Nuclear Safety
NEA/CSNI/R(2019)10
September 2020
www.oecd-nea.org

Use and Development of Probabilistic Safety Assessments at Nuclear Facilities

OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

NEA
Nuclear Energy Agency

NEA/CSNI/R(2019)10

Unclassified **English text only**

3 November 2020

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

Use and Development of Probabilistic Safety Assessments at Nuclear Facilities

Please note that this document is available in PDF format only.

JT03467842

This document, as well as any data and 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.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 37 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, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, 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.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 33 countries: Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Russia, 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 sound and economical use of nuclear energy for peaceful purposes;

– 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 analyses in areas such as energy and the sustainable development of low-carbon economies.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management and decommissioning, 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.

This document, as well as any data and 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.

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

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) is responsible for the Nuclear Energy Agency (NEA) programmes and activities that support maintaining and advancing the scientific and technical knowledge base of the safety of nuclear installations.

The Committee constitutes 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 has 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 reviews the state of knowledge on important topics of nuclear safety science and techniques and of safety assessments, and ensures that operating experience is appropriately accounted for in its activities. It initiates and conducts programmes identified by these reviews and assessments in order to confirm safety, overcome discrepancies, develop improvements and reach consensus on technical issues of common interest. It promotes 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 (e.g. joint research and data projects), and assists in the feedback of the results to participating organisations. The Committee ensures that valuable end-products of the technical reviews and analyses are provided to members in a timely manner, and made publicly available when appropriate, to support broader nuclear safety.

The Committee focuses primarily on the safety aspects of existing power reactors, other nuclear installations and new power reactors; it also considers the safety implications of scientific and technical developments of future reactor technologies and designs. Further, the scope for the Committee includes human and organisational research activities and technical developments that affect nuclear safety.

Foreword

Because of its disciplined, integrated and systematic approach, probabilistic safety assessment (PSA)[1] has become a necessary complement to traditional deterministic safety analysis.

The main objective of the Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRISK), working under the aegis of the NEA Committee on the Safety of Nuclear Installations (CSNI), is to advance the understanding of PSA and to enhance its utilisation for improving the safety of nuclear installations.

The WGRISK mission is accomplished by performing a number of activities to exchange PSA-related information among member countries. This 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 contributions of the experts listed below to this report are gratefully acknowledged, they all provided valuable time and considerable knowledge towards the development of this paper:

Jeanne-Marie Lanore	IRSN, France (Task Leader)
Kwan-Il Ahn	KAERI, Korea
Attila Bareith	NUBIKI, Hungary
François Corenwinder	IRSN, France
Kevin Coyne	NRC, United States
Jaroslav Holy	ÚJV Řež, Czech Republic
Milan Patrik	ÚJV Řež, Czech Republic
Marina Roewekamp	GRS, Germany
Nathan Siu	NRC, United States
Ernest Staron	PAA, Poland
Smain Yalaoui	CNSC, Canada

[1] In this report, the abbreviations PRA (probabilistic risk assessment) and PSA probabilistic safety assessment) are used synonymously.

Table of contents

Tables

List of abbreviations and acronyms

ABWR	Advanced boiling water reactor
ALLEGRO	Demonstrator reactor of the gas-cooled fast reactor (GFR)
ANS	American Nuclear Society
AOT	Allowed outage time
AP 1000	Advanced power reactor 1 000 MWe
APR1400	Advanced power reactor 1 400 MWe
ASME	American Society of Mechanical Engineers
ASEP	Accident Sequence Evaluation Program
ASTRID	Advanced sodium technological reactor for industrial demonstration
ATHEANA	A technique for human event analysis
BSL	Basic safety level
BSO	Basic safety objective
BWR	Boiling water reactor
BWROG	Boiling Water Reactor Owners Group
CCDP	Conditional core damage probability
CCF	Common cause failure
CDF	Core damage frequency
CFD	Computational fluid dynamics
CNRA	Committee on Nuclear Regulatory Activities (NEA)
CPWG	CANDU PSA Working Group (IAEA)
CNSC	Canadian Nuclear Safety Commission
CSNI	Committee on the Safety of Nuclear Installations (NEA)
DEC	Design extension conditions
EC	European Community
EDF	Électricité de France
EOP	Emergency operating procedures
EPR	European pressurised reactor
EPRI	Electric Power Research Institute
ENSREG	European Nuclear Safety Regulators Group
FDF	Fuel damage frequency
FP	Full power
GDA	Generic design assessment
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Germany)
HEP	Human error probability
HRA	Human reliability analysis

HCR-ORE	Human cognitive reliability – operator reliability experiments
HORAAM	Human and organisational reliability analysis in accident management
HRP	Halden Reactor Project (NEA)
HTGR	High temperature gas-cooled reactor
IAEA	International Atomic Energy Agency
ICDE	International Common-cause Failure Data Exchange (NEA)
IDPSA	Integrated deterministic probabilistic safety assessment
IE	Initiation event
INER	Institute of Nuclear Energy Research (Chinese Taipei)
IPE	Individual plant examination
IPEEE	Individual plant examination for external events
IRSN	Institut de Radioprotection et de Sûreté Nucléaire/Radiological Protection and Nuclear Safety Institute (France)
I&C	Instrumentation and control
KAERI	Korea Atomic Energy Research Institute
LCO	Limiting condition for operation
LERF	Large early release frequency
LOCA	Loss-of-coolant accident
LOOP	Loss of offsite power
LPSD	Low power and shutdown
LRF	Large release frequency
LWR	Light water reactor
MCDET	Monte Carlo dynamic event tree
MCR	Main control room
MDEP	Multinational Design Evaluation Programme (NEA)
MEPEM	Méthode d’Evaluation Probabiliste de l’Echec des Missions opérateurs
MERMOS	Méthode d’Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté
MGL	Multiple Greek letter
MSPI	Mitigating Systems Performance Index (NRC)
MSWI	Melt-Structure-Water Interactions
NEA	Nuclear Energy Agency
NPP	Nuclear power plant
NRA	Nuclear Regulatory Authority (Japan)
NRC	Nuclear Regulatory Commission (United States)
OECD	Organisation for Economic Co-operation and Development
PAA	Państwowa Agencja Atomistyki (Poland)
POS	Plant operational state

PRA	Probabilistic risk assessment
PSA	Probabilistic safety assessment
PSR	Periodic safety review
PWR	Pressurised water reactor
QHO	Quantitative health objectives
RHWG	Reactor Harmonisation Working Group (WENRA)
RIDM	Risk-informed decision making
RI-ISI	Risk-informed in-service inspection
ROP	Reactor Oversight Program
R&D	Research and development
SAMG	Severe accident management guidelines
SBO	Station blackout
SFP	Spent fuel pool
SLIM	Success likelihood index methodology
SHA	Seismic hazard analysis
SOAR	State-of-the-art report
SPAR	Standardised plant analysis risk
SSC	Structures, systems and components
STI	Surveillance test interval
THERP	Technique for human error rate prediction
TOP	Topical opinion paper
TS	Technical specifications
TSO	Technical support organisation
WENRA	Western European Nuclear Regulators Association
WGAMA	Working Group on Accident Management and Analysis (NEA)
WGEV	Working Group on External Events (NEA)
WGHOF	Working Group on Human and Organisational Factors (NEA)
WGIAGE	Working Group on Integrity and Ageing of components and structures (NEA)
WGRISK	Working Group on Risk Assessment (NEA)

Executive summary

Background

Due to its disciplined, integrated and systematic approach, probabilistic safety assessment (PSA) is now considered as a necessary complement to traditional deterministic safety analysis.

The main objective of the Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRISK), working under the aegis of the NEA Committee on the Safety of Nuclear Installations (CSNI) is to advance the understanding of PSA and to enhance its utilisation for improving the safety of nuclear installations.

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 (NEA, 2002), then updated in 2007 (NEA, 2007) and in 2012 (NEA, 2013). As with previous versions, the task includes inputs from the International Atomic Energy Agency (IAEA) and the European Union (EU), and this has led to more information, thus providing a better overview on PSA worldwide.

This 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.

Experience feedback on the two previous reports indicates that they have been widely used, especially by decision makers.

Objectives of the task

The objective of this task was to update the previous report, with an emphasis on new developments, general trends and activities of specific interest to the task participants concerning the Fukushima Daiichi reactor accident. As compared with previous versions, the structure and format of the present report is also enhanced so as to better communicate information and insights.

As with previous versions of this report, a "snapshot" is provided of the current situation in member and non-member countries, and hence it includes reference information and various insights of both PSA practitioners and others involved in the nuclear industry.

The report also forms the basis for identifying new tasks for WGRISK.

Process

In December 2015, a proposed new structure of the report was prepared by a core task group. The core task group included representatives from the Institut de Radioprotection et de Sûreté Nucléaire (IRSN, France), the Nuclear Regulatory Commission (NRC, United States), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS, Germany), the

Canadian Nuclear Safety Commission (CNSC, Canada), the Institute of Nuclear Energy Research (INER, Chinese Taipei), the Nuclear Regulatory Authority (NRA; Japan), the Korea Atomic Energy Research Institute (KAERI, Korea) and the Państwowa Agencja Atomistyki (PAA, Poland).

The main aspects of the new structure were the following:

- The general structure was clarified to avoid repetitive answers. In particular, PSA development, PSA methods, PSA results and PSA applications were addressed in different chapters. Also, PSA standards and PSA methods were grouped into the same chapter.
- Post-Fukushima insights were not addressed in a separate chapter but included in each chapter of the report.
- A new chapter was added to discuss international activities.

This new structure was discussed and approved by WGRISK during its annual meeting in March 2016.

Following the approval of the revised report structure, it was requested that each country update its contribution, with an emphasis on new developments. The total contributions, received from 21 countries and one partner economy,[2] totalled several hundred pages.

To develop useful insights from this large amount of information, a small writing group was established by WGRISK. This writing group drafted concise, summary level text for each chapter, as well as a general overview.

The writing group included representatives from IRSN (France), CNSC (Canada), ÚJV (Czech Republic), GRS (Germany), NUBIKI (Hungary) and PAA (Poland).

IRSN was the co-ordinator of the task and drafted the executive summary, the general introduction and the overall conclusions.

General conclusions

It is recognised by the CSNI that PSA is a very useful tool for sustaining and improving safety. The cross-cutting aspect inherent in PSA means that it provides a large potential for identifying safety priorities. This tool is therefore particularly important for optimisation of safety work. For these reasons, a WGRISK task is to present the PSA use and development in member and non-member countries, updated appropriately, to inform PSA as well as non-PSA practitioners on the progress in relation to this topic.

The main insights in this most recent update, as presented below, are related to the increasing role of PSA in all participants(especially in the case of new plants), and all PSA aspects concerning PSA development, as well as PSA utilisations, as reported by the different countries. The effects of the Fukushima Daiichi reactor accident on PSA use and development, although not treated separately in the different chapters of this report, are presented in a particular section of the executive summary as a result of the

[2] Participating countries and territories: Belgium, Canada, Chinese Taipei, the Czech Republic, Finland, France, Germany, Hungary, India, Italy, Japan, Mexico, Korea, Poland, the Netherlands, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, the United Kingdom and the United States.

interest observed during WGRISK discussions. Finally, the use of this information for the WGRISK programme of work is also presented in this report.

Increased role of PSA

This overview confirms the general conclusions of the previous version of the report (NEA, 2013). The position and the role of PSA are increasing in all the respondents and for all PSA aspects:

- Countries' PSA frameworks and environments: more important and precise regulatory requirements are noted. In several member countries, PSA, previously performed on a voluntary basis, has become a regulatory requirement. In particular, in the frame of the periodic safety review, an updated PSA is now required in many countries.
- Numerical safety criteria: although there is not much new information since the previous report, for some countries, more formal safety goals have been defined. An important point is that there is progress for multi-unit sites where, in particular, the problem of risk aggregation needs consideration. Methods are needed for aggregating risk contributions across different reactor units and facilities. These methods need to account for single-unit, multi-unit and non-reactor facility accidents, and need to consider hazard groups and operating states with due regard to differences in the level of realism/conservatism, the level of detail in modelling and the uncertainty treatment.
- The status and the scope of ongoing PSA studies: several new PSAs are mentioned by member countries. In particular, new PSAs are, in most cases, an essential part of the safety assessment for new installations. It should also be noted that many existing PSAs have been or are being updated to take into account recent plant modifications (post-Fukushima modifications). Moreover, the scope of the studies has often been extended, especially after Fukushima (see details below). The most general PSA scope includes Level 1 and Level 2 (Level 3 remains less systematic),[3] for all reactor operating states, and this common scope illustrates progress towards harmonisation. In addition, in many studies, the scope has been extended to cover sources of radioactivity other than the reactor core, most notably the spent fuel pool for the reactor, but also intermediate spent fuel storage facilities.
- PSA applications and decision-making: PSA applications related to risk-informed design, as well as to plant operation improvements, are more and more numerous, with many concrete and practical examples mentioned by several countries.
  - o Several modifications related to electrical sources where PSA is a tool for assessing the benefit of these improvements.
  - o PSA is being used as a tool to support accident management (AM), both for prevention and for mitigation of severe accidents.

[3] Level 1 PSA is the assessment of core damage frequency (CDF). Level 2 PSA is the assessment of frequency and level of releases (large and/or early release frequency [LRF/LERF]). Level 3 PSA is the assessment of the frequency and level of harm to the public and environment outside of the site.

  - The use of PSA for operation optimisation (technical specifications, maintenance planning, online maintenance, etc.) is not new but an increasing number of examples are mentioned , often involving the development and use of risk monitors.
  - PSA is often used to provide a basis for the prioritisation of plant equipment (priorities for inspections).
  - The use of PSA insights for analysing experience feedback (precursor programmes) is increasingly mentioned as an important application.
  - The use of PSA for optimisation of regulatory activities is now being considered in a number of countries.

- *Uncertainties and sensitivity studies:* because of the importance of uncertainty in PSA for decision making, uncertainty and sensitivity analyses are required in several countries. Different validated and verified tools, for quantifying knowledge uncertainties (epistemic uncertainties) as well as statistical uncertainties (aleatory uncertainties) are available. Moreover, several physical supporting studies are aiming to reduce uncertainties (indicated in particular for fire and Level 2 PSA).
- *Future research and development:* several activities are in progress, involving either the follow-up of ongoing actions or the development of new methods and models. Some but not all of the development activities are linked to the Fukushima reactor accidents. Assessing the benefit of plant modifications can require some methodological development, and PSA development and application activities are often performed in parallel. (Key development activities are described below.)
- *International activities:* international co-operative activities, involving both small groups linked by a similar design or a particular topic, as well as large international activities (e.g. organised by the IAEA or the NEA) aiming to share good experience and avoid duplication, are ongoing. International co-operation is often a driver for PSA development and application as well as for harmonisation.

Generally speaking, it clearly appears that this review confirms the conclusions of the previous version of the report. Particularly for new build, PSA is now a necessary part of safety assessment.

Post-Fukushima effects

Post-Fukushima effects on PSA are indicated by many countries and for various topics. The most frequent post-Fukushima effect on PSA is the extension of the scope of the studies, particularly extension or re-evaluation of initiating events related to external hazards and hazard combinations, and the treatment of site risk (multi-unit, multi-source PSA with consideration of all main radioactive sources, including reactors, spent fuel pools and intermediate spent fuel storage facilities).

It should be noted that:

- For many sites, several studies had already been completed or were in progress (e.g. external hazards, LPSD or SFP PSA) prior to the accident in Fukushima.

Nevertheless, after the reactor accidents at Fukushima, these studies were often revised and improved (particularly for seismic PSA, as indicated).

- Other safety significant issues (not linked to Fukushima) are also the subject of important work (internal fire, HRA, digital I&C, etc.).

The topics that can be considered as new after Fukushima are: 1) the large number of external hazards considered within PSA; and 2) risk assessment applied with a site perspective (including multiple units, SFP and other facilities).

Regarding external hazards, long lists of external hazards or combinations of hazards have been previously investigated with more or less formal screening criteria. However, to date, few concrete results have been obtained. Generally, the studies have been limited to demonstration-level assessments of the initiating event frequency. The objective of these demonstrations is to show that various hazards or hazard combinations can be screened out. In some instances, more complete PSAs have been performed for severe weather phenomena such as tornado or extreme temperatures.

Regarding site PSA, important issues of interest to member countries include the topics of risk aggregation, of site safety goals and of common-cause failures.

Another topic with a link to Fukushima is the analysis of long duration sequences (in particular, loss of offsite power [LOOP] sequences). More generally, it is recognised that detailed treatment of the order and timing of events during the sequences can be an issue for PSA research and development.

The effects of the Fukushima accident can mainly be considered as an improvement to PSA in general, considering both PSA developments (scope, methods) and PSA applications (wider field of application, including site issues).

Use of the report by WGRISK

As indicated above, the NEA and WGRISK in particular will use the results of this report to monitor the conduct of ongoing activities, and to promote and implement new international collaborative efforts within the framework of the CSNI. For example, reflecting the topics of external events and site PSA discussed above, the following ongoing activities should be noted:

- The task of “Human Reliability Analysis in External Events PSA – Survey of Methods and Practice” initiated in 2015 is nearly completed.
- The task of “Status of Site Level PSA (Including Multi-Unit PSA) Developments”, which also started in 2015, is aiming to exchange information on how multiple reactor and multiple radioactive source issues are addressed in risk analyses carried out in member countries, identifying key challenges (including risk aggregation) and ongoing research activities for Site Level PSA. The corresponding task report is intended to be published in 2019.

Also, as mentioned above, important PSA topics with no particular link to the Fukushima accident are being addressed. Examples include an updating of the technical opinion papers (TOP) on fire and seismic PSA and the benchmark task relating to the modelling of digital I&C.

1. Introduction

1.1. 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 (NEA, 2002), then updated in 2007 (NEA, 2007) and in 2012 (NEA, 2013). The task was carried out with input from the International Atomic Energy Agency (IAEA) and the European Union (EU), and this has led to more information and thus provided a better overview on PSA worldwide.

This report, intended to be updated every three to four 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 experience feedback indicates that these reports have been widely used, especially by decision makers.

1.2. Objectives of the task

The objective of this task was then to update both the main report and the summary, with emphasis on new developments, general trends, and points regarding activities related to the Fukushima Daiichi accident of specific interest to the task participants. As compared with previous versions, the structure and format of the report was also to be enhanced to better communicate information and insights.

As with previous versions, the report provides a "snapshot" of the current situation in the member and non-member countries and hence provides reference information and various insights to both PSA practitioners and others involved in the nuclear industry.

The report also forms a basis for identifying new tasks for initiation by WGRISK.

1.3. Process

The proposal for the task (in the form of a CSNI Activity Proposal Sheet – CAPS) to update the report was approved by the CSNI in June 2015.

In December 2015 a proposed new structure of the report was prepared by a core task group. The core task group included representatives from the Institut de Radioprotection et de Sûreté Nucléaire (IRSN; France), the Nuclear Regulatory Commission (NRC; United States), Gesellschaft für Anlagen- und Reaktorsicherheit (GRS; Germany), Canadian Nuclear Safety Commission (CNSC; Canada), the Institute of Nuclear Energy Research (INER; Chinese Taipei), the Nuclear Regulatory Authority (NRA; Japan), the Korea Atomic Energy Research Institute (KAERI; Korea) and Państwowa Agencja Atomistyki (PAA; Poland).

The main aspects of the new structure were the following:

- The general structure was clarified to avoid repetitive answers. In particular, PSA development, PSA methods, PSA results and PSA applications were addressed in different chapters. PSA standards and PSA methods were also grouped in the same chapter.
- Post-Fukushima insights were not addressed in a separate chapter but included in each report chapter.
- A new chapter was added to discuss international activities.

This new structure was discussed and approved by the WGRISK during its annual meeting in March 2016.

Following the approval of the revised report structure, each country that participated in the development of the 2012 report updated its contribution, with an emphasis on new developments. In addition, a number of countries that did not participate in the writing of the earlier reports also contributed. Most of the contributions were collected by the Secretariat by March 2017; some contributions were received by June 2017. The total contributions, received from 22 countries, totalled several hundred pages. Moreover information from WGRISK meetings discussions and from past WGRISK Tasks was also used when appropriate.

To develop useful insights from this large amount of information, a small writing group was established by WGRISK. This writing group drafted concise, summary level text for each chapter, as well as a general overview.

The writing group included representatives from IRSN (France), CNSC (Canada), UJV (Czech Republic) GRS (Germany), PAA (Poland), and NUBIKI (Hungary).

