrical Overlay System to provide dedicated electrical supplies following hazards (Dungeness B),

85.enhancement of CO₂ and N₂ injection systems to provide enhanced post-trip cooling and shutdown capability (Dungeness B), and

86.enhancement of the Low Pressure Back Up Cooling System (LPBUCS) (which is the backup to the 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 since 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.

8.3 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:

87.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),

88.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,

89.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

90.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 their 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 ONR'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.

9. Future developments and research

Research in PSA and risk analysis is being carried out by both the licensees and ONR. The research has addressed issues that have arisen as a result of safety case submissions, developments in the state-of-the-art in PSA and its applications, operational matters and reviews that have been carried out of the PSAs that have been produced for the Periodic Safety Reviews.

The focus of much of the research has been to improve the existing PSAs. This includes research activities to support future PSA scope enhancements, improve the realism of the PSAs and make them suitable for a wider range of applications. It is recognised that there is a continuing need to improve PSA methods with the aim of having better and more complete PSAs so that they provide more effective support for safety related decisions at the nuclear installations.

EDF Energy is liaising with the wider EDF group on PSA research and development activities but this is at an early stage. They also keep abreast of issues being pursued by the Electric Power Research Institute (EPRI) and the PWR Owners Group since EDF Energy is a member of both. In addition, both the ONR

and the licensees have been involved in activities on PSA sponsored by international organisations such as IAEA, European Union and OECD/Nuclear Energy Agency (NEA). The main activities currently underway in the UK are described below.

Common Cause Failure modelling: The current method used in the PSAs is the β -factor method with the β -factors quantified using the Unified Partial Method (UPM). However, this approach is considered to be very conservative, requires judgements to be made by the PSA analyst and the method has not been calibrated. EDF Energy has been carrying out work on the use of the more detailed parametric methods such as the α -factor or Multiple Greek Letter (MGL) approach. So far this has included a pilot study for a small part of the PSA, a review of current international practice and a study using the CCF modelling capability of RiskSpectrum. Further work on this topic is ongoing.

International CCF Data Exchange (ICDE): The UK has contributed data to ICDE for a number of components and has been considering how this data can be used in the quantification of the CCF probabilities used in the PSAs.

Nuclear Action Reliability Assessment (NARA): The current approach for deriving the human error probabilities (HEPs) used in the PSAs is the Human Error Assessment and Reduction Technique (HEART). EDF Energy have been carrying out work to improve HEART so that it can be applied more easily to nuclear power plant tasks and takes account of recent research and operating experience data. This updated technique, referred to as NARA, uses the same approach as HEART to derive the HEPs for specific tasks. NARA has an additional functionality that relates to the tasks which can be carried out in an extended timescale (which is the case for loss of decay heat removal for the AGRs where the timescale to restore core cooling is long/ many hours). NARA is now a fully developed viable methodology for the quantification of HEPs. Further work is being carried out which includes: providing further underpinning of NARA, developing a computer programme and providing training.

Level 2 PSA for the AGRs: EDF Energy has been carrying out work to determine the feasibility of carrying out Level 2 PSAs for AGRs. A pilot study has been carried out for a limited number of sequences from the existing Hinkley Point B PSA, allocate them to Sequence Classes and make a more refined estimate of the frequency of the associated radiological releases. Further work is being undertaken to determine the overall benefits and reasonable practicability of carrying out a full Level 2 PSA for the AGRs.

Fuel route PSA for the AGRs: EDF have carried out a pilot study for the PSA for the refuelling and fuel handling operations for the Heysham 1 and Hartlepool AGRs which are currently refuelled off-load with the primary circuit depressurised. This used the same methods as for the internal events, at-power PSA with the PSA model being developed using RiskSpectrum. The event trees modelled the protection, mitigation and the factors that influence the magnitude of the off-site release. Fault trees were developed for the mechanical and electrical interlocks provided on the fuelling machine. The pilot study has indicated that the approach used for the internal events, at-power PSA can be used for the fuel route PSAs.

10. References

- [1] The Tolerability of Risk from Nuclear Power Plants; HSE Books 1992, ISBN 0 11 882043 5; available at <http://www.hse.gov.uk/nuclear/tolerability.pdf>
- [2] Safety Assessment Principles for Nuclear Plants; HSE Books 1992, ISBN 0 11 886368 1; available at <http://www.hse.gov.uk/nuclear/saps/saps1992.pdf>
- [3] Safety Assessment Principles for Nuclear Facilities; 2006 Edition, Revision 1; available at <http://www.hse.gov.uk/nuclear/saps/saps2006.pdf>

- [4] Numerical targets and legal limits in Safety Assessment Principles for Nuclear Facilities - An explanatory note; HSE Publications; available at <http://www.hse.gov.uk/nuclear/saps/explanation.pdf>
- [5] Reducing Risks, Protecting People - HSE's Decision Making Process; HSE Books 2001, ISBN 0 7176 2151 0; available at <http://www.hse.gov.uk/risk/theory/r2p2.pdf>
- [6] Transcript of Proceedings of the Hinkley Point C Inquiry; 1989 JL Harpham Ltd, 55 Queen Street, Sheffield S1 2DX.
- [7] Technical Assessment Guide - Probabilistic Safety Analysis; T/AST/030; available at http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast030.pdf
- [8] Technical Assessment Guide – Guidance on the Demonstration of ALARP; T/AST/005; available at http://www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast005.htm
- [9] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), IAEA Safety Series No 50-P-4, Vienna.
- [10] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), IAEA Safety Series No 50-P-8, Vienna.
- [11] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA Safety Series No 50-P-12, Vienna.
- [12] Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants; IAEA Safety Standards; Specific Safety Guide No. SSG-3, Vienna.
- [13] Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants; IAEA Safety Standards; Specific Safety Guide No. SSG-4; Vienna.
- [14] Report of the System Design and Security Review of the AP1000 Nuclear Reactor; HSE, November 2009; available at <http://www.hse.gov.uk/newreactors/reports/step3-westinghouse-public-report-gda.pdf>
- [15] Report of the System Design and Security Review of the UK EPR Nuclear Reactor; HSE; November 2009; available at <http://www.hse.gov.uk/newreactors/reports/step3-edf-areva-public-report-gda.pdf>
- [16] Generic Design Assessment Step 3 – Probabilistic Safety Analysis of the Westinghouse AP1000; Division 6 Assessment Report No. AR 09/017-P; HSE; available at <http://www.hse.gov.uk/newreactors/reports/step3-ap1000-probabilistic-safety-analysis-report.pdf>
- [17] Generic Design Assessment Step 3 – Probabilistic Safety Analysis of the EPR; Division 6 Assessment Report No. AR 09/027-P; HSE; available at <http://www.hse.gov.uk/newreactors/reports/step3-uk-epr-probabilistic-safety-analysis.pdf>
- [18] Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding; NUREG/CR-6268 (INL/EXT-07-12969); NRC; Sep 2007.
- [19] New Reactor Build Step 3 PSA Strategy. ONR Division 6 Assessment Report No. AR08/029, HSE, March 2008. TRIM Ref. 2008/317683; available at <http://www.hse.gov.uk/newreactors/reports/step3-uk-epr-probabilistic-safety-analysis.pdf>
- [20] Safety Assessment and Verification for Nuclear Power Plants; IAEA Safety Standards Series; Safety Guide NS-G-1.2; International Atomic Energy Agency (IAEA); Vienna; 2001.
- [21] Reactor Safety Reference Levels (Issue O); Western European Nuclear Regulators Association (WENRA); January; 2008.
- [22] Japanese earthquake and tsunami: Implications for the UK nuclear industry; Interim Report; HM Chief Inspector of Nuclear Installations; May 2011;

<http://www.hse.gov.uk/nuclear/fukushima/interim-report.htm>

Appendix B – CONTACT INFORMATION

Regulatory Authority / Technical Support Organisation	Direct Contact
<p>Office for Nuclear Regulation Redgrave Court Merton Road Bootle Merseyside, UK L20 7HS</p> <p>Tel: +44 (0)151 951 4000</p>	<p>Shane Turner and Ana Gomez-Cobo Redgrave Court Merton Road Bootle Merseyside, UK L20 7HS</p> <p>Contact details: Shane: Tel:+44 (0)151 951 3995 Email: shane.turner@hse.gsi.gov.uk Ana: Tel: +44 (0)151 951 4047 Email: ana.gomez-cobo@hse.gsi.gov.uk</p>
<p>Regulatory Authority Website Address:</p>	<p>www.hse.gov.uk/nuclear/index.htm</p>

21. USA

1. Introduction

Here, no contribution is expected from the participants.

2. PSA framework and environment

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 risk-informed 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 50.109²⁶ (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.”

²⁶ Code of Federal Regulations, Title 10, Part 50.109, “Backfitting.”

In issuing the policy statement, the Commission said it expected that implementation of the policy statement would improve the regulatory process in three ways: through safety decision making enhanced by the use of PRA insights; through more efficient use of agency resources; and through a reduction in unnecessary burdens on licensees. The movement toward risk-informed regulation has indeed sharpened the agency's (and, therefore, the licensees') focus on safety, reduced unnecessary regulatory burden, and resulted in 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 engineering considerations to focus regulatory and licensee attention on design and operational issues commensurate with their importance to public health and safety. A risk-informed approach enhances the traditional engineering 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 is Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes To The Licensing Basis." The Standard Review Plan (SRP) associated with RG 1.174 is SRP Chapter 19.2, "Review of Risk Information Used to Support Permanent Plant-Specific Changes to the Licensing Basis: General Guidance." These two documents 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 may be 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), and technical specifications (RG 1.177).²⁷ 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 categorizing structures, systems, and components according to their safety significance (“special treatment requirements”). RG 1.201 provides guidance on this risk-informed application; there is no corresponding SRP section. As another example, 10 CFR 50.48(c) provides an alternative, risk-informed and performance-based fire protection program. RG 1.205 and SRP 9.5.1.2 provide guidance on implementing this alternative to the traditional fire protection program. These risk-informed applications are 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, as well as new light-water reactors (LWRs) currently being licensed under 10 CFR 52. PRAs for these new LWRs indicate significantly lower risk profiles than currently operating reactors. Since many decisions regarding plant changes are based on the plant’s baseline risk, this presents the possibility that plant safety could be reduced during its operating lifetime through changes to the plant’s operations and licensing basis (RG 1.174). To address these concerns, in SECY-10-0121 the NRC staff has recommended identifying appropriate changes to the existing risk-informed guidance for changes to the licensing basis, including operational programs, and to the ROP.

Regarding advanced reactors (e.g., high-temperature gas-cooled reactors, liquid metal reactors, and small modular LWRs), the NRC staff has developed a plan to develop a regulatory structure for new plant licensing in NUREG-1860. 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 applications involving 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. The NRC’s expectations for the technical adequacy of a PSA are set forth in RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.” This is discussed further in Section 4.US.

Regarding new 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

²⁷ Note that RG 1.176, referred to in the 2007 version of this WGRISK survey report, has been made obsolete by the promulgation of 10 CFR 50.69 and the issuance of RG 1.201, and was withdrawn in 2008 (see Federal Register Notice 73 FR 7766, 2/11/2008).

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. Subsequently, 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 Section 7. 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 has benchmarked these models against licensee PSAs. These primarily 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-10-125 discusses the status of the Accident Precursor Program and the SPAR models as of 2010.

3. Numerical safety criteria

As a result of the recommendations from the President's Commission on the Accident at Three Mile Island (Kemeny 79), the NRC issued a safety goal policy statement (51 FR 30028) 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 (NUREG/BR-0058, used to support backfit analyses and rulemaking) and guidance for risk-informing reactor-related regulatory activities. The reactor Safety Goals broadly define an acceptable level of radiological risk to both individual members of the public and society at large. The goals consider the risk from nuclear power plant operation and reactor accidents. The goals do not address environmental considerations, worker protection, routine operation, sabotage, non-reactor activities, or safeguards matters.

The NRC is tasked with assuring adequate protection of the health and safety of the public. "Adequate protection" is the level of safety 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 impose enhancements to safety upon licensees, costs must be considered. The NRC's regulatory analysis must show that there is a substantial increase in the overall protection of the public health and safety or the common defense and security to be derived from the backfit and that the direct and indirect costs of implementation for that facility are justified in view of this increased protection. 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 (CDF) of 10^{-4} /reactor year and a subsidiary objective on large early release frequency (LERF) of 10^{-5} /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 CDF and conditional containment failure probability (CCFP) 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 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 (provided in a Staff Requirements Memorandum on SECY 90-016) introduces large release frequency (LRF) and CCFP metrics and associated goals, as well as design features to prevent and mitigate certain severe accidents.
- NRC Management Directive (MD) 8.3 uses risk criteria to aid in determining the extent of the NRC's response to nuclear plant incidents; i.e., whether to send out an incident investigation team and the type of team to send.
- 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. These results are used to determine the appropriate level of regulatory oversight (e.g., inspections) of a given licensee.

4. PSA standards and guidance

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 and maintenance of consensus standards and associated guidance.

Figure [4.2.1-1] shows the relationship between the standards, guidance documents endorsing these standards, and regulations. (Note that the guidance referred to in this section refers to guidance on determining the technical acceptability of a PSA. There are, of course, numerous sources of guidance on other PSA-related aspects, e.g., methods to perform specific PSA analyses. Some of these latter guidance documents are discussed in Section 6.US of this report.)

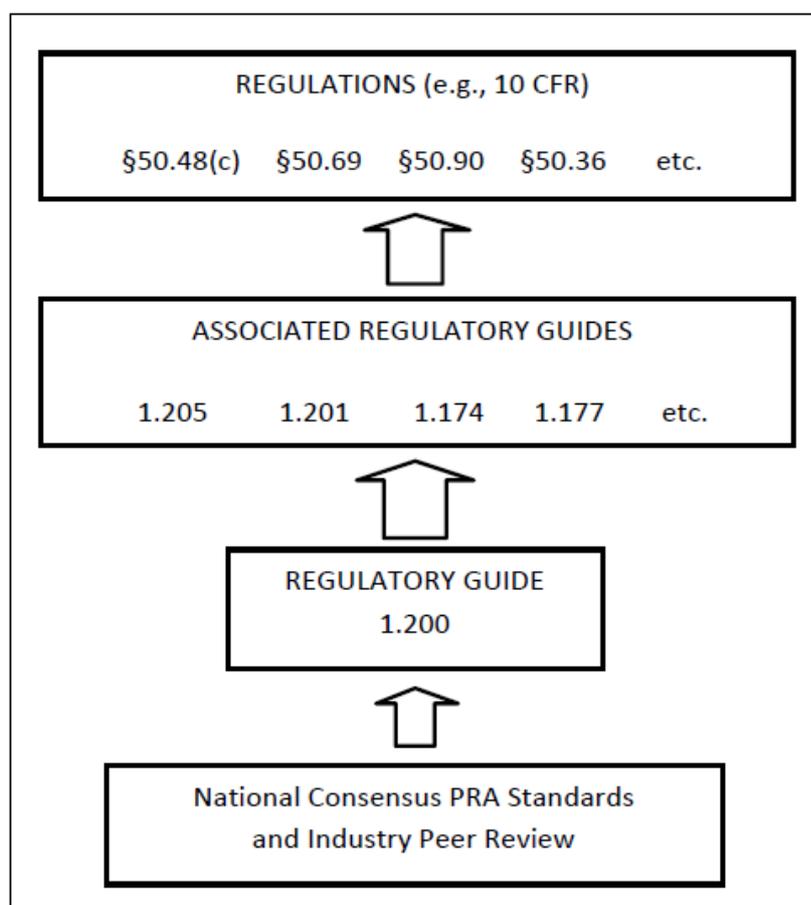


Figure [4.2.1-1]. Relationship of regulations, RGs, and standards for risk-informed activities (source: NUREG-1925, Rev. 1, Figure 5.4)

The top two levels of Figure [4.2.1-1] are discussed in Section [2.US] of this report. The third level, RG 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” provides the NRC staff’s position on one acceptable approach for determining the technical acceptability of a PSA²⁸. As summarized in NUREG-1925, RG 1.200 provides guidance on the technical acceptability of PSA by:

1. Establishing the attributes and characteristics of a technically acceptable PSA.
2. Endorsing consensus PSA standards and the industry peer review process.
3. Demonstrating technical acceptability in support of a regulatory application.

Regarding the attributes and characteristics of a technically acceptable PSA, RG 1.200:

- Defines the scope of a base PSA to include Level 1, 2, and 3 analyses, at-power, LPSD operating conditions, internal and external hazards to support operating reactors and new LWRs.
- Defines a set of technical elements and associated attributes that need to be addressed in a technically acceptable base PSA.
- Provides guidance to ensure that a PSA model represents the plant down to the component-level of detail, incorporates plant-specific experience, and reflects a realistic analysis of plant responses.
- Includes a process to develop, maintain, and upgrade a PSA to ensure that the model represents the as-built, as-operated (or as-designed) plant.

Regarding consensus PSA standards and the industry peer review process, RG 1.200:

- Allows the use of consensus PSA standards and peer reviews (as endorsed by the NRC in RG 1.200) to demonstrate the technical acceptability of a base PSA.
- Provides guidance for an acceptable peer review process and peer reviewer qualifications.
- Endorses the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PSA standard and the Nuclear Energy Institute (NEI) peer review guidance documents. The endorsement of the standard consists of staff objections and proposed resolutions. An application PSA needs to address the staff objections in RG 1.200, where applicable, if the PSA standard is to be considered met.