IRSN was the co-ordinator of the task and drafted the executive summary, the general introduction and the overall conclusions.

1.4. Report content and intended audience

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

As in previous versions of the report, the country-by-country contributions are provided in Appendix A.

The principal audience for this report are PSA-knowledgeable staff from nuclear industry and regulators, technical support organisations (TSOs) and other PSA practitioners with interests in current approaches to the use and development of PSA, as well as those NEA working groups interested in collaborative activities with WGRISK.

1.5. Insights

The major conclusions of this updated report are as follows:

- Continuing the trend discussed in previous versions of this report, the international use and development of PSA continues to grow. There is an increasing trend in the use of multiple characteristics and indicators, including the importance of the PSA framework, the number of studies carried out, the scope of PSA studies, the number of risk-informed applications (for design and operation safety improvements) and the volume of ongoing PSA R&D. In recent years, for example, several countries have instituted new regulatory requirements to the effect that a plant's periodic safety review (PSR) must now include an up-to-date PSA.
- The development of new and advanced designs has led to a more rapid development in certain topic areas. Among others, these areas include the definition of a more formal framework, more precise safety goals, efforts relating to the importance of external hazards and to specific issues such as the reliability of digital systems and the reliability of passive systems. A tendency towards harmonisation has clearly appeared, in particular driven by international co-operation.
- Various, important, ongoing PSA activities have emerged in relation to the Fukushima Daiichi accident. Some of these activities (e.g. whole-site PSA) involve topics that may have been recognised before March 2011 but were not the subject of major projects. Other activities (e.g. external hazards PSA) were already being addressed by development efforts. In both cases, general interest has increased substantially after the accident.

Additional details regarding these major conclusions are provided in chapter 10.

As with previous versions, the NEA, and the WGRISK in particular, will use the results of this updated report 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 frameworks and environments

The use of the Probabilistic Safety Assessment (PSA) as a decision support tool and as an analytical tool has long been accepted by member countries. It is noticeable in the present report that this acceptance is growing step by step, year by year. This process is visible when observing the PSA framework and environment that sets the regulatory requirements in all participants.

The environment for using PSA in regulatory decision making and licensee practices differs in all countries and partner economies depending on the safety philosophy and the legal system. In practice, in all participants except for the United States, the regulator requires that the licensee perform a PSA. However although in the United States developing a PSA for operating plants is voluntary, if a licensee chooses to adopt a risk-informed approach, then a PSA is nevertheless required.

A similar approach was observed in previous years in several other countries, e.g. France where PSA studies were not required (studies were performed outside of the regulatory framework). However, recognition of PSA as a very useful tool for safety analyses has grown and in 2012 an order was issued by the French regulator accepting by law that a regulatory safety demonstration should include a PSA. A similar situation has been reported in Belgium and the Czech Republic where PSA became mandatory respectively since 2011 and 2017.

Practically all regulatory bodies responding to the questionnaire use and support the defence-in-depth (DiD) philosophy and PSA is seen as a provider of necessary information that can efficiently complement reasoning. In particular, PSA supports the risk-informed decision making (RIDM) approach which seems to be gaining ground in regulatory practice. The use of RIDM is explicitly mentioned in the contributions provided by Belgium, Finland, Hungary, Korea, the Netherlands, Spain, Switzerland, and the United States although in comparison to the previous WGRISK report a visible increase in using the RIDM approach is reflected only in the contribution from Belgium.

PSA-based tools such as Living PSA and Risk Monitors also contribute to the enlargement of the PSA framework and environment. The use of those tools is noted in the provided reports from the Czech Republic, Hungary, the Netherlands, Spain, Slovenia, Sweden and Switzerland. However, only in the Czech Republic, the use of Living PSA and Risk Monitors has been recognised as part of the "nuclear safety as a priority" policy established after 2011 and is included in the regulatory requirements.

The PSA framework and environment have visibly evolved following the Fukushima accidents in several countries. Pre-Fukushima developed procedures and regulatory requirements in Finland, Germany, Slovenia, Spain and Switzerland, were assessed as sufficient and no changes followed. However, in other countries the PSA framework and environment has been improved. In Europe a large effort was conducted by ENSREG (European Nuclear Safety Regulators Group) to assess all European nuclear power plants (NPPs) by performing stress tests. National reports were prepared by analysing safety issues in co-operation of utilities and regulatory bodies (www.ensreg.eu/EU-Stress-

Tests). PSA was not directly addressed in the review process. Nevertheless the results and recommendations related to natural hazards and margins as well as extreme natural hazards include risk assessment. As a consequence, revisions of PSA followed, and measures and improvements were proposed that were incorporated into the regulatory assessment process. Changes in the regulations were not always made but it can be noted that in certain countries, several non-mandatory activities that had previously been performed by the licensees and NPP operators as their own initiative became mandatory after 2011. For example in France, the licensee had used PSA as an aid for safety assessment since 1990 however in 2012 a decision was made that the regulatory safety demonstration shall include level 1 and level 2 PSAs for all relevant initiating events. In the Czech Republic PSA activities were mainly initiated by utilities in response to specific NPP needs. Following post-Fukushima activities a new State Law was prepared in 2015 (the law came into force in January 2017), in which the development of level 1 and level 2 PSAs became a mandatory requirement for Czech NPPs, with the scope covering all plant operational states (POS), all internal initiating events and internal as well as external hazards, both natural and human induced (man-made). One other effect of Fukushima noted in the country reports was that several regulators decided that an updated PSA must be part of a Periodic Safety Review (PSR). Such changes have been introduced in the Czech Republic (in 2015), Japan (in 2013) and Korea (in 2014).

A change in the scope of PSA is also noticeable. Efforts are being made to include in the PSA various internal and external hazards and hazard combinations that had not been required before. More efforts have been devoted to initiating events (IE), particularly related to external flooding and man-made hazards – e.g. the development of Level 1 and Level 2 PSA models for internal hazards (including internal fire and flooding events) is required since 2011 by the Belgian legislation.

Considerable attention is paid to seismic hazards occurring in coincidence with other initiating events as presented in the reports from Japan, Switzerland, the United States, the Czech Republic and Chinese Taipei. For example, in Chinese Taipei not many PSA-related regulatory activities took place before the Fukushima accidents, but after 2011 a revision of plant-specific seismic hazard analysis and seismic PSA update were performed and resulted in seismic reinforcement of specific structures and components in 2015. Similarly, in the Czech Republic, an update of the seismic PSA was performed in 2015 in response to the Post-Fukushima National Action Plan and resulted in i.e. the reinforcement of turbine hall walls. In the United States in 2014, as part of its implementation of lessons learnt from the 2011 Fukushima accident in Japan, licensees submitted updated seismic hazard information in response to an NRC request for information.

As a result of numerous activities after Fukushima accident, the scope of PSA has been enlarged to include not only plant operating at full power (FP) but low-power and shutdown (LPSD) conditions as well. This change has been reflected in the regulatory practice in Belgium, the Czech Republic, Japan, Spain and Sweden. For example, in Spain the regulator (CSN) required that before the end of 2014, Level 2 PSA at LPSD conditions should be performed in order to acquire knowledge for the development of severe accident management guidelines in LPSD states.

In some countries, such as France, PSA models are not developed for each and every plant due to the fact that the fleet of operating reactors is highly standardised and reference studies representing classes of several NPPs are deemed sufficient.

Most of the PSA either completed or in progress have been performed by the operators of the plants. However, several PSA have been performed by the regulators or their TSOs in order to support regulatory reviews and/or various applications of PSA in a risk-informed decision-making process (examples from France, Japan, Korea and the United States).

More generally, it is visible that in all countries the assessment process requires co-operation between the regulatory body and the plant owner and/or operator with a TSO involved.

For new plants most countries formally require that a PSA should be performed although again this depends on the safety philosophy and the legal system.

3. Numerical safety criteria

3.1. Status of numerical safety criteria

In 2006, the Nuclear Energy Agency Working Group on Risk Assessment (WGRISK) initiated task (2006)-2 "Probabilistic Risk Criteria" to gather information (methodological and rationales) related to the setting and technical application of the probabilistic criteria. The scope includes the whole range of criteria from individual and societal risk, off-site release, core damage and lower level goals to numerical criteria. The results of this task (NEA, 2009) showed that the numerical criteria and safety goals definition range from high-level qualitative statements (e.g. no significant additional risk to the health of individuals, limitation to a reasonable risk to persons and the environment) to technical deterministic criteria (e.g. maximum centerline fuel cladding temperature), and probabilistic risk criteria (e.g. core damage frequency [CDF] less than 1 in 100 000 years, large release frequency (LRF) less than 1 in a million years). It is also shown that safety goals have been published in different ways spanning from legal documents, legal limits, to internal guides to be used as "orientation values".

In some countries and partner economies, no numerical safety criteria have been defined (Belgium, Chinese Taipei, France, Germany, Mexico and Spain). Some countries use the numerical criteria as an indicative figure (Czech Republic, France, India, and United Kingdom), whereas other countries have identified the safety criteria only for new Fukushima Daiichi reactor accident (Canada, Finland and Slovenia). In some countries, criteria have been defined for existing plants as well as for new build (e.g. Hungary, the Netherlands, the Slovak Republic and Slovenia).

3.2. Framework for defining numerical safety criteria

In some countries, numerical criteria are derived from high-level metrics, i.e. the qualitative safety objectives such as the individual risk and/or societal risk, whereas in other countries, the safety goals are adopted by the regulatory bodies or the licensees from IAEA (IAEA-INSAG-12 [IAEA, 1999]) or from documents published by other bodies.

In general, the numerical criteria established or adopted by most NEA member countries are expressed on a per reactor unit basis. Thus, it has been common practice in the application of these criteria to consider the assessment of risk and the evaluation of its acceptability on an individual reactor unit basis (per reactor-year [ry]). PSAs are, therefore, being developed for individual reactor units with separate treatment of each internal and external hazard group (e.g. internal fires, internal floods, seismic events, external floods, high winds).

The metrics used to define the numerical criteria in order to evaluate the safety level of a plant are grouped as follows:

a. Safety system reliability/unavailability (see Table 3-1);

b. Level 1 PSA numerical criteria: CDF per reactor-year (see Table 3-2);

c. Level 2 PSA numerical criteria: large (early) release frequency (L(E)RF) (see Table 3-3);

d. Numerical criteria for incremental risk increase (see Table 3-4);

e. Individual and societal risk criteria: Expressed by dose limits to the public, and/or by quantitative health objectives (QHO) (number of acute and late fatalities). Numerical criteria for individual and societal risk are established in some countries (United States and Korea) as part of quantitative health objectives (QHOs). These are expressed in terms of early and late fatalities, respectively. The Netherlands and the United Kingdom have defined societal risk criteria in terms of the frequency and the number of incurred fatalities. There are differences in the way these criteria have been defined depending on whether the criteria relate to: acute effects leading to early death or late effects leading to eventual death; whether the consequences should take account of countermeasures such as sheltering, taking stable iodine tablets and evacuation; and whether the numerical values defined are limits or objectives.

3.3. New developments

During the last few years, extensive work has been conducted towards the development of a safety goals structure that encompasses the whole spectrum of nuclear safety, as defined in the International Atomic Energy Agency (IAEA) Fundamental Safety Principles (IAEA, 2006).

In April 2011, the IAEA started a project to develop a more consistent and holistic framework for safety goals that would be composed of a hierarchical structure of qualitative concepts (e.g. defence in depth) and quantitative risk metrics (IAEA, 2012-13). The same structure has also been adopted by the NEA Multinational Design Evaluation Programme (MDEP) (NEA, 2011), Western European Nuclear Regulators Association (WENRA, 2010), and other regulators.

The technical challenges associated with the site-level safety goals were identified during the International Workshop on Multi-unit PSA in Ottawa (November, 2014) (CNSC, 2014). These challenges are:

- Methods of aggregating risk contributions across different reactor units and facilities, single-unit and multi-unit and facility accidents, hazard groups and operating states with due regard to differences in level of realism/conservatism, level of detail in modelling, and uncertainty treatment.
- Methods for comparing calculated risks against existing and new site-based safety goals.
- Question of whether safety goals should be quantitative or qualitative; supported by quantitative safety design objectives.
- Lack of multi-unit site-based acceptance criteria for evaluating the integrated risks from a multi-unit site PSA.
- The need for more international consensus on the approach to safety goals and use of such goals to interpret PSA results.

The IAEA is currently also conducting a project on multi-unit PSA, and risk aggregation. The completion date of these two projects is planned for end-2019.

A technical report prepared within the international ASAMPSA_E (Advanced Safety Assessment Methodologies: PSA Extended) project of the European Commission (EC) provides an extensive list of risk metrics (Wielenberg et al., 2016) and their extension to site level metrics.

The topic of risk metrics and safety goals is also identified as one of the three focus areas of the WGRISK Task 2015 (2) "Site Level PSA (Including Multi-Unit PSA) Developments". A survey was conducted as part of Phase 1 of this task and the general conclusions are as follows:

- Many countries referenced the fundamental safety objective "protect people and environment", as a qualitative safety goal. This fundamental safety objective is supplemented in some countries by the individual risk and societal risk qualitative safety goals. Some countries have defined both qualitative and quantitative safety goals.
- Safety goals are established on a per-unit basis, and most of the participants do not have different safety goals for sites and individual units.
- Numerical values associated with safety goals are consistent with IAEA-INSAG-12 (IAEA, 1999).
- Safety goals are generally used as indicators for design and operation improvements, but not as strict regulatory limits. A common trend is that if the CDF/ L(E)RF were higher than the safety goal limits or targets (as applicable), it was either encouraged or enforced dependent on the regulatory requirements to make adequate provisions to reduce the risk.
- Definition and applicability of the "practical elimination" concept differs among member countries. Only few countries apply this principle for new build.
- CDF is only applicable to some reactor facilities, and it might not be applicable to other reactor facilities such as: high temperature gas-cooled reactors (HTGR), and non-reactor sources such as SFPs, and radioactive waste management facilities. Therefore, this metric is not readily extendable to provide site level risk characterisation.
- No international consensus on what would constitute a quantitative measure for the large off-site release (Level 2 PSA). Only few countries (Canada, Finland, Japan, Sweden and Switzerland) have opted to specify the releases in absolute quantities to characterise a large release (e.g. any release higher than 100 TBq of Cs-137).

Table 3-3-1: Safety systems reliability criteria

Canada	Safety systems and their support systems shall be designed to ensure that the probability of failure on demand from all causes is lower than 1.0 E-03.
Slovak Republic	Failure probability of a safety system < 1.0 E-03
	Failure probability of protection system < 1.0 E-05

Table 3-3-2: Level 1 PSA numerical criteria

Country or territory	Organisation	Frequency	Notes
Canada	Regulator	1.0 E-05 /ry	Limit for new plants
	Licensee	1.0 E-04 /ry	Limit for existing plants
		1.0 E-05 /ry	Objective for existing plants
Chinese Taipei	Licensee	1.0 E-05 /ry	Limit
Czech Republic	Licensee	1.0 E-04 /ry	Objective for existing plants
		1.0 E-05 /ry	Objective for new plants
Finland	Regulator	1.0 E-05 /ry	Objective for new build
France	Regulator	1.0 E-05 /ry	Objective for new plants
Italy	Regulator	1.0 E-05 /ry to 1.0 E-06/ry	Objective
Hungary	Regulator	1.0 E-04 /ry	Limit for existing plants
		1.0 E-05 /ry	Limit for new plants
Japan[4]	Regulator	1.0 E-04 /ry	Objective
Korea	Regulator	1.0 E-04 /ry	Objective for existing plants
		1.0 E-05 /ry	Objective for new plants
Netherlands	Regulator	1.0 E-04 /ry	Limit for existing plants
		1.0 E-06 /ry	Limit for new plants
Slovak Republic	Regulator	1.0 E-04 /ry	Objective for existing plants
		1.0 E-05 /ry	Objective for new build
Slovenia	Regulator	1.0 E-04 /ry	Objective for existing plants
		1.0 E-05/ry	Objective for new build
Sweden	Law	1.0 E-05 /ry	Objective: This is a criterion or safety goal established by the licensees for CDF from Level 1 PSA.
Switzerland	Regulator	1.0 E-04 /ry	Limit for existing plants
		1.0 E-05 /ry	Objective for existing plants
United Kingdom[5]	Regulator	1.0 E-04 /ry	Limit
		1.0 E.05 /ry	Objective
United States	Regulator	1.0 E-04 /ry	Objective

[4] The safety goals were discussed in detail by the Safety Goal Specialised Subcommittee of the former Nuclear Safety Committee (NSC) until 2006. The results of the study are considered to form the technical basis for NRA's discussion of safety goals.

[5] 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.

Table 3-3-3: Level 2 PSA numerical criteria

Country or territory	Organisation	Risk metric	Frequency	Notes
Canada	Regulator	Small release frequency (> 10^{15} Bq of I-131)	< 1.0 E-05 /ry	Objective for new plants
		100 TBq Cs-137[7]	1.0 E-06 /ry	
	Licensee	> 1 % Cs-137	1.0 E-05 /ry	Limit for existing plants
		> 1 % Cs-137	1.0 E-06 /ry	Objective for existing plants
Chinese Taipei	Licensee	Not defined	1.0 E-06 /ry	Objective
Czech Republic	Licensee	Not defined	1.0 E-05 /ry	Objective for existing plants
			1.0 E-06 /ry	Objective for new plants
France	Regulator	Unacceptable consequences (Not defined)	Negligible[6]	Objective for new plants
Finland	Regulator	100 TBq Cs-137	5.0 E-07 /ry	Objective for new build
Hungary	Regulator	Not defined	1.0 E-05 /ry	Limit for existing plants
			1.0 E-06 /ry	Limit for new plants
Japan	Regulator	Containment failure[7]	1.0 E-05 /ry	Objective
		100 TBq Cs137	1.0 E-06 /ry	
Korea	Regulator	LERF	1.0 E-05 /ry	Objective for existing plants
		LERF	1.0 E-06 /ry	Objective for new plants
		100 TBq Cs137	1.0 E-06 /ry	Objective for all plants
Slovak Republic	Regulator	Not defined	1.0 E-05 /ry	Limit for existing plants
		Not defined	1.0 E-06 /ry	Limit for new build
Slovenia	Regulator	Not defined	5 E-06 /ry	Limit for existing plants
		Not defined	1.0 E-06 /ry	Limit for the new build
Sweden	Licensee	> 0.1 % of core inventory	1.0 E-07 /ry	Objective: This is a criterion or safety goal established by the licensees, for L(E)RF from Level 2 PSA.
Switzerland	Regulator	LERF	1.0 E-05 /ry	Limit for existing plants
			1.0 E-06 /ry	Objective for existing plants

[6] The aim is that the sequences that lead to a large early release should be "practically eliminated".

[7] The safety goals were discussed in detail by the Safety Goal Specialised Subcommittee of the former Nuclear Safety Committee (NSC) until 2006. The results of the study are considered to form the technical basis for NRA's discussion of safety goals.

Country or territory	Organisation	Risk metric	Frequency	Notes
United Kingdom	Regulator	100 or more fatalities	1.0 E-05 /ry	Basic Safety Level
			1.0 E-07 /ry	Basic Safety Objective
		Effective off site dose > 1 Sv	1.0 E-04 /ry	Basic Safety Level
			1.0 E-06 /ry	Basic Safety Objective

Table 3-3-4: Incremental risk increase numerical criteria

Country	Numerical criteria
Czech Republic	Change allowed if: - ΔCDF < 5 E-06/ry - ΔLERF < 1 E-06/ry Change not allowed if: - Overall CDF > 1 E-04/ry - Overall LERF > 1 E-05/ry
Korea	Not Allowable Area : - ΔCDF > 1 E-05/ry - ΔLERF > 1 E-06/ry Allowable Area : - ΔCDF < baseline CDF (for baseline CDF < 1 E-06/ry) - ΔCDF < 1 E-06/ry (for baseline CDF < 1 E-04/ry) - ΔLERF < baseline LERF (for baseline LERF < 1 E-07/ry) - ΔLERF < 1 E-07/ry (for baseline LERF < 1 E-05/ry) Area where changes can be considered with detailed assessment Between 'allowable' and 'not allowable' area
Netherlands	- TCDF < 1 E-06/ry - Instantaneous TCDF shall never exceed the value of E-04 /ry - ΔTCDF x AOT < 5 E-08/ry - ΔTCDF < 1 E-04 /ry
Slovenia	Limits for risk increase: - 5 E-07 /ry for CDF, and - 1 E-08/ry for LERF
Spain	Same as in US NRC Regulatory Guide 1.174
Switzerland	Change allowed if: - ΔCDF < 1 E-07/ry - ΔFDF < 1 E-07/ry - ΔLERF < 1 E-08/ry and: - Overall CDF < 1 E-05/ry
United States	NRC Regulatory Guide 1.174

4. Countries' statuses and the scope of ongoing PSA studies

Generally, the scope of the probabilistic safety assessment (PSA) has been extended since the previous version of this report. Extension can be observed in relation to several attributes that characterise the scope of the assessments:

- PSA Level: Level 1, Level 2 and Level 3 assessments, respectively;
- Initiating events: internal events, internal and external hazards;
- Plant operational states: full power, low power and shutdown states;
- Sources of release: reactor, spent fuel pool (SFP) and other sources.

4.1. PSA Level

The vast majority of plants have both Level 1 and Level 2 assessments. Level 2 PSA is often limited to determining large early release frequencies (LERF) or large release frequencies as opposed to a detailed quantitative analysis for a range of different release categories. The scope of PSA, especially Level 2 PSA, varies across countries in terms of the initiating events and plant operating modes addressed, which is mostly attributable to differences in underlying regulatory requirements.

Level 3 analysis with an assessment of off-site radiological consequences and health effects has been reported only for a few countries (Japan, Korea, the Netherlands, the United Kingdom, and the United States) and for some plants. Regulatory requirements and quantitative safety goals do not call for Level 3 PSA in most countries. However, as compared with the situation in 2010 (discussed in the previous version of this report), new research and development (R&D) activities are now being carried out, and pilot studies are either underway or planned in various countries in this area (Canada, Finland, Korea, the Slovak Republic, Sweden and the United States). Korea has very ambitious programmes in place to advance in Level 3 PSA methodology, computer codes and risk quantification. Discussions on potential regulatory requirements for Level 3 analysis are ongoing in Sweden.

4.2. Initiating events

In recent years there has clearly been a move towards extending the range of initiating events quantitatively addressed by PSA, especially with a focus on PSA for external hazards. Parallel to making amendments in the regulatory framework, several country responses witness improvements in selection, screening and probabilistic assessment of site-specific external hazards as well as in assessing plant risk. Over and above seismic PSA that had traditionally been in the focus of risk assessment for external events, more and more efforts are made to perform detailed quantitative risk assessment for an extended range of external hazards. This is especially true for single and combined natural hazards. Over and above the evidence from the country responses, the conclusions of a WGRISK workshop on the status and advances in external events PSA (NEA, 2014) also confirm the increase of PSA scope in this respect.

The Fukushima Daiichi accident has drawn much attention to external hazards PSA methodology and applications. On the one hand, use has been made of available risk assessments in post-Fukushima activities/safety reassessments. On the other hand, the adequacy and appropriateness of existing analyses, being either a fully developed PSA or an alternative, simplified approach, e.g. pilot study on simplified seismic PSA in the Nordic PSA Group, for assessing plant challenges and vulnerabilities, have been evaluated. Among others, the need for assessing risk at the site level by the development and use of multi-unit and/or multi-source PSA has emerged as a result of these activities – see more discussion on this and other aspects in Section 8 on Future Developments and Research.

Besides the efforts devoted to a more rigorous and extended analysis of external hazards, there are also ongoing activities related to extending the range of internal area events explicitly addressed in PSA (e.g. explosion PSA in France or internal flooding in Germany).

4.3. Plant operational states

As with the scope of initiating events, the tendency is to cover all modes of plant operation in PSA. Accordingly, over and above assessing accidents at full power, PSA for low power and shutdown states has been performed in all countries. However, LPSD PSA is not available for all the plants in some countries, since such an analysis is not always required by regulation, and this part of the PSA is still in its developmental phase for some plants. Commensurate with regulatory requirements and licensee goals in risk-informed safety management, the scope of LPSD PSA shows a greater variance than that of the analysis for full-power operation. For instance, Level 2 PSA still does not always include low power and shutdown states. Even if performed, LPSD PSA is often available only for fewer classes of initiating events, e.g. external hazards are not addressed in some cases.

Lessons learnt from the Fukushima Daiichi accident have led both nuclear safety authorities and licensees to direct more attention to low power and shutdown states in risk assessment. This has resulted in useful advances in performing and applying LPSD PSA. New severe accident management guidelines developed in Korea for low power and shutdown accidents are an example of such advancements.

4.4. Sources of release

Mostly the reactor and the spent fuel pool have been considered as potential sources of radioactive release in the assessments. SFP PSA has been performed in more than ¾ of the reporting authorities. The scope of SFP PSA is often narrower than the scope of reactor PSA as fewer classes of initiating events are considered. Mostly in response to regulatory requests, developments in SFP PSA have been intensified in several countries and partner economies following the Fukushima Daiichi accidents (e.g. Chinese Taipei, Finland, Germany, Hungary, Japan, Korea and Spain). This area of PSA is still subject to current or planned research and development activities as well (e.g. Belgium, Japan, Korea and the United States). Also, SFP PSA has been included in various licensing applications in Finland, France and Korea.

To meet regulatory requirements, risk assessments have been performed for release sources other than the reactor and the spent fuel pool in some countries. Examples are: the Olkiluoto interim storage for spent fuel and the spent fuel encapsulation plant to be built in Olkiluoto, Finland; the modular vault dry storage facility in Hungary; experiments, irradiation facilities for the high flux reactor in the Netherlands; and fuel transport between the pressure vessel and the SFP in Sweden. A special, complex case is the release from multiple sources. While quantitative safety goals have basically been developed for single-unit and single-source accidents, the requirements of some nuclear safety authorities (e.g. in Canada) already include an obligation to consider multi-unit effects in PSA, if applicable. In a more general sense, multi-source PSA belongs to the site level risk assessment that is subject to R&D in several countries (see Section 8). International projects are underway through WGRISK and IAEA regarding multi-unit and site level PSA.

4.5. PSA updates

PSA models, results and documentation are regularly updated in most countries. As a minimum, PSRs require updating of PSA, and such reviews are carried out every ten years in most cases (more frequently in some countries). However, there are requirements that tend to be more stringent than that. There is a requirement in place in several countries to ensure that PSA models adequately represent the current plant state and conditions, which is an important precondition for credible and up-to-date risk quantification and for risk-informed applications. A Living PSA procedure (for all or for some plants) has been adopted in about ⅔ of the reporting authorities for this purpose.

The Fukushima Daiichi accident triggered PSA improvements and updates in several countries and partner economies (e.g. PSA improvements in Chinese Taipei, some PSA refinement in Finland, PSA update in Hungary, PSA revision in the Czech Republic and Korea, and updated seismic hazard information in the United States). In addition, modification of PSA to model plant changes, implemented as post-Fukushima safety measures, has also been an important area of PSA updates for numerous plants (e.g. PSA modelling of several post-Fukushima measures in the Czech Republic, sensitivity studies reflecting the post-Fukushima actions in Korea).

4.6. Licensee and regulatory PSA models

In addition to risk assessment by the licensees, several regulatory authorities have also developed independent PSA models or have such models constructed by technical support organisations. These models support regulatory activities in reviewing licensee analyses and/or various applications of PSA in a risk-informed regulatory decision-making framework. For example, PSA models for regulatory use are available in France, Germany, Japan, Korea and the United States. Independently reviewed and verified licensee PSA models are used in regulatory oversight activities in some other countries (e.g. in Spain). These are findings similar to those of the previous version of this report.

4.7. Overall conclusions

In the post-Fukushima era there has been a growing interest in pursuing, to the extent feasible, all-modes, all-hazards and all-sources risk assessments for NPPs and other nuclear installations. The ultimate goals of such extended assessments are to better characterise risk and to provide further support to risk-informed applications by licensees and regulatory bodies as well. Good progress has been made in quite a few areas in the national PSA programmes to meet these goals. However, the need for developments in methodologies, including data assessment and analysis procedures, and in supporting computerised tools has also been recognised. Improvements in PSA studies and in underlying methodologies go parallel in most countries. International co-operation and information exchange is an important driver of advancement in national PSA programmes.

5. PSA methodology and data

Practical Probabilistic Safety Assessment (PSA) methods are available for Level 1 and Level 2 PSA covering the treatment of internal events and relevant internal and external hazards for NPPs at power operation as well for different plant operating states (POS) during low power and shutdown. Most authorities follow methods developed in the United States by the NRC (as published in NUREG documents), EPRI and/or ASME ANS. Guidance provided by the IAEA is used as far as applicable, too. Moreover, several countries (e.g. Germany) developed national guidance.

In principle, the methods used are the same for existing plants and new build; however, the scope of the analyses may vary.

Level 1 PSA methods applied are more focused on core damage frequencies (CDF), fuel damage frequencies (FDF) resulting mainly from SFP damage are often calculated separately and not treated completely in the same manner as core damage. In particular, state-of-the-art methods for internal hazards, which in general cover mainly internal fire and flooding, are available for both power operation as well as low power and shutdown states; however, analyses are mainly carried out for power operation.

PSA methods cover in general the following:

- The small event tree - large fault tree methodology for Level 1 PSA (using fault tree linking) to develop event trees (and the corresponding accident sequences) is applied in principle for modelling the consequences of an initiating event and additional malfunctions and/or failures caused by either random failures or as a consequence of the initiating event.
- For determining initiating event (IE) frequencies, typically a Bayesian update for combining plant-specific data and generic data is applied; for some IEs, their frequency is estimated by means of a fault tree model.
- For human reliability analyses (HRA), a majority of institutions from several countries apply the internationally well-accepted THERP (Technique for Human Error Rate Prediction) and/or ASEP (Accident Sequence Evaluation Program), methodologies, mainly for internal events PSA, partly also in the frame of analysing human actions in case of area events (i.e. events that can affect broad areas of the plant, such as fires and seismic events). HRC-ORE and SLIM (Success Likelihood Index Methodology) are also used as well as MERMOS and ATHEANA. To model the actions of the SAMG for Level 2 PSA, dedicated HRA models have been developed in France: HORAAM by IRSN and MEPEM by EDF. In the United States, the SPAR-H model is used in retrospective PSA analyses assessing the significance of operational events and findings.
- For analysis of equipment failure data, information on equipment failure is typically analysed first, followed by a statistical combination of plant-specific and generic data via a Bayesian method. Common cause failure (CCF) modelling is widely based on the Multiple Greek Letter (MGL) model. Another approach

is based on the use of alpha factors and generic CCF parameter data or on the Beta Factor Model. CCF estimation methods have been improved in the near past to consistently include different sources for estimation of uncertainties applying also Bayesian statistical methods.

- Modelling of new digital instrumentation and control (I&C) systems needed in the near future since the replacement of analogue systems is still challenging, more mature and validated models are needed for sufficiently realistic I&C modelling and quantification for the purposes of licensing regarding the topic of common-cause failures and software reliability. Activities are ongoing in several countries (e.g. Finland, France, Germany, Korea, Sweden and the United States) and on an international basis.

With respect to internal and external hazards modelling, typically the plant internal hazards fire and flooding are modelled in detail; to some extent also explosions or the drop of heavy loads are considered. Other internal hazards are often screened out. Pre-2011 PSAs addressing external hazards typically paid considerable attention to seismic events; other external hazards (e.g. high winds; external flooding from storms, tsunamis, and riverine floods) PSA was less uniform. Following the Fukushima Daiichi reactor accidents, there has been increased attention on these other hazards as well as on related hazards (e.g. flooding from local intense precipitation). Licensees from several countries often apply publicly available methodologies and standards from EPRI, NRC or ASME. As discussed in Section 8, external hazards analysis is also an active area of methods development.

So far, for a single internal or external hazard a multiple step approach is often applied so that most of such hazards can be conservatively addressed in PSA and need not be analysed in detail. Detailed analyses requiring explicit methods have been mainly carried out for internal fire and flooding, and for seismic hazards, tsunami, for external flooding, and in few cases for extreme weather conditions, such as high winds (including hurricane, tornado), lightning or snow as natural external hazards. Man-made hazards such as accidental aircraft crash and the influence of surrounding industry (resulting in the release of dangerous substances, fire or explosion pressure waves) to the plant operation are also considered in more or less detail within PSA.

For fire, mainly the US methodologies described in a number of EPRI and NRC documents, including detailed guidance for fire-induced vulnerability evaluation (FIVE), fire modelling and Fire PSA are applied in most of countries, mainly for fires at power. Other state-of-the-art approaches (e.g. the comprehensive methodology from Germany covering all POS [FAK]) are available and included in national guidance documents. For internal flooding, several countries apply the methodology provided by EPRI/NRC, limited mainly to power operation.

To date, very few external hazards and hazard combinations are addressed in detail within PSA. In most of countries either a hazard screening is performed or hazards to be investigated have been selected based on generic frequency data being available (e.g. in Switzerland, for turbine missiles and tornado). Event combinations or correlations of hazards have been addressed only in very few PSA so far, although treatment is required in some countries (e.g. in Germany) by recent regulation. Validated, generally accepted methods are still missing, although corresponding developments are ongoing.

Methods for treating internal and external hazards in Level 2 PSA are available, but according to existing regulations and available standards and guidance, only applied in few PSA studies so far. In the United States, the NRC is conducting a full scope (all-hazards, all plant operating states), site-level (all-sources) pilot Level 3 PSA. PSA extension in this direction is foreseen in several countries in the frame of PSA updates, e.g. as part of the PSR as required by WENRA.

With a specific focus on highly dynamic, time-dependent event sequences, methods of the dynamic PSA have been developed and are being continuously enhanced. The aim is to enable Integrated Deterministic Probabilistic Safety Analysis (IDPSA) to derive more detailed probabilistic results for risk-informed decision making. Important developments are ongoing in Finland (FinPSA code development related to dynamic IDPSA models), Germany (combinations of MCDET with deterministic codes, e.g. for fire or flooding simulations, stress models), and the United States (development of advanced dynamic event tree modelling tools, e.g. ADAPT, RAVEN; and integrated models including the treatment of operator cognition and actions during accidents, e.g. ADS/IDAC).

Uncertainty and sensitivity analyses are required in several countries, different validated and verified tools (e.g. SUSA in Germany), for quantifying knowledge uncertainties (epistemic uncertainties) as well as statistical uncertainties (aleatory uncertainties) are available in member countries.

A variety of data are needed in the frame of PSA, such as IE frequencies, component failure/unavailability data, HRA data:

- For initiating event (IE) frequency estimations, either generic data (e.g. from NUREG/CR-5750 [INL, 1999)]), or – as far as available and sufficient – plant-specific data, or a combination of both (plant-specific data used for a Bayesian update of generic data) are generally used.
- In principle, plant-specific data are applied as far as available for component failures and unavailabilities including CCF. Several countries consider generic experience, typically from CCF databases, such as the EPRI database or the OECD/NEA ICDE Database (e.g. considered by the Czech Republic, Finland, France, the Netherlands, Sweden). Operating experience from inspections and maintenance collected on a national basis is considered as well (e.g. a specific database from the NPP operators used in Germany and the Netherlands). A Bayesian update is generally applied in order to incorporate the plant-specific operating experience into the failure rates and the initiating event frequencies. National databases on equipment reliability are available in several countries for different types of equipment (e.g. Germany, Japan).
- Concerning HRA data, PSA practitioners need various kinds of data useful not only for understanding the contexts of erroneous behaviour but also for quantifying their likelihood or the HEP (human error probability). Therefore, simulator data are used by some institutions (e.g. from Finland and Korea).

Data sources for generic data are mainly NUREG or EPRI reports. Some generic data, e.g. for CCF, are also given in German regulatory documents.

The computer codes applied for Level 1 PSA are RiskSpectrum and CAFTA, which are used in various countries, but also SAPHIRE, FinPSA and RISKMAN. For Level 2 PSA, many institutions apply different versions of the MAAP, MELCOR and ASTEC codes for severe accident analysis, and the EVNTRE code.

Detailed guidance on PSA methods and data is available in several countries (e.g. Finland, France, Germany, Hungary, the Slovak Republic, Switzerland and the United States) on a national basis; other countries mainly follow guidance given by IAEA and/or NRC, ASME/ANS and EPRI.

Peer reviews are foreseen in a variety of countries and one partner economy, to be carried out either by independent institutions for the licensees or for the regulatory body, such as in Chinese Taipei, Korea, Mexico, Switzerland, the United States, and partly in Belgium, Finland and Germany. Specific guidance for PSA peer reviews is mainly provided in the United States by different organisations in detail and in the Finnish PSA guidance. Benchmarking for validation of PSA results is performed in some countries, such as Finland, Switzerland and the United States as well.

5.1. Overall conclusions

After the nuclear accident at Fukushima Daiichi, methods for addressing internal and external hazards in PSA up to Level 2 have been enhanced and extended. There remain issues, notably the systematic consideration of event combinations and correlations in PSA for all POS, for which the methods are not yet sufficiently mature enough for practical decision-support applications. Noting that some countries now have regulatory requirements requiring the treatment of these issues, developmental work is ongoing.

Risk aggregation including area events but also site-specific aspects, such as multi-unit and multi-source considerations has been recognised as being necessary, at least for multi-unit non-LWR (light water reactor) plants without real containments as well as for sites with operating NPPs and other nuclear facilities (plants under decommissioning, research reactors, on-site nuclear waste storage facilities, etc.). Activities on site level PSA are ongoing in several WGRISK member countries (e.g. Canada, Germany and the United States).

6. Notable results of PSA

Most of the probabilistic safety assessment (PSA) results reported in the questionnaire responses have been developed since the last update of this report issued in 2012 (NEA, 2013). PSA studies continue to evolve worldwide, and this chapter presents a concise summary of the latest results to the extent reflected in the questionnaire responses.

How PSA results are reported varies significantly across countries. Numerical values of risk measures from Level 1 PSA and, in fewer instances Level 2 PSA, are given in some cases. Results from Level 3 PSA are included in the country report of the United Kingdom only.

A few questionnaire responses include the risk contributions of dominant initiating events or groups of initiating events, accident sequences, component failures and human failure events. Some answers refer only to the order of magnitude of CDF and LERF results, and discuss the relationship between the assessed risk level and the quantitative safety goals (if such goals are in place). Some responses give relative contributions of dominant risk factors without indicating the absolute values of the risk metrics.

Values of importance measures for failure events are given in a few answers. Uncertainty bounds of risk estimates are rarely included; numerical values are mostly limited to listing of point estimates.

6.1. Numerical values

It should be cautioned that direct comparisons of "absolute" values from different PSA studies should be done with care. PSA results can usefully reflect important differences in site characteristics, in plant design, and in operations and maintenance practices. However, variations in results can also arise due to differences in scope of the analysis, in the level of detail in the models, in the types of data used and, most importantly, in the underlying modelling assumptions used during the analysis. These differences may stem from the national regulatory framework for PSA, the licensee practices in developing and using PSA models to meet safety requirements and support safety management throughout the lifetime of an NPP, the maturity of the analysis as determined not only by the maturity of methodology and data but by the plant's life cycle phase the PSA is applied to. An important notice is cited from the previous version of this report (NEA, 2013): "*Contextual information regarding the dominant contributors to risk and the reasons for their dominance (including modelling approaches and key assumptions as well as physical factors) will enable the reader to better compare and contrast study resu*lts". The information considered in the writing of the current report is not sufficiently detailed to support a systematic evaluation of reasons for similarities and differences in PSA results reported by member countries. For that reason, the following discussion of results is of a general level.

As to Level 1 PSA, CDF values are in the range of 1.0 E-06/ry to 1.0 E-05/ry, based on the questionnaire responses and supplementary information provided subsequently to receiving the country responses. The key factors affecting the reported CDF estimates are the scope of the analysis (see the scope attributes discussed in Chapter 4) and the design, especially the vintage, of the NPPs. Some countries reported an aggregate (or total) CDF over and above the risk estimates from the different initiating events and hazards (internal or external), but not all the countries provided such aggregate measures. Typically, the method of aggregation was not revealed as it was beyond the scope of the survey. Two countries, the Czech Republic and the Netherlands reported Level 1 PSA results aggregated not only for different initiators but for different release sources, i.e. for the reactor core and for the spent fuel pool as well. However, such kind of aggregation does not seem to be a general practice, and a note should be made that the full area of risk aggregation methodology is subject to development activities at present.

In comparison to Level 1 PSA results, quantitative results of Level 2 PSA are relatively rarely given in the country reports. The conditional probability of LERF (or large release frequency (LRF)) given CDF/FDF is highly plant and site specific and varies significantly over different types of initiators even for the same plant. For example, some plants appear more vulnerable, particularly to external hazards. Another factor that needs to be considered is the definition of large release and large early release. Variations in these definitions have been observed, impacting the feasibility of comparing merely LERF or LRF estimates.