²⁸ An NRC Regulatory Guide provides one way that the NRC staff finds acceptable to meet a regulatory requirement. The staff recognizes that there may be alternate, equally acceptable ways.

Regarding regulatory applications, RG 1.200:

- Recognizes that the needed PSA scope (i.e., risk characterization, level of detail, plant specificity and realism) is commensurate with the specific risk-informed application under consideration.
- Some applications (e.g., extension of diesel generator allowed outage time) may only use a portion of the base PSA, whereas other applications (e.g., safety significance categorization of structures, systems, and components) may require the complete model.
- Demonstrates one approach for technical acceptability of a PSA, independent of application. Inherent in this definition is the concept that a PSA need only have the scope and level of detail necessary to support the application for which it is being used, but it always needs to be technically acceptable.

When used in support of an application, a major goal of RG 1.200 is to obviate the need for an in-depth review of the base PSA by NRC reviewers, allowing them to focus their review on key assumptions and areas identified by peer reviewers as being of concern and relevant to the application. Consequently, RG 1.200 is meant to provide for a more focused and consistent review process.

Regarding consensus standards and industry peer review (the fourth level in Figure [4.2.1-1]):

- The American Society of Mechanical Engineers (ASME) and the American Nuclear Society (ANS) have jointly published a combined standard, ASME/ANS RA-Sa-2009, addressing PSAs for operating LWRs. The scope of the standard includes a Level 1 (plus LERF) PSA for at-power conditions addressing both internal hazards (including internal floods and fires) and external hazards (seismic events, external floods, high winds, etc.). An addendum to this standard is expected to be published in 2011. This addendum will address issues with internal events, internal flood, internal fires, and seismic events. Extensions to ASME/ANS RA-Sa-2009 to address low-power and shutdown (LPSD) conditions and to support new LWRs are underway. Further, standards for Level 2 and Level 3 PSA, as well as PSA for non-LWRs, are under development.
- 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, which is incorporated by reference in 50.48(c), 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 addressed by ASME/ANS RA-Sa-2009, as indicated above.
- The Nuclear Energy Institute (NEI) has published NEI-00-02, "Probabilistic Risk Assessment Peer Review Process Guidance"; NEI-05-04, "Process for Performing Follow-on PRA Peer Reviews Using the ASME PRA Standard"; and NEI-07-12, "Fire Probabilistic Risk Assessment (FPRA) Peer Review Process Guidelines," which include a peer review process for Level 1 LERF PSA for internal events and internal floods, PSA updates and upgrades, and fire PSA, respectively. NEI revised NEI-07-12 in June, 2010.

Revision 3 to RG 1.200 is expected to be published in mid-2011 and is expected to endorse Addendum B to ASME/ANS RA-Sa-2009 and the June, 2010 revision to NEI-07-12.

5. Status and scope of PSA programs

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) for severe accident vulnerabilities. The scope of the IPEEE program included external events including seismic, high wind, external flooding, accidental aircraft crash, transportation, 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 that described the plant-specific PSA results and 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 alia 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 78 Standardized Plant Analysis Risk (SPAR) models representing the 104 operating commercial nuclear plants in the U.S. and has performed a limited scope validation and verification of these models against licensee PSAs and other studies. Model improvements are also identified on a continuous basis as the models are used (e.g., in reactor oversight applications, in special studies such as MSPI reviews), through cooperative research with the Electric Power Research Institute (EPRI), and through industry peer reviews. The NRC has also developed a SPAR model for the AP1000, is in the process of validating a SPAR model for an advanced BWR, and is in the process of developing a SPAR model for the U.S. Advanced PWR design.

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 PSA was performed to demonstrate PSA 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 LPSD 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. The NRC SPAR models were developed to provide risk models independent of those developed by the licensees using common methods and data.

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. For new reactors licensed under 10 CFR 52, each holder of a combined license is required to develop a Level 1 and a Level 2 PSA before initial loading of the fuel. The PSA must cover those initiating events and modes for which NRC-endorsed consensus standards on PSA exist one year prior to the scheduled date for initial loading of fuel. NRC's SPAR models are Level 1 PSAs; a small number of extended Level 1 models (to support LERF and Level 2 modeling) have also been developed.

Initiating events addressed

Most of the licensees' 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).

Some of the U.S. plant PSAs address seismic 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. Similarly, a number of past U.S. plant PSAs have addressed internal fire events; the others have used simplified approaches. Currently, about half of the U.S. plants are developing fire PSA models to support adoption of the risk-informed fire protection program under 10 CFR 50.48(c). Only a limited number of plants have performed PSAs for other external events (e.g., high winds, external flooding, accidental aircraft crashes). As discussed above, new reactors are required to address external events since the NRC staff has endorsed the latest combined ASME/ANS Standard on PSA.

NRC's SPAR models address general transients (including anticipated transients without scram), transients induced by loss of a vital alternating current or direct current bus, transients induced by a loss of cooling (service) water, loss-of-coolant accidents, and loss of offsite power. A number of models have been developed to address external events. Work is ongoing to develop models to address internal fires.

Modes of operation addressed

Most of the current licensee PSAs are limited to consideration of events occurring during full power operation. Only a few PSAs address events occurring during LPSD operation. Although consensus standards on LPSD operation have not yet been endorsed by the NRC staff, most new reactor designs have addressed these events in the PSAs using current best practices.

NRC's SPAR models are similarly focused on at-power operations. However, a number of LPSD models have been developed and are being used to support regulatory applications.

PSA updates

When used to support risk-informed regulatory applications, PSAs are required to reflect current plant conditions relevant to the application. For example, if a licensee implements a risk-informed fire protection program, the PSA it uses to evaluate risk is required to reflect the as-built, as-operated and maintained plant. However, NRC does not require periodic updates for currently operating reactors. For new reactors licensed under 10 CFR 52, each holder of a combined license is required to maintain and upgrade the PSA. The upgraded PSA must cover initiating events and modes of operation contained in NRC-endorsed consensus standards on PSA in effect 1 year prior to each required upgrade. The PSA must be upgraded every 4 years until the permanent cessation of operations.

As discussed earlier, the NRC's SPAR models undergo continuous improvement to address issues and needs identified from peer reviews or applications. The staff completes about a dozen routine model updates annually.

6. PSA methodology and data

Licensee and NRC PSA models for 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. 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.US, many of these models were created in response to GL 88-20. Also as discussed in Section 5.US, the NRC has developed Level 1 PSA models for all plants under the Standardized Plant Analysis Risk (SPAR) program and has benchmarked 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. The PSAs for new reactor design certification applications are only required to have an SMA, while new combined license holders are required to have a full seismic PSA at the time of initial fuel load. 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.US, 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.US, a number of activities are also underway to improve current methods, tools, and data.

Current approaches used for a number of PSA topics of interest can be summarized as follows.

Common Cause Failure: 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.

Human reliability analyses in current U.S. PSAs 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. These include: 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 failure likelihood index methodology (a modified version of the success likelihood index methodology – SLIM). These methods employ different approaches to the identification and treatment of factors affecting human performance. A number of these approaches have been assembled within the Electric Power Research Institute (EPRI) HRA calculator. NRC's SPAR models use the SPAR-H quantification method developed from THERP and ASEP. NRC has also used the ATHEANA method in some applications (e.g., the analysis of pressurized thermal shock scenarios). To support the application of the broad range of HRA methods, the NRC has developed a summary of HRA good practices, documented in NUREG-1792, and has evaluated a selected group of methods against these good practices (NUREG-1842). As described in Section 9.US, efforts are underway to collect and analyze empirical data (both operational and experimental) needed to improve confidence in the modeling and quantification of HFEs, and to address the issue of HRA diversity as related to NRC applications.

Fire PSA: Current guidance for performing fire PSA is documented in two reports jointly developed by NRC's Office of Nuclear Regulatory Research and EPRI: NUREG/CR-6850 (EPRI 1011989) and NUREG/CR-6850 Supplement 1 (EPRI 1019259). The reports, which build on lessons learned from the IPEEE program and subsequent fire-related research, recommend a general fire PSA framework and approach consistent with those used in past U.S. fire PSAs. Perhaps more importantly, they also provide improved guidance on the treatment of specific, difficult fire PSA issues (e.g., the identification and assessment of potentially significant fire-induced circuit failures). As described in Section 7.US, it is expected that a number of licensees will be updating their fire PSAs using these reports.

PSA 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.

To maintain its SPAR models, NRC collects data on the operation of nuclear power plants as reported in licensee event reports (LERs),²⁹ licensees' monthly operating reports (MORs), and the Institute of Nuclear Power Operations (INPO) Equipment Performance and Information Exchange System (EPIX). The data collected include component and system failures, demands on safety systems, initiating events, fire events, common-cause failures, and system/train unavailabilities. The data are stored in discrete database systems, including NRC's Reliability and Availability Data System (RADS), Common-Cause Failure Database, and Accident Sequence Precursor (ASP) Events Database. The SPAR model parameters are estimated using 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.