It is noted that the CDF and LERF or LRF estimates reported for new Generation III+ plant designs appear substantially lower than those for older designs representing most operating plants. However, the operating experience for the new designs is much more limited, and the risk estimates are predominantly based on design stage PSAs. More consolidated and robust assessments are expected as plants of the new designs enter operational status and as operating experience accumulates.

All the results given in the country contributions and summarised in this chapter are for single plants, and most of them are related to single sources of radiation, except for a few cases. If the risk measures – either CDF or LERF – are aggregated over fleets, then the figures get less favourable, i.e. the numbers are not as small any more than those that can be observed for single plants/sources. This aspect needs to be taken into account when judging the degree and significance of nuclear risk. Another important aspect is the fact that, by the nature of this art, the probability of an event with undesired consequences increases monotonically over time, unless safety improvements are made to the fleet members. This feature plays a role in answering the question: how safe is safe enough?

6.2. Main risk contributors

Similar to the overall risk estimates, the main contributors to risk vary substantially across plants. When given, the risk from fires and external events of various kinds appear quite comparable to or even larger than that of internal events. Increased attention has been paid to risk assessment for external hazards following the Fukushima Daiichi accident, therefore more PSA results are available for these risk contributors. Not only the seismic PSAs have been reviewed but a more comprehensive range of site-specific external hazards have been included in a number of PSA studies since the publication of the previous status report (NEA, 2013).

For several plants (e.g. some NPPs in Belgium, the Czech Republic, Finland and Hungary) the annualised risk from low power and shutdown states, i.e. the quantified average annual CDF is quite comparable to the risk from plant operation at full power according to the latest results documented in the country responses. For the Loviisa plant in Finland the low power and shutdown CDF is assessed even higher than the full power CDF.

New developments can be observed in PSA for the spent fuel pools, and the results suggest that damage of fuel in the spent fuel pool can be a significant risk contributor as well. Although the results of spent fuel pool PSA have been reported by only a few countries (a lot less than the number of countries refer to either completed or ongoing efforts in this area), it is noted that the values of fuel damage frequency (FDF) provided are in the same order of magnitude than the CDF estimate for some plants. Vulnerability of the spent fuel pool to loads induced by internal and external hazards and limitations in the capability of the plant to prevent off-site releases following fuel damage in the spent fuel pool can be important safety issues for plant designs where the spent fuel pool is not within the enclosures of the containment building.

Containment failure modes and release categories associated with large releases or large early releases are included only in a few country responses. In addition to the failure modes associated with atmospheric releases, basemat melt-through is also indicated as an important contributor to the Level 2 PSA results (e.g. for some Belgian plants).

6.3. Overall conclusions

As in the previous report on the status of PSA programmes (NEA, 2013), the presentation of PSA results is quite heterogeneous across countries and across plants. Since the purpose, scope, maturity and modelling assumptions of PSA can differ, comparisons of PSA results and risk profiles should be made with considerable caution. Generally, the results and insights from Level 1 PSA have been reported in more detail than the Level 2 PSA, although the discussions on Level 1 PSA results are mostly limited to the reactor PSA, and less attention has been paid to spent fuel pool PSA. The CDF values are in the range of 1.0 E-07 /ry to 1.0 E-04 /ry. These figures are necessarily site and plant specific. Level 3 PSA results have not been reported, except for the United Kingdom. When reported, the risk from fires and external hazards of various kinds appear quite comparable to or even larger than that of plant internal events. Since increased attention has been paid to risk assessment for external hazards following the Fukushima Daiichi accident, more PSA results are available for these risk contributors.

7. PSA applications and decision making

7.1. Summary

In NEA member countries with operating nuclear power plants (NPPs), the probabilistic safety assessment (PSA) is used as a risk-informed decision-support tool to enhance a nuclear plant’s design and operation. In many countries, PSA is also used as part of a safety case demonstration (e.g. as required by a PSR process). In some countries, PSA is to support requests for changes in regulatory requirements. These applications have been ongoing for many years. However, since the last version of this report, the applications have been increasing in number and visibility. For example, as discussed in Chapter 2, PSAs were used to support member country stress tests performed in response to the Fukushima Daiichi accident.

Current PSA applications include the support of: design evaluations, severe accident management, risk monitoring, categorisation and prioritisation of plant equipment, modification of plant technical specifications, online maintenance, pipe inspections, operating experience analysis and various regulatory activities. As with previous years, these applications involve the use of PSA in a risk-informed decision-making framework, where PSA insights are used together with other relevant information (e.g. deterministic analysis results) and considerations (e.g. safety margins, defence in depth, current regulatory requirements, monitoring requirements).

7.2. Evaluation of design

Design evaluation is a frequent and important application of PSA. The insights from PSA, used in combination with those from the deterministic analysis, form an integrated approach to safety. Within this framework, PSA is used to:

- identify the dominant contributions to the overall risk (generally measured by CDF and or FDF and/or L€RF);
- identify weaknesses in the design and operation of the plant; and
- determine whether the design is balanced from a risk point of view.

As discussed in previous chapters, the scope of the PSAs for many NPPs has increased over the last five years. In particular, a number of PSAs have been extended to include external hazards, low power and, shutdown conditions, new sources of risk (such as the SFP), and release-related risk metrics (as determined by Level 2 PSA). Such increases of PSA scope have helped to identify additional weaknesses in plant design and operation and resulting improvements (e.g. increasing of redundancy and diversity of structures, systems, and components (SSC) important to safety, providing additional means for power supply, including mobile sources, providing means for coping with external hazards and ensuring adequate safety functions (e.g. fume cooling towers for ultimate heat sink at the Dukovany NPP) have led to enhanced plant capabilities.

Nowadays, PSAs are used to support decisions on operational and design issues that may have a strong impact on the economic performance of a nuclear power plant. Examples include increasing core power levels and design changes supporting plant life extension. Recent uses of PSA also include unique applications supporting recovery from the consequences of safety significant events.

In many cases, PSA is also an important part of the design and licensing processes of new plants. Here, it may be used for designing and optimising the facility during the design phase with the aim to reach a reasonably balanced risk profile of the design. In the United States, for example, the final safety analysis report (FSAR) submitted as a part of the Design Certification application for LWRs must contain a description and analysis of design features for prevention and mitigation of severe accidents, which is based on PSA. In France, PSA contributions address many items important for the design stage; a specific example is the commissioning of Flamanville Unit 3, where PSA is used to demonstrate the compliance of a new NPP with the assigned safety objectives.

7.3. Enhancement of managing potential accidents and their consequences

Level 2 PSA has been often used recently to identify severe accident management measures. An important part of such efforts has been to support the implementation of generic or plant-specific Severe Accident Management Guidelines (SAMGs). In Paks NPP, Hungary, the use of PSA in support of severe accident management has been of particular importance. The PSA-based, systematic approach was divided into three steps:

1. Selection of feasible and effective measures;
2. Prioritisation of measures from a risk reduction point of view;
3. Development of technical requirements for certain measures.

PSA results have also highlighted the need for additional dispositions in case of multiple failures. For example, in France, Level 1 PSAs covering internal events have been used to define lists of "Design Extension Conditions" (DEC) and PSA insights have been used to demonstrate the acceptability of additional dispositions and to define requirements associated with these dispositions.

PSA has also been used at many plants to provide input to the training programme of control room crews. The aim has been to focus the training on risk significant SSCs, accident scenarios, maintenance activities, etc. In particular, PSA has been used to support (in a risk-informed manner) the prioritisation of scenarios to be addressed by simulator training. As an example, PSA insights are used in France in the of operators training, consistent with WENRA Safety Reference Level O3.5 ("Insights from PSA will be shared as input to development and validation of the safety significant training programmes of the licensee, including simulator training of control room operators") (WENRA, 2014).

7.4. Risk monitoring

Risk monitoring is a widely-accepted PSA application that provides straightforward support of risk-informed decision-making at NPPs. Risk monitors are now in operation at a very large number of plants in member countries. The monitors are typically not installed at the shift supervisor's or safety engineer's main control room table but are used by engineers to support plant management on day to day decisions on changes in configuration of available plant equipment (initiated mainly by maintenance activities). The typical goals of using risk monitors are:

- to avoid simultaneous components unavailability that would lead to a high instantaneous risk (i.e. a risk peak);
- to plan maintenance outages in order to minimise any risk increases;
- to monitor the plant performance over time by addressing the cumulative risk.

A new idea of growing popularity is using risk monitors in training, since they may give a direct indication of how plant activities affect the risk of operation. Other applications of risk monitor in the field of (online) maintenance are given below.

7.5. Categorisation and prioritisation of plant equipment

PSA results and insights, along with the deterministic insights, are being used to prioritise SSCs for enhanced treatment (e.g. testing requirements, monitoring and surveillance in support of ageing management).

As an example of a risk-informed approach, the significance of a component can be assigned using PSA-developed importance measures for that component. For example, components with a high Fussell-Vesely importance or a high risk achievement worth can be tentatively classified as having the highest significance, subject to considerations of factors not addressed by the PSA. Guidance for combining both probabilistic and deterministic insights to group SSCs into four categories according to their safety significance is given in NEI 00-04 document “10 CFR 50.69 SSC Categorization Guideline” (NEI, 2005).

The topic of categorisation of plant equipment is very closely connected with PSA applications in maintenance. Many utilities apply PSA results in programmes for monitoring maintenance effectiveness, performed to ensure that SSCs are capable of fulfilling their intended functions, with the highest priority put upon the most risk significant SSC. In the United States, per the requirements of 10 CFR 50.65 (the “Maintenance Rule”) (NRC, 2017), licensees must assess and manage the risk of maintenance activities performed during all conditions of plant operation, including normal shut down 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. Korea is another example of a country where the principles of risk-informed maintenance are applied broadly. Spain provides yet another example, where all NPPs use a risk monitor to manage maintenance activities under maintenance rule requirements during at-power operation, as required by the Spanish regulatory authority (CSN). In all cases, any possible irregularities in the risk profile provide immediate inputs for the decision-making process.

7.6. Development and use of plant technical specifications

Plant Technical Specifications (TS) 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, current PSA models are used to justify and optimise the LCOs, AOTs and STIs. PSA is also often used to justify proposed changes to the TS.

Regarding plant TS, PSA can identify situations for which a plant shutdown could cause higher risk than continuing power operation while fixing the failures online. For example, when systems used for decay heat removal are seriously degraded, it may be safer to continue operation than to shut down the plant immediately, although such shutdown may be required by the TS (which were developed based on a deterministic approach). In such cases, PSAs have been used to justify requests for regulator discretion in the enforcement of the normal TS requirements.

7.7. Supporting the introduction of online maintenance

The use of PSA for supporting the maintenance of plant equipment during power operation (i.e. online maintenance) is an important application for plant management, because it can provide useful support for changes that may have positive economic impacts (by shortening outages) without contradicting safety requirements. In some specific cases, it has been demonstrated that shifting of maintenance of equipment from plant shutdown to the full-power operation may not necessarily lead to a cumulative increase in risk.

Risk monitors are often used to support on-ine maintenance execution as well as planning. In the Czech Republic, for example, on-ine maintenance during full-power operation is allowed for selected systems (e.g. service water), but PSA specialists are obliged to be continuously on duty in case there is a need to evaluate the risk of any new configuration of plant equipment, which may occur incidentally due to some unexpected event (component failure). The Krško NPP (Slovenia) is another plant, where risk monitor is broadly used for supporting online maintenance.

7.8. Pipe inspection programmes

To optimise piping inspection programmes, risk-informed in-service inspection programmes have been carried out in several plants. Both the Westinghouse and the EPRI methodologies have been applied in development of such programmes in OECD countries. The US NRC has also approved RI-ISI programmes based, in part, on ASME Code Case N-716 (NEA, 2017), identifying segments of piping that are generically considered high-safety-significant (HSS). Internal hazards PSA devoted to flooding PSA has been then used to identify any additional, plant-specific HSS segments.

As another example, the principles of RI-ISI are broadly applied in Spain. Three plants operate the RI-ISI programmes at least for Class 1 piping. The Cofrentes NPP (Spain) runs the broadest RI-ISI programme covering Class 1 and Class 2 piping, motor-operated, pneumatic, solenoid and check valves, and motor-driven pumps.

7.9. Analysing plant operating experience

PSA-based analysis of operating events has long been an activity in many countries supporting the broader task of analysis of operating experience. Typically, PSA models are used to estimate the conditional core damage probability (CCDP), a measure of how much the plant’s safety margin was reduced due to the specific features (e.g. equipment failures, operator errors) of the event. (In the case that an event involves a discovered degraded condition rather than an operational transient, the change in core damage probability (delta CDP) can be used as a measure of significance.)

The US NRC uses PSA models to support decisions regarding the appropriate response to a reported incident or an inspection finding. In particular, the value of CCDP or delta CDP, determined using the Standardized Plant Analysis Risk (SPAR) model for the NPPs involved, is considered when determining the type of inspection team to be sent for follow-up investigation. PSA results are also used in establishing performance indicators used to identify trends in plant safety. For example, the Mitigating Systems Performance Index (MSPI) is used to follow safety systems unavailability in the US plants. As another example, the US NRC also calculates an annual Accident Sequence Precursor Index based on the CCDPs and delta CDPs for that year's events. Although some questions have arisen concerning the interpretation of this index, it has recently been decided that the index is a useful tool and it will continue to be published in annual reports.

In France, the analysis of NPP operating events has a long tradition and is also performed in a comprehensive systematic way (by EDF and IRSN). In the approach used, an operating event is considered as "precursor" when CCDP for the event is greater than 1.0 E-06. Moreover, for the most important events with CCDP higher than 1.0 E-04, the Safety Authority requires the utility to define short term corrective measures and to assess and address the corresponding risk reduction explicitly.

7.10. Supporting the role of regulatory authorities

The PSA applications listed above are broadly used by the utilities, but some of them have also direct impact on the work of regulators, where the risk inputs play more and more important role. In general, the risk information provided by the PSA has been increasingly used by regulatory authorities in planning their activities related to

- prioritisation of tasks so that they focus on risk significant issues;
- determining the significance of inspection findings;
- regulator response to non-compliances.

An example of such effort is large Reactor Oversight Program (ROP) carried out by US NRC. The oversight process provides a means to collect information about licensee performance, to assess this information for its safety significance, and to provide for appropriate licensee and NRC response. Because there are many aspects of facility operation and maintenance, the NRC inspects utility programmes and processes on a risk-informed sampling basis to obtain representative information. PSA results are used in many ways to support the oversight programme including inspection planning and determination of risk significance of inspection findings.

Similar processes to this are carried out in other countries. In Finland, decommissioning-related risks are analysed by the regulator (STUK) to ensure risk-informed NPP decommissioning. A risk-informed approach is also used in some countries as an input for changing the regulations. In the United States, this approach has been used to change the regulations related to fire protection, combustible gas control, emergency core cooling system requirements and pressurised thermal shocks.

It should be recognised that as the applications of PSA grow, challenges will continue to arise. For example, recent concerns about the uncertainties and potential biases in US fire PSAs have led to considerable discussion between the NRC and the nuclear industry. This discussion concerns not only areas of needed technical improvement (see Chapter 8), but also associated regulatory process questions (e.g. how a new method or model can be approved for use in a timely fashion, how the risk estimates from different hazards should be aggregated and contextualised, how uncertainties in PSA results should be accommodated).

8. Future developments and research

Several research and development activities are ongoing in the Working Group on Risk Assessment (WGRISK) member countries. These mainly focus on extending the scope of the probabilistic safety assessment (PSA) and closing existing gaps in PSA methods and data.

8.1. PSA scope extension

The activities cover systematic PSA extensions with regard to internal and external hazards including consideration of event combinations of hazards that may even affect not only one reactor unit but the whole site. This gap in PSA has been recognised in the frame of several national as well as international activities after the reactor accidents at Fukushima Daiichi in 2011, such as the post-Fukushima stress tests, but also in the frame of other activities like the ASAMPSA_E project of the European Commission (EC) (Wielenberg et al., 2016) or the WGRISK workshops on Natural External Hazards PSA (NEA, 2014) and Fire PSA (NEA, 2015).

The application of the updated WENRA Reference Levels (WENRA, 2014) is expected result in a better and more systematic consideration of all plant operational states (POS) and systematic consideration of the spent fuel pool (SFP) in PSA.

Moreover for a number of issues identified from the operating experience on a national or international basis R&D activities will be extended as well. These include, for example, initiating events at support systems, loss of offsite power (LOOP)/station blackout (SBO), addressing uncertainties adequately and exhaustively, and HRA analysis.

8.2. External hazards

The extensions cover a broad range of hazards, including volcanoes (Chinese Taipei), hydrological and other weather induced hazards (Finland, Germany, Japan, Switzerland, the United States) including, in some cases, extreme sea water levels and the effects of global warming. The extensions generally require updates of the supporting probabilistic hazard analyses (e.g. for seismic and for external flooding hazards) and multiple hazard combinations (e.g. seismically-induced fire and flooding in Japan, all types of hydrological events in Germany and the United States). Related PSA research activities concern the improvement of PSA methods for addressing equipment fragilities, as well as plant and operator response. These activities will need to consider the demands of Level 1, Level 2, and Level 3 PSA for all plant operational phases (full power as well as low power and shutdown, including the longer term post-commercial safe shutdown phase).

8.3. Site-level PSA

Currently unresolved issues including safety improvements resulting in particular from the post-Fukushima stress tests, including optimisation for both severe accident and off-site consequence analyses, are receiving high priority in member countries. Site-level (multi-unit, multi-source) PSA research activities are also underway in various countries (e.g. Canada, Finland, Germany, Hungary, Korea and the United States).

A clearly identified issue for R&D, as confirmed by the International Workshop on Multi-Unit Probabilistic Safety Assessment (CNSC, 2014) workshop, is the problem of risk aggregation (how to combine risk related to sequences assessed with a very different level of conservatism and uncertainty?).

Another issue relates to multi-sources interactions and dependencies with in particular the problem of multi-unit common-cause failures and common-cause failures between a large number of equipment's.

8.4. PSA Level 2 and 3

R&D projects are intended or already ongoing for extensions of Level 2 and Level 3 PSA regarding the state of the art (e.g. Hungary).

For analysing specific improvements requested after Fukushima, e.g. filtered containment venting, CFD (Computational Fluid Dynamics) are being used together with thermal-hydraulic codes such as MELCOR (e.g. Mexico, Germany). Such tools are also being used to analyse Melt-Structure-Water Interactions (MSWI) that may occur during the late phase of in-vessel core melt progression and during ex-vessel melt progression (e.g. Switzerland). Adequate modelling of these physical processes is needed in order to support Level 2 PSA.

Other research activities cover response to severe accident emergency situations and improvements with respect to off-site consequence analysis (e.g. Korea, Germany) and modelling mitigating strategies. These developments will support plans for accident and severe accident management.

In the United States the NRC is conducting a full-scope, comprehensive Site Level 3 PSA. This PSA will address all the site radiological sources, all the Initiating Events, all the operating states, and level 1, 2 and 3 PSA (full consequence analysis).

8.5. Human Reliability Assessment (HRA)

HRA is still a topic requiring research and development. In particular two areas of development are HRA for Level 1 and Level 2 PSA for all POS, including longer duration post-operational safe shutdown, and HRA for external hazards PSA (e.g. Canada, the Czech Republic, Finland, France, Germany, Slovenia, Spain, Switzerland and the United States).

8.6. Digital I&C

In light of new reactors being built and analogue control room equipment more and more being replaced by digital I&C systems, the need for R&D on digital I&C including man-machine interface and human reliability in control rooms has been recognised. Activities on a national as well as international basis are ongoing (e.g. the Czech Republic, Finland, France, Germany, Korea and the United States) for analysing digital I&C reliability.

8.7. Dynamic PSA

The issue of order and timing of events during accident sequences was in particular underlined in the Report on PSA Insights Relating to the Loss of Electrical Sources (NEA, 2017).

Some countries (e.g. Finland, France, Japan and Mexico) are planning to use, or at least consider to use, Dynamic PSA (or some approach for taking into account the dynamic aspect of the sequences). Applications include the assessment of the impact on plant safety margins in case of plant modifications, the treatment of the effects of human actions at different points in time during a complex scenario and the treatment of recovery possibilities (for example by mobile systems).

8.8. Other issues

Significance of design extension conditions (DECs) and the effects of design improvements on the PSA results (e.g. in Korea) haves been identified and will also be incorporated in PSA activities.

In a few countries (e.g. India and the Netherlands), PSA for research reactors is ongoing. In Germany, for example, a graded PSA approach for a research reactor is under development.

8.9. PSA for new designs

Several countries are actively pursuing PSA activities relevant to new build, such as new CANDU, ABWR, EPR, APPR1400 and AP1000 reactors. For example, some countries are providing PSA support to the ALLEGRO project, which is developing a demonstration Generation IV gas-cooled reactor (Czech Republic, Slovak Republic and Hungary). As another example, in the United Kingdom, following the Generic Design Assessment (GDA) process for the new reactor designs, full-scope site-specific PSA studies are intended to be performed in order to support detailed design, construction, commissioning and operation of these reactors according to the state of the art including site-specific characteristics, consideration of multi-unit aspects, operational matters and PSA applications. In France a PSA is developed for the design of the French GEN IV Sodium Fast Reactor prototype ASTRID.

In a few countries (e.g. India and the Netherlands,), PSA for research reactors is ongoing. In Germany, for example, a graded PSA approach for a research reactor is under development.

9. International activities

All the responding countries indicate involvement in several PSA-related international activities. These international activities can differ by the size of the group (number of countries involved), by the existence of a common topic (similar installations, similar field of interest), or by particular objectives. The main features of the international activities, as mentioned by the respondents, are summarised below.

9.1. Size of the international groups: Number of countries involved

The international activities could concern a very large number of countries, more limited groups or only bilateral co-operation.

Most or all responding countries are involved in PSA-related activities involving a large number of countries. In addition to WGRISK, these include NEA joint Data Projects and Working Groups (WGAMA, WGEV, WGHOF and WGIAGE). Many countries also support IAEA activities (development of Safety Guides, TECDOCs, etc.) and major international conferences and meetings (e.g. PSAM, ANS PSA, ESREL and Nordic PSA Meetings).

Other international activities concern a more limited set of countries. Notable examples include several European activities (WENRA RHWG, the EC project ASAMPSA_E, etc.), the Nordic PSA Group (mentioned by Finland and Sweden), the Asian Symposium on Risk Assessment and Management (ASRAM).

Several countries indicate also bilateral co-operation. For example, US NRC Office of Nuclear Research (RES) has implemented over 100 bilateral or multilateral agreements with more than 30 countries.

9.2. Objectives

The general common objectives of the entire international activities are to provide mutual help and support general progress in the PSA field. Some examples of specific objectives indicated in the responses are:

- Exchange of information (the main general objective, for example the WGRISK activities and the large PSA international meetings).
- Knowledge transfer (e.g. IAEA PSA training courses).
- Peer reviews (IAEA IPSART service).
- Harmonisation MDEP, IAEA CANDU PSA Working Group (CPWG)).
- Data collection (NEA joint Data Projects, Nordic data collection).
- Common products (Guides, SOAR reports, etc.), common research (Halden Reactor Project (HRP)), common project (Hinkley Point EPR), common research contracts (such as ASAMPSA_E of the European Community).

9.3. Topics of international activities

Many of the member country international activities are driven by a common type of problem, for example PSA for similar types of installations, specific PSA challenges, and problems arising particularly after Fukushima:

9.4. Common types of installation design

- VVER: the VVER group is mentioned by Hungary and the Czech Republic;
- CANDU:
  - CANDU Owners Group (COG) mentioned by Canada and Korea;
  - IAEA CANDU PSA Working Group (CPWG): mentioned by Canada;
  - CANDU PSA Working Group (CPWG) mentioned by Korea;
- BWRs:
  - BWROG (Japan);
  - European BWR Owners Group;
- New designs: the MDEP PSA subgroup relates to new designs, and in particular to the EPR design (France, Finland).

9.5. Specific topics

Although in general international activities cover many PSA topics (very general scope, for example the WGRISK), in some cases the topic is more specifically identified:

- HRA (for example presented by France and Switzerland);
- Fire;
- Seismic;
- Severe accidents (PSA Level 2/3);
- Precursors events (workshops organised by Belgium);
- Dynamic PSA;
- Open PSA.

9.6. Common problems after the Fukushima Daiichi reactor accident

Several international activities are related to questions directly related to the Fukushima reactor accidents, particularly the development of external hazards PSA and of Site Level PSA. Generally existing international groups have introduced some particular tasks in relation to the Fukushima accident (e.g. WGRISK Tasks), and moreover, some new international activities have been created, for example the ASAMPSA_E Project (http://asampsa.eu) and the NEA working Group on External Events (WGEV).

9.7. Conclusions

The responses show a large number of international activities in the field of PSA (number of groups or sub-groups, of international meetings). This important level of exchanges could be explained first by the fact that PSA uses a common language and very similar approaches, and has common objectives and needs, for example need of common data collections.

After the Fukushima Daiichi accident, a various new international activities have been established to address key aspects of these aspects, including external events PSAs and multi-unit interactions. Recognising that pre-Fukushima international activities remain important, it is important that existing and new activities be properly co-ordinated. The responses indicate a need and a progress towards harmonisation. The existence of a common state of the art using the best existing practices is an important help for the demonstration of PSA quality and for a more justified use for decision making.

10. Overall insights

10.1. General conclusions

The Nuclear Energy Agency (NEA) Committee on the Safety of Nuclear Installations (CSNI) has recognised that probabilistic safety assessment (PSA) is a very useful tool for sustaining and improving safety. The cross-cutting aspect inherent in PSA means that it provides a large potential for identifying safety priorities. This tool is therefore particularly important for optimisation of safety work. For these reasons, a task was established for the NEA Working Group on Risk Assessment (WGRISK) to present PSA use and development in member and non-member countries, updated appropriately, so as to inform PSA and non-PSA practitioners on the progress in relation to this topic.

The main insights of this last update, presented below, regard the increasing role of PSA in all participants (especially in case of new plants), the effects of the Fukushima Daiichi accident on PSA use and development, and the use of this information for the WGRISK programme of work.

10.2. Increased role of PSA

This overview confirms the general conclusions of the previous version of the report. The position and the role of PSA are increasing in all the respondents and for all PSA aspects:

- Countries' PSA frameworks and environments: more important and precise regulatory requirements are noted. In several member countries, PSA, previously performed on a voluntary basis, has become a regulatory requirement. In particular, in the frame of periodic safety review, an updated PSA is now required in many countries.
- Numerical safety criteria: although there is not much new information since the previous report, for some countries more formal safety goals have been defined. An important point is that there is progress regarding goals for multi-unit sites, where in particular the problem of risk aggregation needs consideration.
- Countries' statuses and the scope of ongoing PSA studies: several new PSAs are mentioned by member countries. In particular, new PSAs are, in most cases, an essential part of the safety assessment for new installations. It should also be noted that many existing PSAs have been or are being updated, in particular to take into account recent plant modifications (post-Fukushima modifications). Moreover, the scope of the studies has often been extended, especially after Fukushima (see details below). The most general PSA scope includes Level 1 and Level 2 (Level 3 remains less systematic) and all reactor operating states. This common scope illustrates the progress towards harmonisation. In addition, in many studies, the scope has been extended to cover sources of radioactivity

other than the reactor core, most notably the spent fuel pool for the reactor, but also intermediate spent fuel storage facilities.

- PSA applications and decision making: PSA applications related to risk-informed design as well as plant operation improvements are more and more numerous, with many concrete and practical examples mentioned by several countries.
  - Several modifications relate to electrical sources where PSA is a tool for assessing the benefit of these improvements.
  - PSA is being used as tool to support accident management, both for prevention and for mitigation of severe accidents (selection and prioritisation of effective measures and corresponding equipment).
  - The use of PSA for operation optimisation (technical specifications, maintenance planning, online maintenance, etc.) is not new but an increasing number of examples are mentioned , often involving the development and use of risk monitors.
  - PSA is often used to provide a basis for prioritisation of plant equipment (priorities for inspections).
  - The use of PSA insights for analysing experience feedback (precursor programmes) is increasingly mentioned as an important application.
  - The use of PSA for optimisation of regulatory activities is now being considered in a number of countries.
- Future research and development: several activities are in progress, involving either the follow-up of ongoing actions or the development of new methods and models. Some but not all of the development activities are linked to the Fukushima Daiichi accident. Assessing the benefit of plant modifications can require some methodological development, and PSA development and application activities are often performed in parallel. (Key development activities are summarised below.)
- International activities: international co-operative activities, involving both small groups linked by a similar design or a particular topic, as well as large international activities (e.g. organised by IAEA or NEA) aiming to share good experience and avoid duplication, are ongoing. International co-operation is often a driver for PSA development and application as well as for harmonisation.

Generally speaking, it clearly appears that this review confirms the conclusions of the previous version of the report. Especially for new plants, PSA is now a necessary part of safety assessment.

10.3. Post-Fukushima effects

Post-Fukushima effects on PSA are indicated by many countries and for various topics. The most frequent post-Fukushima effect on PSA is the extension of the scope of the studies, particularly the extension or re-evaluation of initiating events related to external hazards and hazard combinations, and the treatment of site risk (multi-unit, multi-source PSA with consideration of all main radioactive sources, including reactors, spent fuel pools and intermediate spent fuel storage facilities).

It should be noted that:

- For many sites, several studies had already been completed or were in progress (e.g. external hazards, LPSD or SFP PSA) prior to the Fukushima accident. Nevertheless, after the reactor accidents at Fukushima, these studies were often revised and improved (this is indicated in particular for seismic PSA).
- Other safety significant issues (not linked to Fukushima) are also the subject of important work (fire, HRA, digital I&C, etc.).

The topics that can be considered as new after Fukushima are: 1) the large number of external hazards considered within PSAs; and 2) risk assessment applied with a site perspective (including multiple units, SFP and other facilities).

Regarding external hazards, long lists of external hazards or combinations of hazards have been previously investigated with more or less formal screening criteria. However, to date, few concrete results have been obtained. Generally, the studies have been limited to demonstration-level assessments of the initiating event frequency with the objective of showing that various hazard/hazard combinations can be screened out. In some instances, more complete PSAs have been performed for severe weather phenomena such as tornado or extreme temperature.

Regarding site PSA, important issues of interest to member countries include the questions of how to combine risks ("risk aggregation"), what are appropriate targets (i.e. site safety goals), and what are the multi-sources interactions and dependencies (e.g. common-cause failures).

Another topic with a link to Fukushima is the analysis of long duration sequences (in particular loss of off-site power [LOOP] sequences). More generally, it is recognised that detailed treatment of the order and timing of events during the sequences can be an issue for PSA research and development.

10.4. Use of the report by WGRISK

As previously, the NEA, and the WGRISK in particular, will use the results of this report to monitor the conduct of its ongoing activities, and to promote and implement new international collaborative efforts within the framework of the CSNI. For example, reflecting the topics of external events and Site PSA discussed above, the following ongoing activities should be noted:

- The task "Human Reliability Analysis in External Events PSA – Survey of Methods and Practice" initiated in 2015 is nearly completed.
- The task "Status of Site Level PSA (including Multi-Unit PSA) Developments", which also started in 2015 is aiming on exchanging information, how multiple reactor and multiple radioactive source issues are addressed in risk analyses carried out in member countries, identifying key challenges (including risk aggregation) and ongoing research activities for Site Level PSA. The corresponding task report is intended to be published in 2019.

Also mentioned above, important PSA topics with no particular link with Fukushima are being addressed. Examples include an updating of the technical opinion papers (TOP) on fire PSA and seismic PSA and a benchmark task relating to the modelling of digital I&C.

Regular updates of this report are an important precondition for maintaining its usefulness. Some important facets of PSA and PSA results will need to be addressed in future updates. For instance, based on the experience gained thus far, more attention should be paid to uncertainties in PSA, including not only methodological aspects but reporting on quantified measures of uncertainty as obtained in the different PSA studies covered in the present report.

References

Canadian Nuclear Safety Commission (CNSC) (2014): “Summary Report of the International Workshop on Multi-Unit Probabilistic Safety Assessment”, CNSC, Ottawa.

Idaho National Engineering and Environmental Laboratory (INL) (1999): Rates of Initiating Events at US Nuclear Power Plants: 1987 – 1995, NUREG/CR-5750, INEEL/EXT-98-00401, United States Nuclear Regulatory Commission (NRC), Washington, DC, United States, www.nrc.gov/docs/ML0705/ML070580080.pdf.

IAEA (1999): Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, A report by the International Nuclear Safety Advisory Group, Vienna, Austria. www-pub.iaea.org/MTCD/publications/PDF/P082_scr.pdf.

IAEA (2006): *Fundamental Safety Principles*, IAEA Safety Standards Series No. SF-1, Vienna, Austria.

IAEA (2012-2013): DRAFT TECDOC “Development and Application of a Safety Goals Framework for Nuclear Installation”, Vienna, Austria.

NEA (2002), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): “The Use and Development of Probabilistic Safety Assessment in NEA Member Countries”, NEA/CSNI/R(2002)18, OECD Publishing, Paris. www.oecd-nea.org/nsd/docs/2002/csni-r2002-18.pdf.

NEA (2007), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Use and Development of Probabilistic Safety Assessment*, NEA/CSNI/R(2007)12, OECD Publishing, Paris. www.oecd-nea.org/nsd/docs/2007/csni-r2007-12.pdf.

NEA (2009), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Probabilistic Risk Criteria and Safety Goals*, NEA/CSNI/R(2009)16, OECD Publishing, Paris.

NEA (2011): *The Structure and Application of High Level Safety Goals – A Review by the MDEP Sub-committee on safety goals*, OECD Publishing, Paris.

NEA (2013), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Use and Development of Probabilistic Safety Assessment: An Overview of the Situation at the End of 2010*, NEA/CSNI/R(2012)11, OECD Publishing, Paris. www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=NEA/CSNI/R(2012)11&docLanguage=En

NEA (2014), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Probabilistic Safety Assessment (*PSA*) of Natural* External *Hazards*

Including Earthquakes. *Workshop Proceedings*, Prague, Czech Republic, 17-20 June 2013, NEA/CNRA/R(2014)9, OECD Publishing,Paris, www.oecd-nea.org www.oecd-nea.org/nsd/docs/2014/csni-r2014-9.pdf.

NEA (2015), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Proceedings of International Workshop on Fire PRA*, NEA/CSNI/R(2015)12, OECD Publishing, Paris, www.oecd-nea.org/nsd/docs/2015/csni-r2015-12.pdf.

NEA (2017), Committee on the Safety of Nuclear Installations (CSNI) Working Group on Risk Assessment (WGRISK): *Probabilistic Safety Assessment Insights Relating to the Loss of Electrical Sources*, NEA/CSNI/R(2017)5, OECD Publishing, Paris.

Nuclear Energy Institute (NEI) (2005):*10 CFR 50.69 SSC Categorization Guideline*, NEI 00-04, Washington, DC, United States, www.nrc.gov/docs/ML0529/ML052910035.pdf.

Western European Nuclear Regulators Association (WENRA) (2010): WENRA Statement on safety objectives for new nuclear power plants.

Western European Nuclear Regulators Association (WENRA) (2014): RHWG *Report WENRA Reference Safety Levels for Existing Reactors*, Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf.

Wielenberg, A., et al. (2016): *Risk Metrics and Measures for an Extended P*SA*,* Technical report ASAMPSA_E/WP30/D30.5/2016-17 Advanced Safety Assessment Methodologies: Extended PSA (ASAMPSA_E). European Commission (EC), Petten, the Netherlands, http://asampsa.eu.

United States Nuclear Regulatory Commission (NRC) (2017): *Requirements for monitoring the effectiveness of maintenance at nuclear power plants*, 10 CFR 50.65, Washington, DC, www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0065.html.

Appendix A

CONTRIBUTORS

Belgium

Canada

Chinese Taipei

Czech Republic

Finland

France

Germany

Hungary

India

Italy

Japan

Korea

Mexico

Netherlands

Poland

Slovak Republic

Slovenia

Spain

Sweden

Switzerland

United Kingdom

United States

BELGIUM

1. INTRODUCTION

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 review (PSR) has to be performed every ten years. In this context, a plant-specific internal events PSA (during power and shutdown states) has been performed for each plant. Also the PSA update process (for the upgrade of methodologies and the update of data) is linked to the periodic safety reviews, although intermediate updates (only for data) are also foreseen.

Since 2011, the development of Level 1 and Level 2 PSA models for internal events (including internal fire and flooding events) for NPPs is required by the Belgian legislation (R.D. of 30 November 2011: Safety Requirements for Nuclear Installations). The utility is also required to use these PSA models to identify the weaknesses in the design or operation of the power plants and to assess the need for modifying systems, procedures or operating practices. The PSA shall also be used to assess the adequacy of modifications to the plant, in procedures and in technical specifications, and to study the significance of operational events.

A phase out of the nuclear energy has been decided in the last years. The building of any new NPP is thus not foreseen in Belgium.

The Belgian NPPs are regrouped on two sites (Doel and Tihange). The PSAs for the Doel and Tihange nuclear power plants (which are pressurised water reactors) are performed by Tractebel Engineering, the architect-engineer of these plants, on behalf of the utility Electrabel. Bel V, as subsidiary and technical support of the Federal Agency for Nuclear Control (FANC), is performing an online regulatory review of the development and the updating of the PSA models. This means that technical documents (e.g. proposed methodologies, documents describing event trees construction, system reliability studies) are transmitted continuously to Bel V for review. They are discussed with Electrabel (with the support of Tractebel) on an interactive basis. At the end of each

PSA project (after publication by Electrabel/Tractebel of the final report) Bel V establishes a PSA evaluation report.

After the Fukushima Daiichi accident, several safety improvements have been implemented on each site, however, they are not yet reflected in the current PSA models. Indeed, the most recent Level 1 PSA models are based on the design of the plant as it was at the beginning of 2010. The plant modifications performed since 2010 are being implemented in the current update of the PSA models. In parallel, PSA models are also developed for internal fire and internal flooding.

The Level 2 PSA studies are performed for four representative units (i.e. Doel 1-2, Doel 3, Tihange 1 and Tihange 3). The last Level 2 PSA models in date are valid for the plant design at the beginning of 2010. All the Level 2 PSA models include identification of containment failure modes and radioactive release categories for both power and shutdown states.

3. SAFETY CRITERIA

Except for the evaluation of the required protection against external man-made hazards (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). PSA is used to show that the risk of the NPP's is well balanced, to identify the important contributions to the CDF and to support the decision-making process.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

As already mentioned in § 2, an update of the Level 1 and Level 2 PSA models (for all units) is ongoing. The purpose of this update is to make to PSA models representative of the plant status of 1st January 2015, to update the data (e.g. the initiating event frequencies) and to upgrade some methodologies (e.g. the HRA methodology). Also, the possibility of identifying additional initiating events is considered.

Currently, the efforts are placed on the integration of Internal Fire and Flooding hazards in the PSA models. Some results have already been obtained for the Internal Flooding PSA studies.

5. PSA METHODOLOGY AND DATA

PSA standards and guidance

Neither national standards, nor national regulatory guides have been developed in the area of PSA. No specific guidelines (either national guides or guides from international organisations or other countries) have been indicated as being strict guides to be followed for the PSA analyses of the nuclear power plants. Nevertheless, state-of-the-art methodologies are used, and for this purpose several reference documents are considered (IAEA standards, EPRI guidelines, NUREGs, etc.). This is further detailed hereafter.

Level 1 PSA

In the PSA models, power and shutdown states are analysed, represented by 6 Plant Operating States (POS) covering about 99% of the operating profile of the NPPs. A wide scope of internal initiating events is covered, including LOCAs, secondary line breaks, primary and secondary transients, and loss of particular support systems (electric sources, heat sink, compressed air, etc.).

For the main tasks of the Level 1 PSA (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. In particular, the following sources of data have been considered:

- Reliability Data of Components: version 6 (version 8 for the ongoing PSA update) of the T-Book ("Reliability Data of Components in Nordic Nuclear Power Plants") is used to the extent possible, and otherwise (i.e. for components not represented in the T-Book) US and French databases are exploited;
- Common cause failures: NUREG/CR-5497 or its updated version from 2003 (the CCF-modelling is based on the Alpha Factor Model and uses generic CCF-parameter data);
- Initiating Event frequency: either generic data (NUREG/CR-5750), or plant-specific data, or a combination of both (plant-specific data used for a Bayesian update of generic data); for some Initiating Events, the frequency is determined by means of a fault tree model;
- Unavailability data due to preventive/corrective maintenance or test: based on plant-specific input;
- Time spent per Plant Operating State: based on plant-specific input;
- Human Reliability Analysis: pre- and post-initiating event human errors are modelled by using a methodology that is largely based on THERP and SPAR-H methodologies (the latter for the current PSA update only) ;
- Thermal-hydraulic calculations (using the RELAP code) have been performed to determine success criteria and intervention times. These calculations were performed for representative sequences in the event trees.