As shown in Figure 6.US-1, in addition to supporting the estimation of SPAR model parameters, the data input into the RADS database are used to verify and validate information used in the Mitigating Systems Performance Index (MSPI) Program (see Section 7.US), to review the efficiency and effectiveness of the MSPI, and to suggest improvements to the index. NRC's operational data collection efforts also support the Industry Trends Program (ITP), which trends such information as thresholds for initiating events; system, component, and common-cause failures; and ASP events.

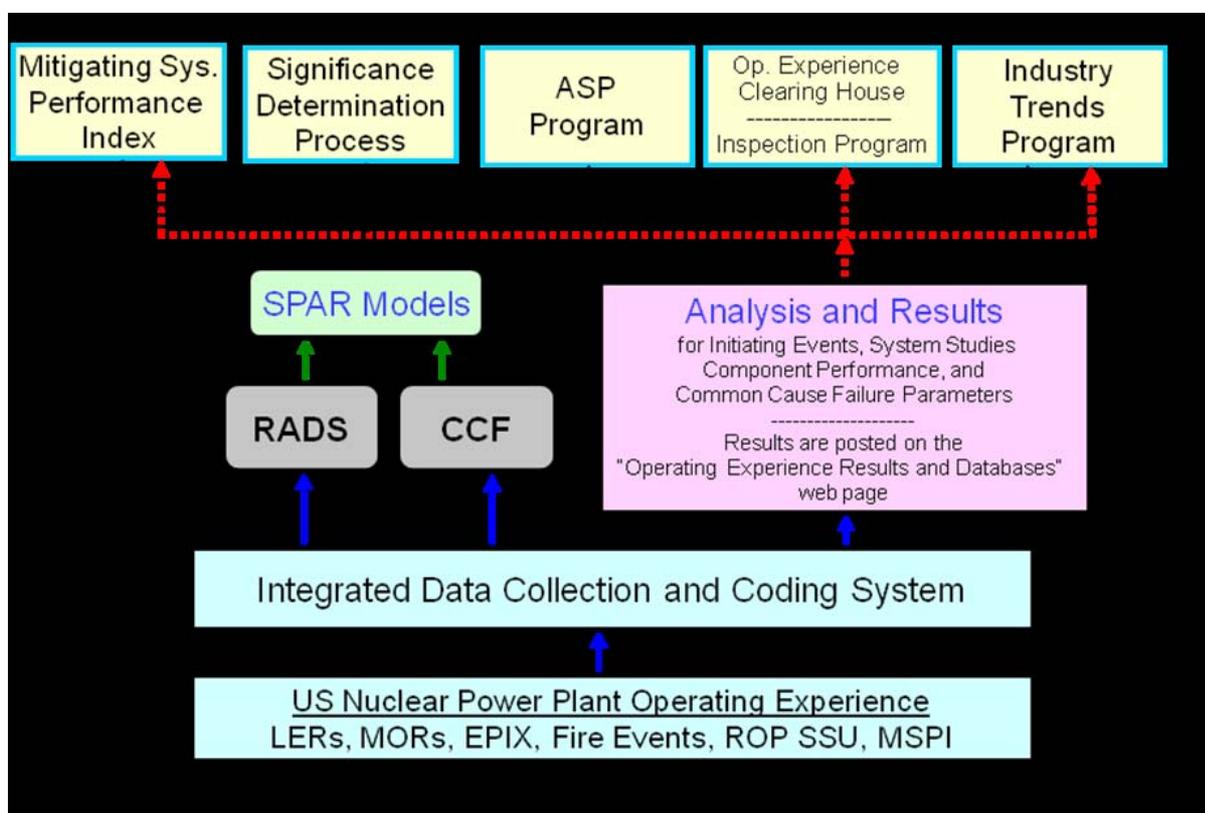


Figure 6.US-1. Sources and uses of operating data and analyses in NRC regulatory programs

²⁹LERs can be individually searched using the LERSearch program, accessible through the NRC's public web site: <https://nrcoe.inel.gov/secure/lersearch/index.cfm>. Current operating experience information can be found on NRC's Reactor Operating Experience Results and Databases web site (<http://nrcoe.inel.gov/results/>).

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 MSPI, which is one of the plant performance indicators used in NRC’s Reactor Oversight Program.

PSA for Reactor Oversight: As discussed in Section 7.US, the NRC staff performs risk assessments of inspection findings and reactor incidents to determine their significance for appropriate regulatory response. Currently, these assessments support the Reactor Oversight Program, Accident Sequence Precursor (ASP) Program, and Incident Investigation Program. To provide standard methods and tools for these programs, while recognizing differences in purpose among the programs, NRC has initiated a Risk Assessment Standardization Project (RASP). As discussed by Wong, et al., it is expected that RASP will promote improved consistency among NRC staff analyses. The major RASP activities include:

- developing standard procedures and methods for the analysis of internal events, internal fire and flooding events, external events, and shutdown events;
- providing enhanced-quality, integrated SPAR models for internal and external events, including shutdown events;
- enhancing the Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) code used to develop SPAR models; and
- providing technical support to NRC analysts.

7. PSA applications

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.

Use of PRA during Plant Operation and Oversight

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.

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 (internal events at power only) to be used in the calculation of the index.

Additional information can be found at: <http://www.nrc.gov/reactors/operating/oversight.html>.

Maintenance Rule – 10 CFR 50.65: The Maintenance Rule requires licensees to assess and manage the risk of maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance). The risk assessment addresses the increase in risk that may result from the proposed maintenance activities. The licensee must assess and manage the risk of maintenance activities performed during all conditions of plant operation, including normal shutdown operations. While the risk assessment may be qualitative or quantitative, most licensees use their plant-specific PSA when assessing the risk of maintenance activities performed during power operation. Many licensees use a risk monitor to quickly evaluate the risk of a specific plant configuration that results from taking equipment out of service to perform maintenance.

Incident Investigation: As part of the NRC's Incident Investigation Program performed following NRC Management Directive (MD) 8.3, the NRC staff uses PSA models to support decisions regarding the appropriate response to a reported incident. Conditional Core Damage Probability (CCDP) is calculated and is considered along with other factors (including uncertainty of the results) when determining the type of inspection team to send with a higher CCDP generally leading to a larger, more thorough inspection team. Risk insights from the PSA models are also used in considering the number of inspectors to send, their expertise, and the areas of focus.

Accident Sequence Precursor Analysis: The NRC established the Accident Sequence Precursor (ASP) Program in 1979 in response to NUREG/CR-0400, "Risk Assessment Review Group Report," issued September 1978. The ASP Program systematically evaluates U.S. nuclear power plant operating experience to identify, document, and rank the operating events most likely to lead to inadequate core cooling and severe core damage (precursors), given the likelihood of additional failures. The operating events can involve either an initiating event (e.g., a reactor trip or a loss of offsite power) with any subsequent equipment unavailability or degradation, or a degraded plant condition indicated by unavailability or degradation of equipment without the occurrence of an initiating event.

ASP analyses utilize information obtained from: (1) inspection reports and 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.

Using PSA results and perspectives to identify possible changes to NRC's reactor safety requirements

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.

New reactor design certification: Each design certification (DC) application must include a separate document entitled “Applicant’s Environmental Report - Standard Design Certification,” which must address the costs and benefits of the severe accident mitigation design alternatives (SAMDA), and the bases for not incorporating SAMDA in the design to be certified. The DC application for a light-water reactor design must contain a final safety analysis report (FSAR) that includes a description and analysis of design features for the prevention and mitigation of severe accidents, e.g., challenges to containment integrity caused by core-concrete interaction, steam explosion, high-pressure core melt ejection, hydrogen combustion, and containment bypass. Similar regulations pertain to combined license applications.

Risk-informed categorization (also referred to as “special 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.

Combustible gas control (10 CFR 50.44): 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.

Emergency core cooling system requirements (10 CFR 50.46): 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.

On July 29, 2005, in response to SECY-05-0052, "Proposed Rulemaking for 'Risk-Informed Changes to Loss-of-Coolant Accident Technical Requirements,'" the Commission directed the NRC staff to publish for public comment a proposed rule adding a new Section 50.46a, "Alternative Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors" to 10 CFR Part 50.

Current light-water reactor licensees could voluntarily adopt these requirements, which are intended to give licensees additional flexibility to change the designs of reactor ECCS. The proposed rule divides the current spectrum of LOCA break sizes into two regions. The division between the two regions is determined by a "transition" break size (TBS). The first region includes small 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 of the largest reactor coolant system pipe. Pipe breaks in the smaller break size region are considered more likely than pipe breaks in the larger break size region. Consequently, each region is subject to ECCS requirements commensurate with the relative likelihood of breaks in that region. LOCAs in the smaller break size region will continue to be considered "design basis accidents" and will be analyzed by current design basis accident methods, assumptions, and acceptance criteria. LOCAs in the larger break size region must also be mitigated, but they may be analyzed with more realistic analytical methods and initial conditions without postulating the loss of offsite power or the worst case single failure.

The staff published the proposed rule in the Federal Register on November 7, 2005 (70 FR 67598). The

public comment period ended on March 8, 2006. The staff held two public stakeholder meetings to provide for enhanced public participation on this rulemaking. As a result of these interactions, the staff made changes to the draft rule language with the objective of reducing burden on licensees while maintaining adequate protection of public health and safety.

On October 16, 2006, the staff sent draft final rule language for risk-informing 10 CFR 50.46 and the draft Federal Register notice for the final rule to the NRC's Advisory Committee on Reactor Safeguards (ACRS) for review. The staff met to discuss the rule with the ACRS subcommittee on October 31 and with the full committee on November 1, 2006. After these meetings the ACRS issued its letter dated November 16, 2006.

The ACRS letter recommends that the final 10 CFR 50.46a rule not be issued in its current form.

The staff issued SECY 07-0082 on March 16, 2007. The SECY informed the Commission of the impacts of the ACRS recommendations on the draft final rule, sought Commission clarification on its direction regarding defense-in-depth considerations for beyond transition break size LOCAs, and sought a decision on the staff's recommended option for proceeding with the rule.

In response to SECY 07-0082, the Commission directed the staff to address the ACRS issues and provided additional Commission guidance. As the NRC modified the rule in response to the ACRS recommendations and the Commission's direction, the NRC staff made many substantive changes to the requirements. After considering the extent of these changes, the NRC decided to provide an additional opportunity for public stakeholders to review and submit comments on the revised rule language. The NRC published the supplemental proposed rule on August 10, 2009 (74 FR 40006). On August 18, 2009, NEI requested a 120-day extension to the public comment period. The NRC granted the extension request by extending the comment period for all stakeholders until January 22, 2010. The NRC evaluated public comments received on the supplemental proposed rule and prepared a draft final rule which was made publicly available on May 12, 2010, and posted on www.regulations.gov. The NRC held a public meeting on June 4, 2010, to discuss resolution of public comments and the draft final rule language with stakeholders. The NRC then prepared the final rule. The NRC staff conducted its final briefings of the ACRS subcommittee and full committee on September 22 and October 7, 2010, respectively. In its October 20, 2010, letter, the ACRS recommending publishing the rule but expressed some reservations about how the rule might be applied to new reactor designs. In SECY-10-0161 dated December 10, 2010, the NRC staff provided the proposed final rule to the Commission for approval. A Commission brief on the proposed final rule is scheduled in early 2011.

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. The existing regulations establish screening limits that were developed based on what NRC believed to be a conservative probabilistic fracture mechanics analysis. Several licensees will exceed the screening limits in the current rule during their license renewal periods. The staff proposed to provide alternate fracture toughness requirements which reflect the updated technical basis in the proposed 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. The proposed rule was to amend the Commission's regulations (§ 50.61) that protect against brittle fracture of reactor vessels during severe cooldown events.

The NRC has been engaged in a research program to reevaluate and update the technical basis of the risk of throughwall cracking due to PTS, and recommends that the regulations be amended to reflect the updated technical basis. Revising the PTS requirements would permit some reactor vessels that are approaching the current maximum permissible level of embrittlement to postpone permanent shutdown. Current regulations allow licensee to avoid shutdown if they perform a safety analysis to show that operation with a PTS higher than the screening criteria is safe, or that they anneal the reactor vessel.

The staff issued SECY 07-0104 "Proposed Rulemaking — Alternate Fracture Toughness Requirements for Protection against Pressurized Thermal Shock Events (RIN 3150-AI01)" on June 25, 2007. On September 11, 2007, the Commission approved publication of a proposed rule, 10 CFR 50.61a, "Alternative Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events," for a 75-day public comment period. The staff published the proposed rule for public comments in the Federal Register on October 3, 2007 (72 FR 56275). During the development of the PTS final rule, the staff determined that several changes to the proposed rule may be needed to adequately address issues raised in stakeholder's comments. The staff published a supplemental proposed rule for public comment on proposed modifications that may not represent a logical outgrowth from the October 2007 proposed rule's provisions in the Federal Register on August 11, 2008 (73 FR 46557). The comment period for the supplemental proposed rule closed on September 10, 2008. The staff completed the final rulemaking package and in its SRM on SECY-09-0059, Final Rule Related to Alternate Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock Events (10 CFR 50.61a) dated September 22, 2009, the Commission directed the staff to make some minor changes to the rule and issue it in the Federal Register. The Final Rule was issued on Monday, January 4, 2010 (75 FR 00013).

Licensing actions

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 National Fire Protection Association (NFPA) 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 well-defined fire protection licensing bases and enables licensees to manage their fire protection programs with minimal regulatory intervention. To support implementation of the rule, NEI developed NEI 04-02, "Guidance for Implementing a Risk-Informed, Performance-Based Fire Protection Program under 10 CFR 50.48(c)," Rev. 2, and NEI 00-01, Rev. 2, "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," Rev. 1, with exceptions and clarifications.

Currently, as documented in a February 17, 2011, ACRS letter , two plants have transitioned their fire

protection programs to meet the requirements of 50.48(c) and 30 other sites (with 50 nuclear units) have indicated their intent to make this transition. Supporting guidance for performing fire PSA in this application is provided in NUREG/CR-6850 (EPRI 1011989) and in Supplement 1 to that document, as discussed in Section 6.US.

Risk-informed technical specifications (RITS): 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 is following 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 hot shutdown instead of cold shutdown as the preferred end state for technical specification actions; 2) increase the time allowed to delay entering required actions when a surveillance is missed; 3) modify existing mode restraint logic to allow the use of 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) replace fixed surveillance frequencies with a licensee-controlled program to permit optimization of surveillance frequencies; 6) modify selected LCO 3.0.3 actions for low risk systems to allow a 24-hour period prior to the required shutdown; 7) define actions to be taken when equipment is not operable due to unavailability of seismic snubbers or hazard barriers; and 8) risk-inform the scope of the TS rule. All initiatives have been completed and are in the implementation phase, except initiative 8 for which there is no current activity.

Risk-informed in-service inspection (RI-ISI): 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.

The NRC has also approved RI-ISI programs based, in part, on ASME Code Case N-716, *Alternative Piping Classification and Examination Requirements, Section XI Division 1*. This code case identifies sections of systems that are generically considered high-safety-significant (HSS), and relies on a flooding PSA to identify any additional, plant specific HSS segments. The NRC is completing its review of EPRI Topical report 1021467, *Nondestructive Evaluation: Probabilistic Risk Assessment Technical Adequacy Guidance for Risk-informed Inservice Inspection Programs* that specifies the quality of the flooding PSA that the staff finds acceptable to use in RI-ISI programs. NRC may endorse the Code Case in RG 1.147, with limitations and conditions (e.g., that the quality of the PSA is acceptable as measured against the EPRI Topical) where appropriate.

Risk-informed in-service testing (RI-IST): 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 a couple of other applications, generally of limited scope. RI-IST was applied at a limited number of facilities because, in part, each test interval change required review and approval by the NRC. Currently, the TechSpec surveillance testing initiative (see RITS Initiative 5, above) provides greater flexibility in selecting test intervals by licensees without the need for NRC review and approval of every change. As a result, no license applications are anticipated to request to implement a RI-IST program.

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.

In 2008, the NRC staff endorsed the NEI industry guideline NEI 94-01 Revision 2-A, Industry Guideline for Implementing Performance-Based Option of 10 CFR Part 50, Appendix J and a supporting Electric Power Research Institute (EPRI) technical report EPRI Report No. 1009325, Revision 1, December 2005, "Risk Impact Assessment of Extended Integrated Leak Rate Testing Intervals. The NRC staff is currently processing ILRT interval extension of up to 15 years based on these endorsed methodologies.

8. Results and insights from the PSAs

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.

- 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.
- 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.

- 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.
- 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 IPEEs 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.
- 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.
- For new LWR designs, Dube reports that that the risk as measured by CDF and LRF is substantially lower than the fleet of currently operating plants by one or more orders of magnitude. For all new LWR designs, the contribution of anticipated transients without scram (ATWS), interfacing systems loss-of-coolant accidents (ISLOCA), and station AC blackout (SBO) on an *absolute* (per reactor-year) scale are low because of features specifically designed to address these events.

Moreover, Dube notes that one can observe a clear distinction in the risk profiles between the passive designs (e.g., AP1000 and ESBWR), and those employing more conventional active mitigation systems (e.g., ABWR, U.S. EPR, and US-APWR). The passive designs tend to have a risk profile with balanced contributions from LOCAs and transients. There is minimal dependence on support systems, and offsite power is of low importance. Passive component failures tend to have the highest FV importance measures.