For Doel 1 and 2, which are twin units, particular attention had to be devoted to the modelling of shared systems configurations for the various POS combinations.

Concerning the internal hazards:

- The Internal Fire PSA is mainly based on the guidelines presented in NUREG/CR-6850 and NUREG/CR-1921;
- The Internal flooding PSA is based on the EPRI guideline 1019194.

Finally, as mentioned previously, the quantification of the results of the Level 1 PSA models is performed with the RiskSpectrum software.

In 2011, a peer review of the Level 1 and Level 2 PSA models of the KCD3 unit has been performed by an external company. The conclusions of this review have been used as input for the current PSA update.

Level 2 PSA

Regarding the Level 2 PSA, the analyses of internal events have been performed for Doel 1/2, Doel 3, Tihange 1 and Tihange 3, for both power and shutdown states. The

Doel 3 and Tihange 3 Level 2 PSA models are considered as representative of the Doel 4 and the Tihange 2 units respectively.

For internal fire and flooding events, the Level 2 PSA is currently developed for Doel 3 only.

For all Level 2 PSA sequences, the containment failure modes, along with the release categories in the Early and Late phases (i.e. before and after vessel failure) have been characterised.

Similarly to Level 1 PSA, reference documents (NUREGs, IAEA guidelines, ASAMPSA2 guidelines, etc.) have been considered for the Level 2 PSA tasks. Methodologies have been developed regarding the L1/L2 PSA interface processing, the containment isolation assessment, the human reliability analysis and the basic event quantification.

- It has to be noted that the Level 1 PSA and the Level 2 PSA models are processed separately with different software tools, i.e. RiskSpectrum and EVNTRE respectively. Thus a Level 1/Level 2 PSA Interface is necessary to transmit Level 1 PSA sequences to the Level 2 PSA by means of the definition of Plant Damage State (PDS). A transition event tree is built, covering most PDS Attributes, and processed with RiskSpectrum.
- The Level 2 PSA accident progression analysis makes use of a large and detailed accident progression event tree (APET), which is more or less similar to the approach of NUREG-1150;
- Human Reliability Analysis: the methodology for PSA Level 2 is largely inspired by the SPAR-H methodology.
- Basic event quantification is based on supporting calculation results (e.g. MELCOR calculations), or expert judgement techniques, or international literature findings on severe accident phenomenology (e.g. documents issued by OECD, IAEA, USNRC)

Finally as mentioned previously, EVNTRE is used as software for the Level 2 PSA models.

6. NOTABLE RESULTS OF PSAs

Level 1 PSA – internal events

The main insights related to the CDF are:

- The most contributing POS is the POS A;
- The loss of Component Cooling Water System (CCWS) or Essential Service Water System (ESWS) as an initiating event is a major contributor to the total CDF;
- The LOCA family and the LOOP event are also important contributors to the total CDF.

During the analysis of the results, the study of additional indicators is also performed:

- Importance analysis: based on the Risk Increase Factor (RIF) and the Fussel Vessely (FV) factor. The definition of the importance of a failure mode to the total PSA result is the following:
- Fussell Vessely is greater than 5E-03: the failure mode of the equipment is High Safety Significant
- Risk Increase Factor greater than 2: the failure mode of the equipment is Medium Safety Significant
- Other cases: the equipment is Low Safety Significant.
- In most units, the emergency diesel generators are most important from the PSA L1 point of view.
- Uncertainty analysis: performed using RiskSpectrum and the Error Factor associated to each parameter;
- Sensitivity analysis: the performance depends on the result obtained. These analyses are performed in order to evaluate the impact on the CDF of:
- The modification of some assumptions;
- The introduction of some design improvements.

The table hereunder presents the PSA results for the models which modelled the situation of each unit at the 1st January 2010. The update of the PSA results related to the situation of the units at the beginning of 2015 is ongoing (and therefore not presented in the tables hereunder).

Unit	Contribution of power states to CDF	Contribution of shutdown states to CDF
Doel 1-2	86.4%	13.6%
Tihange 1	80.4%	19.6%
Doel 3	81.7%	18.3%
Doel 4	61.7%	38.3%
Tihange 2	82.8%	17.2%
Tihange 3	54.7%	45.3%

Unit	For power states (% of to the total CDF)	For shutdown states (% of to the total CDF)
Doel 1-2	SLOCA: 40% Loss of CCWS/ESWS: 14 %	Loss of RHRS: 4%
Tihange 1	SLOCA: 20% LOOP: 17%	Loss of CCWS/ESWS: 7% Reduction of level in the primary circuit at mid-loop operation: 5% Loss of RHRS: 2%
Doel 3	SLOCA: 22% Loss of CCWS/ESWS: 13% LOOP: 7%	LOOP: 6% Loss of CCWS/ESWS: 5%

Unit	For power states (% of to the total CDF)	For shutdown states (% of to the total CDF)
Doel 4	SLOCA: 24%	LOOP: 11% Loss of CCWS/ESWS: 9% Reduction of level in the primary circuit at mid-loop operation:8%
Tihange 2	SLOCA: 26% Homogeneous dilution: 8%	Reduction of level in the primary circuit at mid-loop operation: 6% SLOCA: 2%
Tihange 3	SLOCA: 22% Loss of CCWS/ESWS: 6%	Loss of RHRS: 18% Loss of CCWS/ESWS: 10%

Level 2 PSA – internal events

For the L2 PSAs, the main results are given in the following table, regarding the containment failure (CF), the main containment failure modes, and the "Not Small" (i.e. releases more than 0.01% of the initial core inventory) Early and Late releases. It is recalled that the results correspond to the status of the units in 2010.

Unit	Proportion of CFF to CDF	Main CF modes	Proportion of Not Small Early releases frequency to CDF	Proportion of Not Small Late releases frequency to CDF
Doel 1/2	40%	Basemat melt-through Containment bypass Ex-vessel steam explosion	12%	63%
Doel 3	53%	Long-term pressurisation Basemat melt-through Ex-vessel steam explosion	5%	49%
Tihange 1	42%	Long-term pressurisation Basemat melt-through Isolation failure	5%	34%
Tihange 3	51%	Basemat melt-through Ex-vessel steam explosion Containment bypass	2%	4%[8]

Besides, sensitivity studies on phenomenology related basic events and on accident management related basic events have been performed.

[8] Tihange 3 "Not Small" Late releases: its proportion to the CDF is much lower than those of the other units because of 1) the Tihange 3 containment is more robust, thus less occurrence of containment failure due to long term pressurisation; 2) the occurrence of basemat melt-through as the only containment failure mode is higher in Tihange 3, but the fission product releases following basemat melt-through are not accounted for in atmospheric release categories.

Internal hazards (fire, flooding)

Finally, the obtained results of the internal flooding PSA Level 1 show that the risk induced by internal flooding events (e.g. due to the rupture of pipes) is smaller than the risk related to the above-mentioned initiating events (i.e. LOCA, loss of CCWS/ESWS).

The Fire PSA studies are still ongoing and final results are not yet available.

7. PSA APPLICATIONS AND DECISION MAKING

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. As a conclusion of each PSA update, some hardware modifications are proposed. As a result of the Level 2 PSA studies, the installation of a filtered containment venting system has been recommended.

The assessment of the adequacy of modifications in the plant design (proposed in another framework than PSA) by means of the PSA is also required in the Belgian legislation (as a result of the application of the 2008 WENRA Reference Levels). A significant increase in CDF or releases (frequency of magnitude) would not be permitted.

Accident management: Based on the results of the first PSA studies (L1 and L2) performed for the Doel 3 and Tihange 2 plants, the utility decided in the nineties to install catalytic hydrogen recombiners in the containment of each nuclear power plant. The Level 1 PSA studies have also been used to assess the adequacy of post-accidental procedures. The PSA studies have for example identified the importance of having a complete set of post-accidental procedures during shutdown states. The Level 2 PSA studies have led to recommendations for improvements of procedures regarding ventilation activation, steam generator isolation and containment spraying for certain units. They have also led to the improvement of the severe accident management strategy in Tihange where it has been recommended to ensure a dry reactor cavity before the occurrence of a potential vessel failure and study the feasibility of the implementation of an additional mean to inject water into the reactor cavity.

The assessment of the adequacy of modifications in the post-accidental procedures (decided in another framework than PSA) by the use of the PSA is also required in the Belgian legislation (as a result of the application of the 2008 WENRA Reference Levels). A significant increase in CDF or releases (frequency of magnitude) would not be permitted.

PSA-based event analysis: The assessment of the operational experience feedback by using PSA is endorsed by the utility (systematically) and by Bel V (for a selection of cases). The need of the analysis of operational events by using PSA has been integrated in the Belgian legislation (as a result of the application of the 2008 WENRA Reference Levels). The Conditional Core Damage Probability of 1.00E-06 is used by Level 1 PSA to determine if an event is a precursor or not. Then, insights are made and recommendations proposed.

Evaluation of Technical Specifications: The assessment of the adequacy of modifications of Technical Specifications with PSA is required in the Belgian legislation (as a result of the application of the 2008 WENRA Reference Levels). The goal of this

PSA application is to verify that any adaptation of Technical Specification (decided in another framework than PSA) doesn't lead to a significant increase in the CDF or in the expected releases (frequency or magnitude). So far, no requests for modifications to the Technical Specifications based on PSA insights have been discussed with the utility.

Use of PSA insights for training: In the framework of the Belgian action plan for WENRA 2008 Reference Levels, an action was defined concerning the use of PSA insights for training purposes. This action was defined to comply with WENRA Reference Level O3.5. Electrabel organised (with support of Tractebel Engineering) training sessions on L1 PSA for the Electrabel staff (in corporate divisions and on-site). Further Electrabel investigated how L1 PSA insights can be used to provide input for the training programmes of plant staff, including control room operators (for instance in simulator training sessions). Regarding L2 PSA, certain L2 PSA results related to the impact of human actions have been introduced into the training materials of severe accident management guidance.

Risk Monitoring: No surveillance of the risk by the use of PSA is performed on a daily basis. Nevertheless, the follow-up of the Risk Increase Factor (RIF) (taking into account the actual unavailabilities on plant) is performed a posteriori by the utility, which publishes monthly reports of the follow-up of the RIF indicator.

Management of the unavailabilities on site: The application Risk Matrix is used on the KCD site to reduce the risk induced by the unavailabilities of safety equipment. The combined unavailability of components necessary within the context of similar accidental sequences is avoided.

8. FUTURE DEVELOPMENTS AND RESEARCH

The future PSA developments will be made in the frame of the updated WENRA Reference Levels (which will be integrated in the Belgium legislation). One of these developments is the modelling of the spent fuel pool (at least for PSA Level 1).

9. INTERNATIONAL ACTIVITIES

Up to now, Belgium is involved in the Advanced Safety Assessment Methodologies PSA Extended (ASAMPSA_E) project (supported by the European Commission under the 7th Framework Programme for Research & Technological Development) for both Level 1 and Level 2 PSA projects. The aim of this project is to develop guidance related to the development of PSA in the frame of the external hazards. It allows each country involved in this project giving some guidance, insights from their own experiences.

Belgium also contributes to the OECD Fire ignition frequencies Database project.

CANADA

1. INTRODUCTION

Nothing to add

2. PSA FRAMEWORK AND ENVIRONMENT

Regulatory Document REGDOC-2.4.2 “Probabilistic Safety Assessment for Nuclear Power Plants” [1] was issued in April 2014 as an amendment of the previous CNSC standard S-294, in response to CNSC Fukushima Task Force recommendations [2]. REGDOC-2.4.2 sets high-level requirements for the development of Level 1 and Level 2 PSA with a formal quality assurance process, and requires the licensees to seek CNSC acceptance of the methodology and computer codes to be used for the PSA. The standard also requires the inclusion of both internal and external events, consideration of both at-power and shutdown operational states, as well as the inclusion of sensitivity analysis, uncertainty analysis, and importance measures.

The amendments included in REGDOC-2.4.2 include the addition of the following requirements:

Objectives of the PSA: This section was added to clarify the purpose for conducting a PSA. It enumerates eight objectives in accordance with IAEA SSG-3 [3].

Consideration of other radioactive sources

Multi-unit considerations

Inclusion of external events and their potential combinations

PSA update every five years. PSA models have to be updated sooner if the facility undergoes major changes.

Public disclosure: This requirement is newly added following the public request for an increased disclosure of the PSA results and in accordance with licensees’ public information programmes established under RD/GD-99.3, Public Information and Disclosure [4]. The amendment requires that a summary of the results and assumptions of PSA should be made available to interested stakeholders.

3. NUMERICAL SAFETY CRITERIA

Nothing to add

4. STATUS ON ONGOING PSA STUDIES

A request for the development of a Whole-site PSA for the Pickering Nuclear Generating Station was made by the Commission following the Pickering licence renewal hearing in 2013 [5]. An International workshop on Whole-site PSA was organised by Canadian industry in January 2014, and Ontario Power Generation (OPG) and CANDU Owners Group (COG) submitted in February 2014 a high-level concept methodology for whole-site PSA.

This was followed by an International Workshop on Multi-site PSA organised by the CNSC in November 2014.

5. PSA METHODOLOGY AND DATA

As part of their effort to comply with REGDOC 2.4.2, the Canadian licensees prepared and submitted for CNSC staff acceptance the following new PSA methodologies:

Whole-site PSA methodology

Identification and screening of other radioactive sources.

Identification and screening of other Plant Operating State

Crediting Emergency Mitigating Equipment (EME) (a new HRA methodology is developed for EME credits)

Crediting SAMGs in the PSA

6. NOTABLE RESULTS OF PSA

Nothing to add

7. PSA APPLICATIONS AND DECISION MAKING

Probabilistic safety assessment (PSA) assists CNSC staff to target resources where the largest benefit for plant safety can be obtained. The range of PSA applications covers: Licensing; Regulatory oversight; Risk-informed decision making; Operational event evaluation and abnormal plant configurations; Life extension projects; and Changes to the licensing basis.

References

[1] Canadian Nuclear Safety Commission (CNSC), *Probabilistic Safety Assessment (PSA) for Nuclear Power Plants,* regulatory document REGDOC-2.4.2, May 2014, www.nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-4-2/index.cfm.

[2] Canadian Nuclear Safety Commission (CNSC), “CNSC Fukushima Task Force Report”, CNSC INFO-0824, October 2011, www.nuclearsafety.gc.ca/pubs_catalogue/uploads/October-2011-CNSC-Fukushima-Task-Force-Report_e.pdf.

[3] International Atomic Energy Agency, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants”, IAEA Specific Safety Guide SSG-3, 2010.

[4] Canadian Nuclear Safety Commission (CNSC), “Public Information and Disclosure”, regulatory document RD/GD-99.3, March 2012, www.nuclearsafety.gc.ca/pubs_catalogue/uploads/RD_GD-99_3-eng.pdf.

[5] Canadian Nuclear Safety Commission (CNSC), “Ontario Power Generation Inc. – Application to Renew the Power Reactor Operating Licence for the Pickering Nuclear Generating Station”, Record of Proceedings, Including Reasons for Decision, Public Hearing Dates: 20 February and 29-31 May 2013.

CHINESE TAIPEI

1. INTRODUCTION

Nothing to add

2. PSA FRAMEWORK AND ENVIRONMENT

Taiwan Atomic Energy Council (TAEC), the nuclear regulatory agency in Chinese Taipei, was founded in 1955 at the ministerial level under the Executive Yuan. With Chinese Taipei's first reactor (a research reactor in National Tsing Hua University) reaching 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.

For three operating nuclear power plants, with two identical units for each plant, plant-specific PSA model was developed in 1980's under the co-operative research project initiated by TAEC, INER and utility (Taipower Company, TPC). Scope of the first Level-1 PSA includes internal events, internal fire, internal flood, typhoon and seismic for power operation. Shutdown PSA model was developed for internal events in 1990's. Only core damage frequency was considered as a risk index. After the release of USNRC RG 1.174, INER help TPC to develop PSA models for estimating risk index of large early release frequency. Since then, all PSA models were maintained by INER under series research projects sponsored by TPC. It was not until 2005, the implementation of maintenance rule, PSA became a requirement by TAEC. Utility is asked to update PSA model periodically and submit to TAEC for reference. Peer review following ASME standard was performed to show the technical adequacy of the plant-specific PSA model.

Risk-informed application is not encouraged by TAEC at all time. There is not much PSA-related regulatory activity before the Fukushima nuclear accident. In 2010, evidence of active near site faults was discovered. TPC was asked to re-evaluate the seismic risk and to provide justification of continuous operation of nuclear power plant. Methodology of seismic margin assessment (SMA) was selected with a plant-specific review level earthquake (RLE) that was approved by TAEC. Some structures and components were identified to have concern of low seismic capacity. Seismic reinforcement on those structures and components were completed in 2015.

After the Fukushima accident, additional PSA-related requirements from TAEC includes the stress test of severe accidents, systematic screening assessment of external events, seismic risk re-evaluation, tsunami risk assessment and volcano risk assessment. To response to the requirements, INER had completed the following PSA-related tasks through research project from TPC.

- Stress test for seismic and tsunami event
- Screening assessment of external events following the ASME PSA standard
- Revision of plant-specific seismic hazard analysis
- Seismic PSA update
- Risk evaluation of spent fuel pool

- Development of integrated methodology for tsunami PSA
- Estimation of tsunami CDF and LERF
- Development of aircraft impact PSA for Lungmen nuclear power plant which is under construction
- Development of plant-specific Level-2 PSA model including the risk from seismic and tsunami event

3. SAFETY CRITERIA

For the time being, the TAEC did not officially announce any quantitative or qualitative safety criteria. The utility adopt the USNRC safety criteria to manage the plant risk when the first plant-specific PSA was completed in 1980’s. Both CDF and LERF were applicable to single unit. After Fukushima nuclear accident, TAEC requested TPC to perform risk evaluation of spent fuel pool. Since no risk criteria were specified from TAEC, methodology of EPRI 1025287 was adopted to identify possible fast draining scenario for spent fuel pool.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

The PSA status of all nuclear power plants was shown in the table below. The PSA activities after Fukushima nuclear accident were mainly focused on the response to requests from TAEC. New PSA issues include complete external event analysis, seismic risk re-evaluation, tsunami risk and spent fuel pool risk. Fire PSA is now being updated following the methodology of NUREG/CR-6850. Periodic PSA update will include the collection of plant operating data, scheduled response to peer review comments, adoption of latest generic data and safety issues.

Summary of PSA Status in Chinese Taipei

Plant		Chinshan	Kuosheng	Maanshan	Lungmen
Reactor Type		GE BWR 4	GE BWR 6	3-Loop PWR	ABWR
Level-1 PSA	Full Power	Internal Events, Screening analysis of External Events, Seismic, High Wind, Internal Flood, Internal Fire, Tsunami, Aircraft Impact (Lungmen Only)			
	Low Power	N/A	N/A	N/A	Internal Events
	Shutdown	Internal Events			
LERF Index	Full Power	Internal Events, Seismic, High Wind, Internal Flood, Internal Fire, Tsunami, Aircraft Impact (Lungmen Only)			
Level-2 PSA	Full Power	Internal Events, Seismic, Tsunami			N/A
Level-3 PSA	Full Power	N/A	N/A	N/A	N/A
Spent Fuel Pool (for decommission programme)		Internal Events, Seismic, Internal Fire and Flood, High Wind, Aircraft Impact		N/A	N/A

To meet the TAEC requirement that the related calculations of emergency planning zone (EPZ) should be updated using latest data and technology every five years, INER developed a plant-specific Level-2 PSA for every operating nuclear power plant in 2015. Results of source term estimation were then sent to EZP calculation as an input of MACCS code.

Operation of two nuclear power plants in Chinese Taipei is now near the end of 40-year licence. The government announced to decommission the first plant (BWR 4) in 2018. INER is now preparing the decommission programme for the utility. A PSA for the risk of fuel uncovery in spent fuel pool was developed. The results showed that over 95% of risk was caused by the spent fuel pool structure failure during earthquake. Since the estimated HCLPF capacity of spent fuel pool structure is much higher than the plant SSE and the RLE defined in plant SMA, it is concluded that the proposed plant configuration during decommission had no significant risk concern on the spent fuel integrity.

5. PSA METHODOLOGY AND DATA

The first PSA was developed following the guidance of NUREG/CR-2300. In 2002, a peer review using NEI 00-02 was completed. Most F&Os of significance A and B were solved by the periodic PSA update. In 2011, additional peer review using ASME PSA Standard was conducted. Those PSAs developed after 2011 such as internal fire, external event screening analysis, high wind, tsunami and seismic will initiate separate peer review process following the latest version of ASME PRA standard.

Data used in PSA quantification process is the heart of PSA. Initiating event frequencies, component failure rates, common-cause failure parameters were obtained from latest technical reports which were summarised in the table below. Some plant-specific initiating event frequencies were obtained from the plant design, configuration or operation. Those data from nuclear industry was treated as the generic data. Collection of plant operating data will be conducted every three years. Those plant data will be used to update related PSA data using Baysian update process.

Source of Generic Data for PSA

Data Type		Data Source
Initiating Event Frequency	All Transients	NUREG/CR-5750
	LOOP	NUREG/CR-6890
	LOCA	NUREG-1829
	ISLOCA	NUREG/CR-5124 plus specific fault tree of plant configuration
	System Failure	specific initiating event fault tree of system operation
	Earthquake	convolution of site seismic hazard and SSC seismic fragilities
	High Wind	convolution of site wind hazard and SSC wind fragilities
	Fire	NUREG-2169
	Flood	EPRI 1013141
	Tsunami	site tsunami hazard and results of plant damage analysis
Component Failure Rate		NUREG/CR-6928
Common Cause Failure Parameter		NUREG/CR-6268 plus latest update on USNRC website
Probability of System Unavailable		plant operating data
Human Error Probability		EPRI TR-100259, NUS-4531, NUREG/CR-1278
Recovery Probabilities of Offsite Power and Diesel Generator		plant operating data

Tsunami risk is not a significant event for most of the nuclear power plant. Thus, there are not many researches on the quantification of tsunami risk. Per request of TAEC to clarify the tsunami risk after Fukushima nuclear accident, INER helped TPC to develop a practical methodology to quantify CDF and LERF of tsunami event. The methodology is focused on the plant damage analysis to define the relationship between tsunami event frequency and plant damage status. Guidance on tsunami plant walkdown as well as the qualitative screening criteria is well defined in the methodology. Plant damage status in terms of a corresponding tsunami intrusion height is then determined by the characteristic of tsunami and plant design.

6. NOTABLE RESULTS OF PSAs

Since TAEC does not announce a safety goal, the utility adopt the USNRC safety goal to manage the plant risk. Before Fukushima nuclear accident, all plant risk index meet the goal of CDF less than 1E-4 per year and LERF less than 1E-5. Also, there is a wide safety margin for all plants. After Fukushima nuclear accident, all plant seismic PSAs were updated using the latest plant seismic hazard that considering the discovery of active near site faults. A preliminary seismic PSA results suggested that some plant risk index will have a significant increase and there may be no reasonable safety margin exist. TPC initiated reinforcements on seismic capacity to significantly reduce the seismic risk. The list of SSCs and the target of reinforcement were based on the plant SMA results. The final seismic PSA suggested that all plant risk index meet the safety goal with reasonable safety margin.

Tsunami is always an important risk source while designing a nuclear power plant in Chinese Taipei. Important facilities will be designed to locate at an elevation significant higher than the possible tsunami intrusion height. After Fukushima nuclear accident, a new site tsunami hazard analysis suggested that there will be a frequency of exceedance higher than 1E-4 per year that a tsunami will flood into the main site. That will possibly cause a severe damage on safety systems since there may be no enough tsunami protection for SSCs located at main site. While developing tsunami PSA, TPC and INER conducted a comprehensive tsunami walkdown. Several vulnerable flood paths at main site were found. Those flood paths included significant opening on the structure and access door with no ability to against flood impact or hydrostatic pressure. Corrections on the tsunami walkdown findings have been made immediately. The final tsunami PSA showed that the tsunami risk still contributes around 7% of plant CDF. More than 60% of CDF is caused by tsunami flood height lower than the elevation of main site. Damage on service water system was expected. Almost 40% of CDF is caused by less than 55 cm height of tsunami intrusion at main site. Additional diesel driven auxiliary pump failure was expected.

7. PSA APPLICATIONS AND DECISION MAKING

In Chinese Taipei, PSA became a requirement after the implementation of maintenance rule. TAEC did not have the ability to develop, to maintain or to use PSA for regulatory activities. Per request of TAEC site inspectors, INER helped TEAC to develop a risk significant determination tool PRiSE (PRA Model Based Risk Significant Evaluation) for evaluation of inspection findings. PRiSE allows inspector to redefine plant configuration based on the inspection finding and output the increase on CDF and LERF. The results will be an important reference for on-site decision making. With the well-designed user friendly interface and super risk engine, the process can be done within a few minutes.

On the utility side, before Fukushima nuclear accident, PSA was used on risk related calculations for maintenance rule, applications of unexpected online maintenance, daily shutdown risk prediction and optimisation of outage schedule. A plant-specific risk monitor was developed to help the plant staff managing plant risk. After Fukushima nuclear accident, PSA for additional external events were requested by TAEC. The results of seismic PSA update showed a very significant increase on plant CDF and

LERF. Screening analysis of external event found that frequency of aircraft impact may be significant for the ABWR plant which had inherent lower plant risk. An aircraft impact PSA was developed for the ABWR plant and the results showed that the aircraft impact contributed 1% of plant CDF and 9% of plant LERF.

For the purpose of EPZ calculation update, a Level-2 PSA was developed for each operating plant. Tsunami risk and the updated seismic risk were included in the Level-2 PSA. Although there is a very significant increase on seismic risk, the updated EPZ still meet the design basis, i.e. 5 miles of radius around the site.

8. FUTURE DEVELOPMENTS AND RESEARCH

Most of the PSA research activities in response to TAEC requests after Fukushima nuclear accident have been completed. TAEC is now reviewing the results by inviting experts. There is no specific schedule for the review process. Regarding the significant increase on seismic risk, one suggestion from the review is to conduct a detail site seismic hazard analysis, especially on the geological survey and the modelling of the near site faults. Utility is now conducting a project for SSHAC level-3 review on site seismic hazard. Results of site seismic hazard curve, UHRS and floor response spectra will be available at 2020. Seismic PSA will then be updated by the new site hazard analysis.

Risk from volcano is another concern of TAEC after Fukushima nuclear accident. In the TAEC original request, quantification analysis was required to solve the issue. There still be discussions between TAEC and utility on what should be done.

9. INTERNATIONAL ACTIVITIES

There is no PSA-related international activity in Chinese Taipei. Invited participation to WGRisk is the only exception. INER is not the regulatory authority but helps both TAEC and utility on all PSA-related activities.

10. OVERALL INSIGHTS

Nothing to add

APPENDIX: Overview of PSA programmes in Chinese Taipei

Past	Level-1 PSA	First PSA on internal events, seismic, typhoon, internal fire and flood PSA update and transfer model from main frame to personal computer NEI 00-02 peer review and PSA update per review comments PSA model for LERF index following NUREG/CR-6595 Full-scope PSA for ABWR plant which is under construction Periodic operating data collection and PSA update ASME PRA standard peer review and PSA update per review comments Fire PSA update following NUREG/CR-6850 for BWR 4 and ABWR plants Screening analysis of all external events Development of tsunami PSA Seismic PSA update in response to seismic risk re-evaluation after Fukushima Spent fuel pool PSA for BWR 4 decommission programme
	Level-2 PSA	Level-2 PSA for EZP calculation
	PSA Application	Development of risk monitor for utility Development of fault tree engine INERFTE

		Development of risk significance determination tool for TAEC site inspector Risk evaluation for the implementation of maintenance rule Risk evaluation for unexpected online maintenance Relief request of ILRT interval Risk-Informed Inservice Inspection Program Optimisation of outage schedule Risk evaluation on design changes for the under construction nuclear unit Stress test in response to TAEC request after Fukushima
Ongoing	Level-1 PSA	Fire PSA update following NUREG/CR-6850 for BWR 6 and PWR plants Periodic operating data collection and PSA update Spent fuel pool PSA for BWR 6 decommission programme
	PSA Application	Update of risk significance determination tool for TAEC site inspector
Planning	Level-1 PSA	Seismic PSA update by site seismic hazard with SSHAC Level-3 review process Tsunami PSA update by latest geographic survey results Spent fuel pool PSA for PWR decommission programme Development of volcano PSA Peer review by latest version of ASME standard

CZECH REPUBLIC

1. INTRODUCTION

2. PSA FRAMEWORK AND ENVIRONMENT

In the Czech Republic there are two WWER sites (Dukovany /4 x WWER 440/213/ uprated to 500 MW, and Temelín /2x WWER 1000/320/ uprated to approximately 1100 MW). PSA studies were developed and have been continually maintained for both NPPs.

In past, there were no explicit legal requirements to perform PSA studies by licensee in the Czech Republic. In past, PSA activities were mainly initiated by utility based on concrete NPP needs, experience of other countries and consideration of regulatory recommendations. The PSA activities were conducted to enhance the safety level of the plant operation in the frame of existing safety culture environment. The long-term (10 years) operation license has included the requirements regarding Living PSA and risk monitoring to be performed.

In 2011, after the Fukushima accident, the Czech Prime Minister declared, that “nuclear safety is a priority for the government of the Czech Republic”. The Czech Republic followed relevant recommendations for reassessment/stress tests proposed by ENSREG. National report analysing safety issues connected with operation of Czech NPPs was developed in co-operation of utilities and Czech Regulatory Body. The stress tests performed in 2011 for NPP sites Dukovany and Temelín within the scope defined by ENSREG were followed in 2012 by creation and evaluation of strategies and adequate measures, both in the area of prevention of severe accidents and in the area of mitigation of their consequences.

In relation to the Fukushima accident, the revisions of PSA external hazard analyses continued for NPP Dukovany. For NPP Temelín, the external events risk analysis was decided to be a part of overall update of NPP Temelín PSA to be carried out next years. A special project for systematic evaluation and justification of proposed measures/improvements coming from stress tests by PSA has been opened for NPP Dukovany in 2012.

In 2013, the first post-Fukushima measures were adopted at NPP Dukovany and were addressed consequently in plant PSA model in 2014 in the Living PSA project. The continuing adoption of measures reacting to Fukushima events and stress tests was supposed to have a significant impact on PSA models of Czech NPPs. First, a long list of measures taken has to be addressed in PSA models and the impact of new measures regarding risk had to be evaluated. Secondly, the stress tests indicated need of deeper understanding of possible accident scenarios, resulting in a set of new supporting analyses, which also had to be reflected in PSA studies.

In 2014, adoption of measures responding to the information about Fukushima events and to the results of stress tests was proven as having significant impact on the results of quantification of PSA models of Czech NPPs, leading to significant decreasing of risk of plants operation, in particular in case of external events scenarios. **The revisions and updates of PSA external hazard analyses was planned to continue also in next years**

for NPP Dukovany. Although the external events risk has been assumed as being not dominating for NPP Temelín on the base of previous analyses, the revision of external events PSA was also initiated.

In 2015, extensive PSA activities were organised at both Czech NPPs – NPP Dukovany and NPP Temelín. In NPP Dukovany, the recommendations provided by the stress tests regarding modifications in the design and operation of Czech NPPs were in the final phase of realisation (some of them completely ready, some of them finished during the year), including all related aspects (procedural support, training of plant crew, etc.) Significant progress in addressing all safety important measures generated by the stress tests for NPP Dukovany in the PSA project was reached. All risk significant measures based on Post Fukushima Czech National Action Plan (NAcP) were addressed in the PSA model in the frame of Living PSA project. After considering and addressing the changes in Dukovany NPP design and operation in the PSA model, relevant changes were also transferred into the Dukovany risk monitoring model. In November 2015, the updated risk monitor was verified to be immediately used for evaluation of some real configurations of plant equipment corresponding to maintenance acts organised at Dukovany plant in December 2015.

The work on addressing the measures adopted for nuclear safety increase continued also at NPP Temelín, where the PSA is being under broad revision and extension. Complete NPP Temelín PSA team is involved in PSA update and, in addition, a specific contract was signed between CEZ, a. s., company and UJV Rez to address specific PSA areas in this update (human reliability, external and internal hazards, spent fuel pool risk, etc.) by expertise of UJV specialists.

A new State Law was under preparation in 2015, where development of Level-1 and Level-2 PSAs was decided to be required as mandatory for Czech NPPs, with the scope covering all operational states and all internal initiating events and hazards as well as external hazards, both natural and human induced. This Law was approved by Czech Government and Parliament in 2016 and will come into the force at 1 January 2017.

3. NUMERICAL SAFETY CRITERIA

During the time period 2011 -2015, the numerical safety criteria remain the same those used in previous time period. The safety goals adopted by the utilities were based upon the IAEA INSAG target value recommendations for CDF and LERF. No explicit regulatory probabilistic safety criteria were required to be met by the operator as there has been no explicit legal requirement to conduct PSA up to now. There was only regulatory body recommendation to comply with IAEA probabilistic safety criteria in INSAG-12.

The risk-informed applications were required to be supported with conservative criteria by regulatory body:

1) the licensee-initiated change was allowed provided that it was supported by the evidence that the risk increase is small, i.e.: ΔCDF or ΔFDF (when the change would have impact on spent fuel pool) < 5 x 10^{-6}/y **AND** ΔLERF < 1 x 10^{-6}/y

AND

2) the licensee-initiated change resulting in risk increase would not be allowed, as soon as the overall FDF (including risk from spent fuel pool) would exceed 10^{-4}/y **OR** the overall LERF would exceed 10^{-5}/y (to fulfil INSAG 12 objectives).

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

A regular update of PSA was performed each year for NPP Dukovany in frame of the Living PSA project during the time period 2011-2015. In 2014, for example, the update included incorporation of:

- design changes, for example:
  - measures to allow in-vessel retention,
  - seismic monitoring system,
  - reinforcement of cooling pump station for extreme natural hazards,
  - measures to facilitate bubble tower drainage,
- regular update of PSA input data including the update of:
  - component reliability data, IE frequencies, unavailabilities due to test/repair/maintenance, POS durations.

The impact of each design/procedure change regarding inputs, assumptions made and results of quantification of the PSA model was determined.

A comprehensive update of the Level 2 PSA for NPP Dukovany for full-power operation was performed in 2014. **The scope of the Level 2 PSA for Dukovany NPP covers internal events and hazards for all plant operating modes (including spent fuel pool). Beside the above-mentioned modifications, the impact of the new passive autocatalytic recombiners on Level 2 PSA results was assessed.**

In 2015, the regular update of PSA included, for example:

- incorporation of design safety measures from Post-Fukushima National Action Plan, for example:
  - installation of fan cooling towers (UHS) for essential service water system,
  - installation of the third EFW pump in each unit,
  - installation of hydrogen recombiners (PARs) in each unit,
  - reinforcement of turbine halls to withstand postulated seismic event and snow load,
  - installation of the additional stationary DG (SBO DG) for the twin-unit,
  - acquisition of the mobile DG for each unit to provide emergency power supply for I&C.
- update of Level 2 PSA and its extension to external hazards in all plant operating modes.

Beside the above-mentioned external events, some other changes were incorporated into Level 2 PSA for NPP Dukovany: 1) new definiton of LERF established (release of >1% Cs137 till 10 hours after core demage); 2) new SAMGs for low power and shutdown modes considered; 3) using of emergency measures of fire brigade for open reactor/SFP cooling considered; 4) new findigs of above-mentioned deterministic analyses considered.

At Temelín site, broad regular replacement of original PSA data by new plant-specific reliability data and first part of update of PSA models for internal initiating events were ongoing in 2014. In addition, the ongoing update included also the approved post-Fukushima measures, which were implemented in years 2014 to 2015 at Temelín.

The examples of the main measures adopted in NPP Temelín PSA with potential impact on NPP Temelín PSA results are:

- diverse system for secondary heat removal (additional feedwater system),
- diverse system for depressurised RCS heat removal (additional system for Containment Sump/RCS/Spent Fuel Pool makeup,
- alternate (flexible) system for Containment Sump/RCS/Spent Fuel Pool makeup,
- alternate (flexible) system for SG feedwater for secondary heat removal,
- additional SBO DG per unit,
- SBO power supply lines capable to supply any of 6kV buses at the plant using any of available DGs (safety grade/nonsafety grade/SBO DGs) at the plant,
- alternative mobile power supply means (mobile DGs and cabling) for supplying selected set of equipment,
- alternate power supply from external sources in case of SBO (power supply from Lipno dam, Orlik dam), etc.
- batteries alternative recharging using mobile DGs,
- alternative refuelling diesel using tank trucks for long-term operation of the DGs,
- reinforcement of passive autocatalytic hydrogen recombiners inside containment.

5. PSA METHODOLOGY AND DATA

In 2011, CEZ company became a member of EPRI project, which enables to use various advanced methodologies developed by EPRI and its partners for solution of specific methodological issues in Czech PSA studies. This was a real milestone in development of PSA studies for Czech NPPs. The initial areas, where EPRI methodological support was concretely applied, were seismic risk, loss of piping integrity frequencies and modelling of I&C systems.

The data sources providing inputs for quantification of component and human reliability parameters were continually updated within the time period 2011-2015. A new extensive simulator data collection project started in 2012 at NPP Dukovany full-scope simulator with one of the goals devoted to the support of human reliability analysis for the purpose of PSA. In December 2012, UJV Rez, a.s. became member of the NEA ICDE project with the aim to enhance quantification of common-cause failure parameters in PSA studies for Czech NPPs. The database of information about operational events - equipment failures, initiating events (precursors) and common-cause failures, which had been developed in 2007, was continually supported by new information in time period 2011-2013 to be ready for next regular update of NPP Dukovany PSA parameters in 2014.

The methodologies for selected important areas of PSA were analysed and improved, with strong impact of know-how transfer from EPRI sources, improving, for example, the methodology of seismic risk analysis, modelling of new digital I&C systems, fire risk analysis and screening approach for external hazards analysis.

The challenges connected with modelling and quantification of digital I&C failure potential were another specific subject of research activities. This effort employed the results of NEA DIGREL working group, UJV Rez, a.s. had been participating in, and also the inputs from co-operation with EPRI, where the project of know-how transfer from UJV to EPRI, oriented to the lessons learnt from the replacement of I&C at NPP Dukovany, was realised successfully.

The human factors related information continued being gathered by extensive NPP Dukovany simulator data collection in years 2012 and 2013 providing new inputs for control room crew human error probabilities estimation. On the base of data collection and analysis, a set of human factors oriented lectures was prepared and presented to all NPP Dukovany control room crews (approximately 80 control room operators participating).

In the important area of external events, there was intensive direct co-operation between UJV and NEA WGRISK. An international workshop was organised in Prague in June 2013, which was devoted to PSA for external events and followed the results of WGRISK survey on this topic. Almost 60 experts from OECD countries participated in this workshop. The main output of the workshop was a special report covering various aspects and current challenges in external event analysis and published all presentations made during the workshop.

In the NEA FIRE project, UJV specialists contributed to the final report of Phase 3 of the project (time period 2011-2013) and to the preparation of Phase 4 of the project (time period 2014-2015). UJV specialists took part in the process of update of fire database structure (removing of some uncertainties in understanding of meaning of the factors describing fire causes).

In the ICDE project, a systematic revision of database structure was carried out by UJV specialists with the aim to define component types, the operational history of Czech NPPs can contribute to the database. On the base of analysis of operational events occurred at Dukovany NPP, it was found that there is relevant information about CCF events for 7 out of 11 component types covered by the database. Examples of events were presented on IECD meeting and the information from NPP Dukovany was included into the database in April 2014. The information from ICDE database was used broadly in the project of update of data analysis for NPP Dukovany PSA, particularly CCF parameters, in 2014.

In addition to the know-how transfer from EPRI to UJV/CEZ, two contracts between UJV and EPRI were opened, where the PSA experts from UJV provided know-how transfer to EPRI in the following areas

- simulator data collection and analysis
- low power and shutdown PSA.

These two projects of co-operation with EPRI were finished successfully. The results of the project of simulator data collection and analysis were summarised in an internal EPRI report “Use of Simulator Data in Support of HRA – A Case Study from UJV Rez” released at the end of 2013.

The new research and development project started in 2014 in the Czech Republic, which was oriented to the topic of stability and reliability of electric grid and the mutual interactions of the grid and the events/failures happening there with the operation, trips and instabilities of big electrical sources, NPPs in particular. As a part of the scope, the impact of events caused by external natural hazards on the grid was analysed.