On the other hand, the risk profiles for some of the new active designs are shown to mirror IPE results to some extent. For example, the *relative* (percent) contribution of support system initiators such as loss of component cooling water to CDF, the importance of heating, ventilation and air-conditioning (HVAC) as a support system, and the large impact of reactor coolant pump (RCP) seal LOCAs tend to resemble the risk attributes of operating plants in many regards.

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.

9. Future developments and research

As described in SECY-07-0074, in order to support and integrate its ongoing efforts to risk-inform its regulatory processes, the NRC established the Risk-informed and Performance-based Plan (RPP) as a replacement and enhancement of its Risk-Informed Regulation Implementation Plan. The RPP is designed to coordinate the NRC's strategy to risk-inform regulatory activities in the arenas of reactor safety, materials safety, and waste management. Additionally, the RPP calls for: evaluating which risk-informed initiatives should be continued, which should be retired, and what new initiatives are needed; performing effectiveness reviews for completed activities; and providing a database of ongoing initiatives on the NRC's public website. The RPP is updated annually; the updating process includes updating the website database and associated documents, including a description of recent and near term projected accomplishments.

The October, 2010 version of the RPP is available in SECY-10-0143. The RPP database as well as general information on the NRC's use of risk in regulation can be obtained from NRC's website:

<http://www.nrc.gov/about-nrc/regulatory/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 intended to enhance the safety and improve the economics of existing and future nuclear power plants. As stated on the EPRI website (<http://portfolio.epri.com/ProgramTab.aspx?sId=NUC&rId=184&pId=5434>), these activities include: work on the refinement of PSA models to guide effective design, operation, and asset management decisions for critical plant issues; performance of technical analyses supporting continued regulatory acceptance of risk-informed activities; the development of analytical and software tools for safety evaluations, configuration risk management, fault tree analysis, and security assessments; and work supporting the development of a larger pool of trained nuclear risk professionals. . Current specific activities include: continued development of the next generation of risk professionals through its Education of Risk Professionals course; computer-based training overview of PSA fundamentals and risk-informed regulation suitable for management and the end users of risk information; update of EPRI's Safety and Operational Benefits of Risk-Informed Initiatives report (EPRI 1016308); and continued improvements and enhancements of PSA and risk technology, most notably in the fire and seismic hazard areas.

The remainder of this section addresses some noteworthy examples of ongoing developmental activities.

PSA Models

As discussed in Section 4.US, the NRC and industry are continuing to make a significant effort to develop PSA guidance documents (including consensus standards and regulatory guides) as well as supporting technical reports. Previously, this work was performed for operating reactors under the "Plan for the Implementation of the Commission's Phased Approach to Probabilistic Risk Assessment Quality" detailed in SECY-04-0118. Publication of revisions 2 of RG 1.200 in March, 2009 completed the final phase of the plan, which did not cover new reactors. With this work completed, it is expected that the industry will

have full-scope (i.e., internal and external hazard) PSAs that are fully quantified and are reviewed and approved by NRC. It is expected that the effort will, among other things, result in improved and more complete PSA models.

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: Support System Initiating Events, Loss of Offsite Power/Station Blackout, Uncertainty, Human Factors, TH Calculations, and Seismic.

PSA Data

The NRC's routine data collection and analysis activities are described in Section 5.US of this report. On the developmental side, the NRC's Office of Nuclear Regulatory Research (RES) is continuing its work on 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, which is summarized in NUREG/CR-6903, has developed a data framework aimed at addressing the issues of sparse and imperfect empirical data.

In the area of fire PSA, RES and EPRI are jointly updating the fire events database supporting NUREG/CR-6850 / EPRI 1011989. The work centers on the updating of fire ignition frequencies based on recent data, and the transitioning of frequency estimates from a plant basis to a component basis. The work also involves additional information collection and validation for events that have occurred. RES is also supporting an expert elicitation effort aimed at developing probabilities for fire-induced electrical short circuits in direct current cables.

Modeling of Physical Processes to Support PSA

To improve the realism of PSA models, RES, industry, and the U.S. Department of Energy (DOE) are working on a number of efforts involving the use of phenomenological models in PSA. Most of the work is aimed at coupling these models into event sequence analyses; some of the longer-term work presumes direct use of the models in a sampling-based analysis framework.

In the area of success criteria, RES is completing a study of the success criteria used in NRC's SPAR models. To date, the study has investigated: small-break loss-of-coolant accidents (dependency on aligning the emergency core cooling system water source to the containment sump); feed-and-bleed decay heat removal (the minimum number of pressurizer power-operated relief valves and high-head pumps needed); spontaneous steam generator tube rupture (time available for operators to mitigate the accident before core damage); station blackout (time available to recover power); and medium and large loss-of-coolant accidents (minimum equipment needed to prevent core damage). Ongoing and planned future work include: the development of a NUREG report documenting these analyses; implementing the results of the analyses in appropriate SPAR models; developing additional MELCOR³⁰ plant models for future analyses; investigating Level 1 PRA end-state issues (e.g., the relative conservatism of common core damage surrogates); and collaboration with external stakeholders.

In the area of fire PSA, RES, in concert with EPRI and the U.S. National Institute of Standards and Technology (NIST), completed a verification and validation study of a number of fire models in 2007. This study is documented in NUREG-1824. More recently, RES performed a Phenomena Identification and Ranking Table (PIRT) exercise to identify needed fire modelling capabilities (NUREG/CR-6978), and, together with NIST, developed and benchmarked a simple cable damage model for use in general purpose

³⁰ MELCOR is a computer code used to analyze severe accidents in nuclear power plants.

fire models. RES is continuing to work with EPRI and NIST to develop technical guidance to support fire modelling for nuclear power plant scenarios.

In the area of seismic PSA, RES, DOE, and EPRI, are characterizing the seismic sources for the Central and Eastern United States and, in conjunction with the U.S. Geological Survey (USGS), developing new, state-of-the art ground motion prediction equations. This work is a follow-up to a project, conducted by the Pacific Earthquake Engineering Research Center, which focused on the western United States. RES is also developing practical guidelines for implementing the Senior Seismic Hazard Analysis Committee (SSHAC) framework for performing probabilistic seismic hazard analysis, as documented in NUREG/CR-6372. This project will capture lessons learned during recent SSHAC Level 3 and 4 projects, and will also address the treatment of new information.

Regarding other external events, RES is working with the USGS and the National Oceanic and Atmospheric Administration (NOAA) to develop models for tsunami generation and propagation and explore probabilistic tsunami hazard assessment methods. RES is also working on models for extreme precipitation and storm surge. Although this work is aimed at determining design-basis flood levels, consideration is also being given to the treatment of uncertainties and the development of probabilistic approaches that should be useful in PSA.

In the area of Level 2 PSA, as discussed further below, RES is investigating the feasibility of a dynamic event tree approach that uses MELCOR in conjunction with the IDAC dynamic operator response model (developed at the University of Maryland) in the generation and analysis of scenarios.

In the area of passive components performance, RES and DOE are developing phenomenological models for material degradation intended to support risk-informed decision making. The RES effort, which is aimed at assessing the probability of rupture for reactor coolant system components, is intended to consider all contributing degradation mechanisms and the uncertainties in these contributions. The DOE effort is aimed at supporting life extension for operating plants.

PSA Methods

Human Reliability Analysis (HRA)

Recognizing the diversity of methods currently available to perform HRA, RES, supported by EPRI, is working on a project aimed at identifying either a single method for NRC applications or guidance on which method(s) should be used in which circumstances. This project, which was initiated in response to a November 8, 2006, memorandum from the Commission (SRM-M061020), is pursuing a formalization approach and a quantification tool capable of performing HRA in a consistent and efficient manner. The formalization approach incorporates behavioral science knowledge by providing decompositions of human failures, failure mechanisms, and failure factors that reflect both PSA-relevant contextual information and findings from scientific papers documenting theories, models, and data of interest. For quantification, the project uses a conventional PSA conditional probability framework, delineated to a level adequate for associating the probability of a human failure event with conditional probabilities of the associated contexts, failure mechanisms, and underlying factors (e.g., performance shaping factors). It is anticipated that the methodology will be developed and available for public review and comment by late 2011.

Fire PSA

As discussed in Section 7.US, a number of plants are risk-informing their fire protection programs, supported by fire PSA guidance provided in NUREG/CR-6850 (EPRI 1011989) and Supplement 1 to that document. Observing the application of this guidance in developing fire PSAs for these plants, industry has identified a number of areas where improvements could lead to more realistic results. The Nuclear

Energy Institute (NEI) has recently developed a research roadmap to address a broad range of topics (including fire event data characterization, fire severity characterization, detection and suppression, fire growth and damage modelling, fire-induced circuit failures, HRA, and PSA plant modeling). Currently, EPRI is working with RES on a joint project to update and improve the fire events database used for NUREG/CR-6850 (EPRI 1011989). Initially, fire ignition frequencies will be updated; however, other applications are also envisioned. RES is also developing fire PSA methods for low power and shutdown conditions, with EPRI as peer reviewers, and RES and EPRI are jointly developing a methodology and associated guidance for fire HRA. The latter will be documented in a final report published in early 2011.

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. RES is undertaking a research project whose objective is to identify and develop methods, analytical tools, and regulatory guidance to support (1) nuclear power plant licensing decisions using information on the risks of digital systems and (2) inclusion of models of digital systems in PRAs of nuclear power plants.

Previous RES projects have identified a set of desirable characteristics for reliability models of digital systems and have applied various probabilistic reliability modeling methods to an example digital feedwater control system. The results of these benchmark studies have been compared to the set of desirable characteristics to identify areas where additional research might improve the capabilities of the methods. RES is currently reviewing quantitative software reliability methods and plans to develop one or two technically sound approaches to modeling and quantifying software failures in terms of failure rates and probabilities. Assuming such approaches can be developed, they will then be applied to an example software-based protection system in a proof-of-concept study.

The results of the benchmark studies have also highlighted the following areas for which enhancement in the state of the art for PRA modeling of digital systems is needed:

- approaches for defining and identifying failure modes of digital systems and determining the effects of their combinations on the system;
- methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures;
- better data on hardware failures of digital components, including addressing the potential issue of double-crediting fault-tolerant features, such as self-diagnostics;
- better data on the common-cause failures (CCFs) of digital components;
- methods for modeling software CCF across system boundaries (e.g., when there is common support software);
- methods for addressing modeling uncertainties in modelling digital systems;
- methods for human reliability analysis associated with digital systems;
- process for determining if and when a dynamic model of controlled plant processes is necessary in developing a reliability model of a digital system

Advanced PSA Methods

As discussed above, RES is investigating the feasibility of a dynamic event tree approach for Level 2 PSA. This approach is intended to: reduce reliance on unnecessary modeling simplifications and surrogates (i.e., more phenomenological); address methodological shortcomings identified by NRC's State-of-the-Art Reactor Consequence Analysis (SOARCA) project; improve the treatment of human interaction and mitigation; make the analysis process and results more scrutable; leverage advances in computational capabilities and technology developments while remaining computationally tractable; and allow for ready production of uncertainty characterizations. The dynamic event tree approach was selected as the result of a scoping study, which considered a variety of approaches ranging from traditional, static event tree oriented methods to sampling-based simulation methods.

Currently, RES, Sandia National Laboratories, the University of Maryland, and the Ohio State University are developing a tool that uses the MELCOR accident analysis program in conjunction with a dynamic operator response model. (Figure 9.US-1 illustrates a potential scheme for combining existing computer programs in a manner that facilitates dynamic accident simulation.) The initial development, including application of the approaches to a demonstration problem, is scheduled to be completed in 2011.

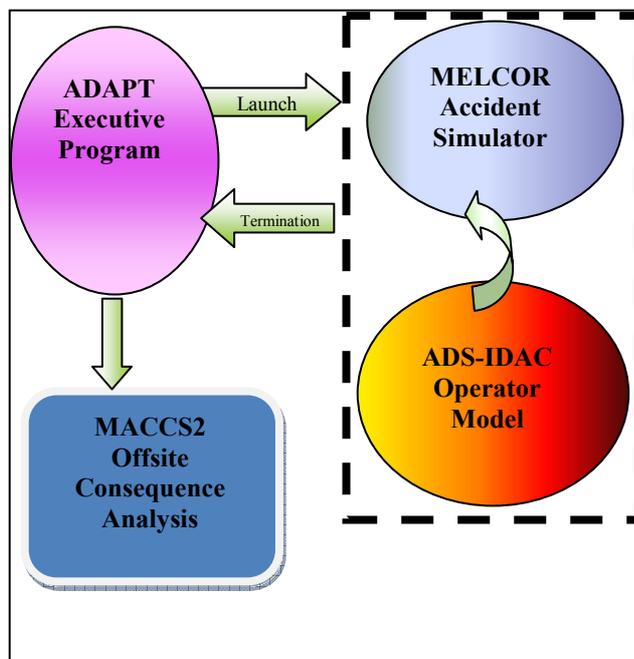


Figure 9.US-1. Sample high-level code coupling scheme (source: NUREG-1925, Rev. 1, Figure 5.14)

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. In March, 2009 the NRC published NUREG-1855, "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making." This NUREG covers the treatment of parameter, model and completeness uncertainties for internal events and internal floods in at-power operating reactors

including calculations of CDF and LERF. A revision of NUREG-1855 including internal fires, seismic, LPSD and Level 2 is expected to be completed in 2011. This work is being coordinated with EPRI

Comprehensive Site Level 3 PSA

Although Level 3 PSAs are required to directly estimate the risk to the public from nuclear power plant accidents, the NRC does not routinely use them in risk-informed regulation. In fact, NRC-sponsored Level 3 PSAs have not been conducted since the late 1980s. These Level 3 PSAs were documented in a collection of NUREG/CR reports and a single corresponding summary document, NUREG-1150. The NUREG-1150 study provides a set of PSA models and a snapshot-in-time (circa 1988) assessment of the severe accident risks associated with five commercial nuclear power plants of different reactor and containment designs. The NRC has used the landmark NUREG-1150 results and perspectives in a variety of regulatory applications, including development of PSA policy statements, support of risk-informed rulemaking, prioritization of generic issues and research, and establishment of numerical risk acceptance guidelines for the use of CDF and large early-release frequency (LERF) as surrogate risk metrics for early and latent cancer fatality risks.

Since then, the NRC has ensured safety primarily by using results obtained from Level 1 and limited Level 2 PSAs—both less expensive than Level 3 PSAs—and how they relate to lower level subsidiary safety goals based on CDF and LERF to risk-inform regulatory decisionmaking.

There are several compelling reasons for conducting a new comprehensive site Level 3 PSA. First, in the two decades since the publication of NUREG-1150, there have been substantial developments that may affect the results and risk perspectives that have influenced many regulatory applications. In addition to risk-informed regulations implemented to improve safety (e.g., the Station Blackout and Maintenance Rules), there have been plant modifications that may affect risk (e.g., the addition or improvement of plant safety systems, changes to technical specifications, power uprates, and the development of improved accident management strategies). Along with NRC and industry acquisition of over 20 years of operating experience, there have also been significant advances in PSA methods, models, tools, and data—collectively referred to as “PSA technology”—and in information technology. Finally, the NRC is conducting a State-of-the-Art Reactor Consequence Analysis (SOARCA) study, which leverages many of the same safety improvements and technological advances, integrates and analyzes two of the essential technical elements of a Level 3 PSA for some of the more likely reactor accident sequences—the severe accident progression and offsite consequence analyses. A new level 3 PSA could therefore seek to leverage the methods, models, and tools used in the SOARCA analysis and capitalize on the insights gained from the application of state-of-the-art practices.

In addition to these developments, the Level 3 PSAs documented in NUREG-1150 are incomplete in scope. Figure 9.US-2 illustrates the scope of a complete site accident risk analysis, with the approximate scope of the NUREG-1150 PSAs shown by the gray-shaded region. These PSAs were limited to the assessment of single-unit reactor accidents initiated primarily by internal events occurring during full-power operations. The partial coverage of external events indicates that a limited set of external events (fires and earthquakes) were considered for only two of the five analyzed nuclear power plants.

To update and improve its understanding of reactor accident risks, the NRC is considering evaluating accidents that might occur during any plant operating state, that are initiated by all possible internal events and external events, and that may simultaneously affect multiple units per site. Moreover, for a comprehensive site accident risk analysis, the NRC is also considering analyzing the risk from other site radiological hazards, such as spent fuel and radioactive waste streams. Because corresponding surrogate risk metrics that can be meaningfully integrated with and compared to CDF and LERF do not exist for these other radiological hazards, this analysis can only be accomplished in Level 3 space.

For these reasons, the NRC staff has identified three specific objectives for a potential new comprehensive site Level 3 PSA project. The first objective is to update and improve staff understanding of site accident risk by (1) incorporating plant safety improvements, insights from SOARCA, and advances in PSA technology that have occurred in the two decades since NUREG-1150, and (2) integrating the risk from additional radiological hazards using consistent assumptions, methods, and tools to enable a meaningful comparison and ranking of risk contributors to focus the NRC’s safety mission. Second is to upgrade and disseminate information about the NRC’s PSA technology, using 21st-century information technology in a comprehensive risk analysis toolbox that will enhance the NRC’s ability to risk-inform current and future regulatory decisionmaking. Third is to develop PSA expertise by training a new generation of risk analysts who will gain state-of-the-art knowledge and experience.

RES has initiated a scoping study to identify various options for the following elements of a pilot study: (1) site selection, (2) project scope, (3) PRA technology to be used, (4) new research needed to accomplish the project’s objectives, and (5) resource estimates and information needs to better understand and address potential challenges. The results of this scoping study, along with a specific recommendation for a Level 3 PSA pilot project, to the Commission for consideration in 2011.

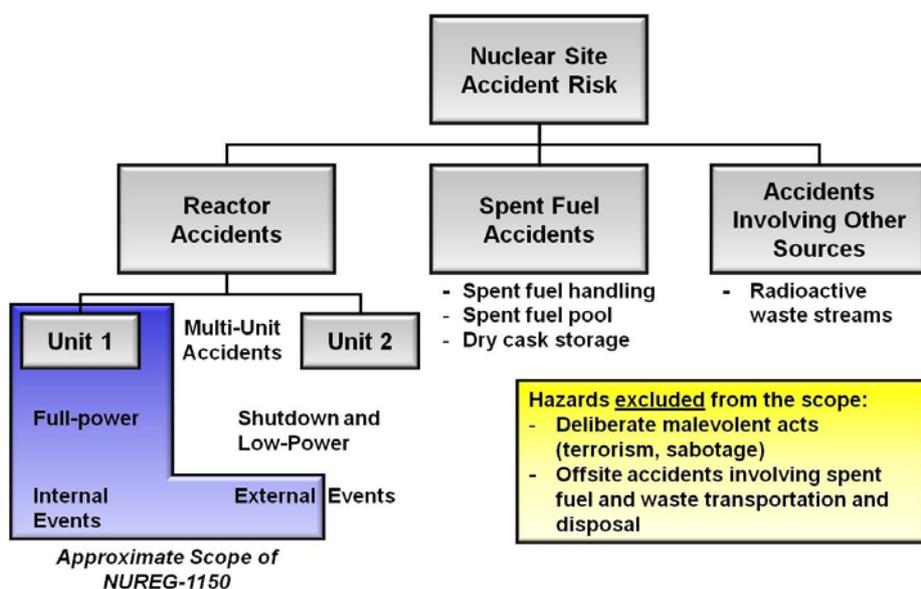


Figure 9.US-2. Site Accident Risk and Approximate Scope of NUREG-1150 (source: NUREG-1925, Rev. 1, Figure 5.3)

References

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.

Dube, D.A., "Comparison of New Light-Water Reactor Risk Profiles," PSA 2008, Knoxville, TN, 2008.

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.

Electric Power Research Institute and U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research, "Fire Probabilistic Risk Assessment Methods Enhancements," NUREG/CR-6850 Supplement 1/EPRI 1019259, 2010.

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.

Nuclear Energy Institute, "Roadmap for Attaining Realism in Fire PRAs," December, 2010.

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.

Kemeny, John G. "Report of the President's Commission on The Accident at Three Mile Island: The Need for Change: The Legacy of TMI," October, 1979.

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, "Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationships to Current Regulatory Requirements," Staff Requirements Memorandum SECY-90-016, 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. 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 Rev. 2, 2009.

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.

U.S. Nuclear Regulatory Commission, “Evaluation of Human Reliability Analysis Methods Against Good Practices,” NUREG-1842, 2006.

U.S. Nuclear Regulatory Commission, “Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, Volumes 1 and 2,” NUREG-1860, 2007.

U.S. Nuclear Regulatory Commission, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications,” NUREG-1824, 2007.

U.S. Nuclear Regulatory Commission, “Update on the Improvements to the Risk-informed Regulation Implementation Plan,” SECY-07-0074, 2007.

U.S. Nuclear Regulatory Commission, “A Phenomena Identification and Ranking Table (PIRT) Exercise for Nuclear Power Plant Fire Modeling Applications,” NUREG/CR-6978, 2008.

U.S. Nuclear Regulatory Commission, “Interim Staff Guidance, Probabilistic Risk Assessment Information to Support Design Certification and Combined License Applications,” DC/COL-ISG-3, 2008. U.S. Nuclear Regulatory Commission, “Modifying the Risk-Informed Regulatory Guidance for New Reactors,” SECY-10-0121, 2010.

U.S. Nuclear Regulatory Commission, “Annual Update of the Risk-Informed and Performance-Based Plan,” SECY-10-0143, 2010.

U.S. Nuclear Regulatory Commission, “Current State of Licensee Efforts to Transition to National Fire Protection Association (NFPA) Standard 805,” Letter from S. Abdel-Khalik, Chairman of the Advisory Committee on Reactor Safeguards, to G. Jaczko, Chairman, U.S. Nuclear Regulatory Commission, February 17, 2011.

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.

Wong, S.M., et al., “Risk Assessment Standardization Project (RASP) Handbook for Risk Assessment of Operational Events,” *Proceedings of ANS International Topical Meeting on PSA (PSA 2008)*, Knoxville, TN, September 7–11, 2008.

APPENDIX C

CAPS

New Proposals

WGRISK (2010) 2

Project/Activity Title	<p>The Use and Development of Probabilistic Safety Assessment in Member and non-Member countries.</p> <p><i>This proposal is to update the report NEA/CSNI/R(2007)12, which was issued November 2007. The previous version (NEA/CSNI/R(2002)18) was issued in July 2002.</i></p>
Objectives	<p>The mission of the Working Group on Risk Assessment (WGRISK) is to advance the understanding and utilisation of Probabilistic Safety Assessment (PSA) in ensuring continued safety of nuclear installations in Member countries. In pursuing this goal, the Working Group shall recognise the different methodologies for identifying contributors to risk and assessing their importance.</p> <p>This report, intended to be updated every 3 to 4 years, provides descriptions of the current status of PSA programmes in Member countries including basic background information, guidelines, various PSA applications, major results in recent studies, PSA based plant modifications and research and development topics. The scope of the original report is expended to include non-member countries along with NEA member countries.</p> <p>In addition synthetic summaries of each chapter are written and grouped as a Technical Note with the aim of a large diffusion. The experience feedback indicates that these reports were widely used, especially by decision makers.</p> <p>The objective of this task is to update both the main report and the summary, with emphasis on the new aspects, the general trends and specific points of interest if mentioned by the contributors.</p>
Scope/Justification/ Deliverables, Expected results and users, Relation to other	<p>Scope</p> <p>While the compilation is a not complete compilation, it provides a “snapshot” of the current situation in the member and non-member countries and hence it provides reference information and various</p>

<p>projects</p>	<p>insights to both the PSA practitioners and others involved in the nuclear industry. The interest and usefulness of the two previous versions indicate that an updating is necessary. These reports are in particular a basis for identification of interesting new detailed tasks, and more generally to follow the main trends of PSA development and application in the world.</p> <p>Activities</p> <ul style="list-style-type: none"> • Each country having participated to the 2007 report updates his contribution to the different chapters, with emphasis on the new inputs. Countries which did not participate but wishing to be involved can also contribute, following the format of the report. • The updated and new contributions are collected by the Secretariat. • A small writing group is setup in order to prepare the updated summaries of each chapter and a general overview. <p>Deliverables</p> <ul style="list-style-type: none"> • A report providing descriptions of the current status of PSA programmes in Member countries including basic background information, guidelines, various PSA applications, major results in recent studies, PSA based plant modifications and research and development topics. • A Technical Note providing a summary and a synthesis of the main report <p>Expected users</p> <ul style="list-style-type: none"> • Industry and regulators interested in current approaches. • NEA working groups interested in collaborative activities. <p>Relation to other projects</p> <ul style="list-style-type: none"> • Several CSNI or CNRA projects find elements and inputs in this report.
<p>Safety significance/ priority</p>	<p>Regarding the priority criteria set in Section IV.1 of the CSNI Operating Plan:</p> <ul style="list-style-type: none"> • Criterion 1: Issue of high safety significance and of importance to nuclear regulators.

	<ul style="list-style-type: none"> • Criterion 2: Better accomplished by international group. • Criterion 3: Likely to bring conclusive results in reasonable time frame.
Safety Issue and topic covered	<p>The following CSNI Main Challenge (and associated Safety Issue and Topic) are addressed by the proposed project:</p> <ul style="list-style-type: none"> • Increased public expectation on safety in use of nuclear energy. <ul style="list-style-type: none"> • Use of Risk-Informed methods • Transparent technical basis for safety assessment
Milestones (deliverables vs. time)	<p>If approved, the Secretariat will issue requests for updated inputs from members and new information from non-members (through the IAEA) in December 2010.</p> <p>It is expected to complete the updated report by September 2011.</p> <p>The summaries will be prepared by May 2012.</p>
Lead organization(s) and coordination	<p>For the main report, coordination will be performed by the NEA Secretariat.</p> <p>For the summaries a small group, including Bel V, GRS, IRSN and USNRC can be set-up (as previously). IRSN will be the coordinator.</p>
Participants (individuals and organizations)	All WGRISK members will participate.
Resources	1 to 2 men-months per participant to the small group in charge to prepare the summaries. 1 to 2 weeks for each participating organization to update the report.
Requested action from PRG/CSNI	Endorsement of proposal.
PRG Recommendation	Endorsed by PRG on 2 November 2010
CSNI Disposition	Approved by CSNI on 8 December 2010.