In the NEA ICDE project, the main contribution of UJV experts in 2014 was hosting the 39th technical meeting of the ICDE working group and the corresponding Steering committee meeting. The technical meeting was focused on the following areas and topics:

- enhancement and regular work of the database of common-cause failure events,
- general coding guidelines for ICDE events,
- impact of quality of operating procedures on the potential of common-cause failure to occur and to cause significant risk,
- review of the ICDE related activities in the individual countries participating in the project,
- specifics of common-cause failure events according to the component types,
- description of the ways, ICDE database is used in the individual member countries.

In 2015, another European project with UJV participation was FASTNET, which is focused on the analysis and improvement of NPP accident management. As a part and the first step of the project, the activities focused upon defining a representative set of risk important accident scenarios for various classes of NPPs were carried out, where the UJV experts covered the task of development a representative set of such scenarios for VVER reactors.

In the ICDE project, the UJV specialists initiated and took part in development of methodology of coding of common-cause failures for another type of NPP equipment – invertors. The motivation came from real practice, because invertor failures led to several acts of significant endangering of safe operation of NPPs in the past. The UJV specialists also took part in the update ICDE database containing CCF records from operational history of plant operated in OECD countries for 11 equipment types.

6. NOTABLE RESULTS OF PSA

The latest NPP Dukovany Level 1 PSA results (end of 2015) for internal events and internal hazards in all applicable plant operating modes were:

- an estimation of CDF ranges from 6.5 × 10-6/y to 7.2 × 10-6/y depending on the unit,
- an estimation of FDF (it covers risk from the reactor core and SFP) ranges from 1.05 × 10-5/y to 1.13 × 10-5/y depending on the unit.

The latest Level 1 PSA results (end of 2015) for external hazards in all applicable plant operating modes are:

- an estimation of CDF ranges from 3.26 × 10-5/y to 3.56 × 10-5/y depending on the unit,
- an estimation of FDF (it covers risk from the reactor core and SFP) ranges from 3.32 × 10-5/y to 3.63 × 10-5/y depending on the unit.

The latest Level 2 PSA results (end of 2015) for internal events and internal hazards in all applicable plant operating modes are:

- an estimation of LERF ranges from 1.17 × 10^{-6}/y to 1.21 × 10^{-6}/y depending on the unit.
- The latest Level 2 PSA results (end of 2015) for external hazards in all applicable plant operating modes are:
- an estimation of LERF ranges from 1.06 × 10^{--5}/y to 1.19 × 10^{-5}/y depending on the unit.
- Those results do not take into account procedures for diverse and mobile (DAM) equipment and Extensive Damage Mitigation Guidelines (EDMG) which are being incorporated into PSA model in 2016.

As an example of analysis results, the following table shows CDF and FDF values for the 1st unit of Dukovany NPP from internal groups of IEs for each POS. These values are related to the average length stay of unit in specific POS during a calendar year.

POS	**Brief Description**	**CDF [1/year]**	**% of total CDF**	**FDF [1/year]**	**% of total FDF**
BS	Empty reactor with all fuel removed to SFP	-	-	2.9E-07	2.6%
S1	Power operation	4.26E-06	59%	6.92E-06	61%
S2	Reactor shutdown or start-up	2.5E-07	3.5%	2.5E-07	2.2%
S3	Hot shutdown or heat-up	1.4E-07	1.9%	1.4E-07	1.2%
S4	Semi-hot shutdown with steam-water mode cooldown	4.4E-08	0.6%	4.4E-08	0.4%
S5	Semi-hot shutdown with water-water mode cooldown	3.2E-08	0.4%	3.2E-08	0.3%
S6	Cooldown with RCS pressure > 2 MPa	7.2E-08	1.0%	7.2E-08	0.6%
S7	Cooldown with RCS pressure < 2 MPa	4.0E-07	5.5%	4.0E-07	3.5%
S8	Open reactor before refuelling	4.3E-07	6.0%	9.6E-07	8.5%
S9	Refuelling with flooded refuelling pool	<1E-09	<0.1%	6.1E-08	0.5%
S10	Open reactor after refuelling	1.9E-07	2.6%	7.2E-07	6.4%
S11	Start-up after refuelling with RCS pressure < 2 MPa	<1E-09	<0.1%	<1E-09	<0.1%
S12	Heat-up after refuelling with RCS pressure > 2 MPa	3.8E-08	0.5%	3.8E-08	0.3%
S13	Heat-up after refuelling with RCS temperature > 90°C	1.27E-06	18%	1.27E-06	11%
S14	Unsealed primary circuit	9.8E-08	1.4%	9.8E-08	0.9%
Total		**7.22E-06**	**100%**	**1.13E-05**	**100%**

Another example of Level 1 PSA important quantitative output is the frequency of fuel damage for each of the internal IEs groups, presented in the following table.

IEs Group	Brief Description	CDF [1/year]	% of total CDF	FDF [1/year]	% of total FDF
C1	Cold RPV overpressurisation	8.1E-08	1.1%	8.1E-08	0.7%
FL1	CCW leakage in TG hall	2.5E-08	0.3%	2.5E-08	0.2%
FL2	Flooding of room A(B)242	-	-	2.1E-08	0.2%
HL	Heavy load drops into open reactor or SFP	1.4E-07	2.0%	4.19E-06	37%
L0	Very small LOCA (0-10 mm)	6.0E-08	0.8%	6.0E-08	0.5%
L1	Small LOCA (10-20 mm)	9.8E-07	14%	9.8E-07	8.7%
L2	Small LOCA (20-60 mm)	1.09E-06	15%	1.09E-06	9.7%
L3-4	Medium LOCA (60-200 mm)	1.30E-06	18%	1.30E-06	12%
L5-6	Large LOCA (200-500 mm)	1.9E-07	2.6%	1.9E-07	1.7%
LI-TF10	Interfacing LOCA into system TF10	1.7E-08	0.2%	1.7E-08	0.2%
LOSP	Loss of off-site power supply	1.2E-08	0.2%	1.3E-08	0.1%
LPOOL	LOCA into refuelling pool	6.7E-08	0.9%	6.7E-08	0.6%
MIL	Human-induced LOCA	9.3E-08	1.3%	9.3E-08	0.8%
MIS	Missiles in TG hall and auxiliary building	1.5E-07	2.1%	1.5E-07	1.3%
PL	Internal fires resulting in LOCA	3.3E-08	0.5%	3.3E-08	0.3%
PT	Internal fires resulting in transients	7.3E-07	10%	7.3E-07	6.5%
R1	Uncontrolled reactivity insertion	2.3E-07	3.2%	2.3E-07	2.0%
R3	Boron dilution in primary circuit	7.2E-08	1.0%	7.2E-08	0.6%
SGCR	Steam generator collector rupture	3.4E-07	4.7%	3.4E-07	3.0%
SGTR	Steam generator tube rupture	2.4E-07	3.3%	2.4E-07	2.1%
T1	MSC rupture	2.5E-07	3.5%	2.5E-07	2.2%
T2	FW or steam line rupture	1.5E-09	<0.1%	1.5E-09	<0.1%
T3	Loss of ESW train	1.6E-09	<0.1%	2.0E-09	<0.1%
T4	FW collector rupture	5.0E-09	0.1%	5.0E-09	<0.1%
T5	Loss of 400 kV or 110 kV power supply	1.9E-08	0.3%	1.9E-08	0.2%
T6	Loss of 6 kV busbar	7.6E-08	<0.1%	7.7E-08	<0.1%
T7	Unintended drainage of secondary circuit	5.2E-08	0.7%	5.2E-08	0.5%
T8	General transient following reactor trip	1.3E-08	0.2%	1.3E-08	0.1%
T9	Loss of CCW	9.0E-08	1.3%	9.0E-08	0.8%
T10	FW tank leakage	6.4E-09	0.1%	6.4E-09	0.1%
T11	Loss of FW pumps	1.5E-07	2.1%	1.5E-07	1.3%
T12	FW flow interruption	4.0E-08	0.6%	4.0E-08	0.4%
T13	Loss of natural circulation due to causes in RCS	6.2E-07	8.6%	6.2E-07	5.5%
T14	Loss of SFP cooling pumps	-	-	<10-9	<0.1%
Total		**7.22E-06**	**100%**	**1.13E-05**	**100%**

The PSA model for NPP Temelín was not significantly changed in time period 2011-2013 (some changes took place – for example modelling of I&C systems). In 2014, broad complete revision of NPP Temelín PSA started, which has been planned for several years. The presented results reflect the status of NPP Temelín PSA before the broad scope revision started.

The Level 1 - at power results for NPP Temelín are: the point estimate core damage frequency, for the updated PSA for internal initiating events is 1.39E-5/year. LOCAs contribute by 31% approximately to the CDF, primary to secondary leakage events by approximately 24% and transients by approximately 45%. The IEs related to internal fires contribute by the value of 7.42E-6/year to the total CDF, internal floods by 1.35E-6/year and seismic and other external events by the values below 1E-7/year.

Level 1 - low power and shutdown results for NPP Temelín are: the CDF for all 23 low power and shutdown plant operating states is, in total, 9.28E-6/yr. The dominant contributor is LOSP with 8.05E-6/yr. This initiator contributes around 87% to the total CDF value. No other initiating event contributes more than 5% to the CDF for shutdown PSA.

In Level 2 PSA, 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 the long term. A 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 the long term. The frequency of No Failure modes is 3.7E-06 (24.2 % of CDF). Late containment failure mode frequency is 6.8E-06 which is 45.4 % of CDF. Early Containment Failure mode 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 mode (LERF) was found to be 4,0E-6/year.

7. PSA APPLICATIONS AND DECISION MAKING

In time period 2011-2015, some PSA applications in Czech NPPs were continuing being oriented to the following traditional areas:

Evaluation of modifications: The systematic process of risk evaluation of most of proposed modifications of plants design and operation continued with specific topic of online maintenance at the beginning of year 2011. However, in response to Fukushima event, most of planned activities of that kind were postponed, because the core of engineering support of plant operation was oriented to detailed analysis of current status of plant safety issues necessary to be produced for European stress tests.

Event Analysis: New analysis of operational events using PSA for both plants was performed for Czech Regulatory Body each year during this time period. In 2011, for example, more than 1 600 events recorded during time period 2007-2010 in operation of both Czech NPPs were filtered to get the semi-final list of more than one hundred events, which were elaborated more in detail to get four events eventually for very detailed analysis. Basically, no one among these events was evaluated as a very significant risk contributor/precursor to core damage.

Operational Risk Monitoring: The risk models developed within the PSAs of Czech NPPs were transferred to a real-time risk calculation software (Safety Monitor), analysing both scheduled and real plant conditions for determining the impact of plant configurations on operational risk level. These regular analyses producing risk profiles of NPP operation continued each year for both Czech NPPs during the time period 2011-2015. The major purpose of using the Safety Monitor was the ability to provide an online risk measure based on the current plant configuration, online preventive/corrective maintenance or testing status, so enabling plant staff to plan and perform maintenance activities in such a way that safety is maximised, and at the same time unnecessary plant shutdown is avoided. In such manner, within 2011-2015, Dukovany NPP four unit outage schedules and Temelín NPP two-unit plant schedules were evaluated for their risk performance, including various risk-informed schedule modifications and also compared subsequently against real outage conditions and risk profiles. The most risk contributing configurations were then identified, analysed and recommendations were made for next outage risk reduction, in terms of fulfilling given internal risk criteria regarding both actual and cumulative outage risk. In addition, the risk was monitored in offline manner during outages by participating in outage scheduler meetings and recalculating potential schedule configuration changes, whenever required. Similar approach to planning and evaluation of outages continued being used also in the next years.

At both NPPs, PSA and Safety Monitor models were extensively used for various other applications in 2011, e.g.:

- JCOs (Justification for Continued Operation) to demonstrate very low risk (core damage) increase of continuing operation following some safety issues identification
- support for essential service water or diesel generators online maintenance (OLM), including comparison of various types of different system train unavailability combinations for different site units (using latest plant-specific reliability data available)
- development of Cost Benefit Analysis (CBA) Guideline to estimate cost benefits of selected risk-informed (delta CDF/delta LERF) design improvements and options
- evaluation of turbine(s) runback feature risk importance for LOSP/SBO issue.
- participation in SOER response and plants “Fukushima” stress tests reports – probabilistic part of the site reports.
- analysis of specific PSA reliability data as an input for SSCs related RCM activities
- risk indicators evaluation to indicate annual risk monitoring results and comparison among all plants and units.
- monthly, quarterly and annual risk profiles and reports with associated reporting of most risky configurations to the utility and regulatory body.

In 2012, a specific PSA application was pressurised thermal shock (PTS) analysis for NPP Dukovany. A systematic analysis of PTS potential for LOCA scenarios was performed by means of plant PSA model. This PTS study continued in 2013 by evaluation of other categories of initiating events. The output of the work was a basis for the consequent RPV integrity assessment for Dukovany NPP. Similar PTS analysis was performed for Temelín NPP in 2014 and 2015.

Another specific PSA application related to two DG OLM activities was performed at Dukovany plant in 2013 and, in addition, one ESW (Essential Service Water) OLM activity at Temelín NPP. Two OLM cases for different ESW train combinations at multi-unit sites were evaluated by means of PSA and documentation was prepared to help the proposed change (OLM) to be approved by the regulatory body for both NPPs in 2014.

In 2014-2015, the main PSA applications for both Czech NPPs were the evaluations of risk impact of a broad set of modifications carried out as a consequence of evaluation of Fukushima events. 24 plant measures were analysed for NPP Dukovany and their impact on the overall PSA results was determined. Recommendations to maximise the effects of the measures were specified. The analyses covered both the modifications in plant design including some very important design changes (new back-up cooling towers, new emergency dieselgenerators, mobile equipment determined for plant response to initiating events) and the modifications in procedures providing new back-up means of solution of specific accident scenarios.

The typical applications of both Dukovany and Temelín NPPs risk monitoring tools (using software Safety Monitor and plant/unit specific risk monitoring models) also continued during 2015. A specific attention was paid to evaluation of risk profiles for preventive maintenance of essential service water and DGs at-power operation in Dukovany plant. Moreover, before any outage of NPP Dukovany and NPP Temelín unit carried out in 2015, the outage schedule developed during planning was evaluated to identify all possible unacceptable risk peaks, including various risk-informed schedule variants/alternatives, and the schedules without risk peaks were suggested to be followed during the outage. This part of analysis has been repeated when all tag-out orders became available for detailed analysis. The final outage schedule, optimised from risk level point of view (both for actual and cumulative outage risks) was than tracked during the outage performance and if some deviations from originally scheduled activities appeared, the relevant parts of the outage schedule were recalculated. Later on, after finish of the outage, the real recorded outage configurations, usually somewhat differing from those initially scheduled, were also evaluated using Safety Monitor and risk monitoring models to confirm that the corresponding risk profiles were all right, without significant risk increase in some specific time points.

In addition, if some changes in plant equipment configuration were proposed based upon the outage in 2015, the risk impact of the changes was immediately recalculated by the PSA/risk monitor experts on a daily basis and the decision was made whether the given proposal of configuration change is acceptable from risk point of view or it should be modified. Last, but not the least, risk profiles (CDF/LERF) for all NPP units and each month of operation were provided to the plant/utility managers monthly and annually, as well as quarterly to the Czech regulatory body, to follow all CEZ units licence requirements.

8. FUTURE DEVELOPMENTS AND RESEARCH

In the research area, significant part of the activities will be again oriented to human reliability. The goal of the new project prepared to be started in 2017 is oriented to further development and testing of the nuclear power plant (NPP) control room (CR) simulator data collection methods and results. These data collection methods will be primarily oriented to the scenarios of abnormal and emergency NPP operation. The methods of data collection will be developed to cover the following topics of human factors treatment at the NPP: 1) improvement of control room operators training; 2) improvement of ergonomics of symptom based and other procedures used by CR crew;

3) searching of priorities in human factors treatment for CR crew, including support of plant risk model (PSA).

Another planned project regarding human reliability is being prepared for the EUROATOM Horizon 2020 call in October 2016. UJV Rez was, together with Swedish company AF Consult, main initiator of the project, which is going to be organised by Consortium of 9 partners, including VTT (Finland), PSI (Switzerland), IRSN (France). The goal of the project is provide guidance in problem areas of HRA methodology, data and risk oriented applications and to make steps to harmonisation of HRA methodology and good practice over Europe. The examples of topics solved: human reliability under the conditions of new (digital) MMI, treatment of organisational factors in HRA, long time scenarios and extreme (external events) conditions in HRA, simulator data collection, integration of several sources (of different quality) in development of HRA data, errors of commission. The proposal of such project was, in co-operation with several other European partners, transferred into the format of NUGENIA Template 2 and provided to NUGENIA EXCOM for possible labelling. The project got NUGENIA label June 2016.

The UJV specialists plan to continue in participation of a number of activities belonging to NEA working groups and projects:

- ICDE project on collection of information about common-cause failure events,
- FIRE project on collection of information about fire events,
- OPDE project on collection of information about events with loss of piping integrity,
- WGHOF as working group on human and organisational factors,
- WGRISK including the effort oriented to HRA for external events).

As a part of WGRISK membership, UJV is preparing new proposal for CAPS devoted to the impact of Fukushima events on safety of NPPs in OECD countries and, in particular, the role of PSA in the response to Fukushima.

Although the main focus of PSA activities has been put on engineering support of NPPs operation in the Czech Republic, there are other potentially important areas for research and future development and applications of PSA methods. In the next future, the work will be oriented to using PSA methodology for evaluation of safety of Generation IV reactors. As a part of this goal, support will be provided for the ALLEGRO project of development of new demonstrator of Generation IV gas-cooled reactor.

PSA Level-3 is topic of future research and preparation for applications. In 2013, UJV specialists started with collecting and analysis of current PSA Level-3 methodologies, with the focus on the activities initiated by IAEA. Suitable available computer codes supporting PSA Level-3 were analysed and an agreement with US NRC was reached providing the code MACCS2 for testing and analyses.

Another important topic, where the research activities were initiated several years ago and will continue in specific projects, is using the methods of probabilistic safety assessment in the area of security and cyber security.

The very important area of external events persists as the field for research and development activities. Here, the research effort is still focused on the methods of estimation of frequencies of natural external events of very high intensity on the base of rare data (covering relatively very short time periods). The estimation of frequencies and modelling of plant response to the external hazards, which are combinations of several hazards usually treated individually, was considered as an interesting and important problem, as it may lead to identification of hazards combinations, where the individual hazards may be just of mild safety effect, but the combination of them may be much more safety significant. Another key topic for research and development related to external hazards is vulnerability and fragility analysis as a part of analysis of plant response to hazard occurrence (the supporting components and systems vulnerability and fragility characteristics may be not transferrable among the hazards, the components and systems under concern may face to.

The PSA models developed for Czech NPPs, NPP Dukovany in particular, represent large integrated multi-unit models analysing various sources of risk potential. One of the topics of possible methodology development regarding risk and safety management is aggregation and balancing of various risks for the purposes of risk-informed decision making. Another interesting subject can be the best way how to extend a PSA model developed for just one unit to cover all possible safety relevant interactions with other units located at the site, taking into consideration different operational states of various units at a given time point (all combinations of different operational states of all units influencing availability of shared systems used in response to initiating event impacting just one or even more units).

The challenges connected with modelling and quantification of digital I&C failure potential continued being another subject of development activities in 2015 and next time. This branch of research and development was motivated by the needs of sufficiently realistic I&C modelling and quantification for the purposes of licensing regarding the topic of common-cause failures and software reliability. Correct modelling of a digital I&C with the respect to its variability and different sources of common-cause failures, including those caused by software, represents a challenge both regarding modelling techniques and parameters estimation. The use of representative models of digital I&C in PSA provide valuable validation tools of I&C architecture and associated procedures.

A broad scope co-operation between ÚJV Rez and NPP Temelín is planned for the whole year 2016, as well as next years, with the aim to carry out a broad update of NPP Temelín PSA. The most important topics planned for 2016 for further development NPP Temelín PSA model are:

- to integrate updated models and failure probabilities of CR crew actions in response to initiating events into the PSA model,
- to incorporate updated models of current I&C systems into the plant PSA model,
- **to update new plant-specific data into the PSA models, initiating event frequencies both for full-power operation and for low power and shutdown, in particular,**
- to update the internal initiating events PSA models with the aim to address the most current plant design and procedures status,
- to continue in the update of the human reliability analysis, particularly in the area of control room crew activities connected with treatment of information provided by the I&C systems,
- to finish the update of the fire risk initiating events frequencies,

- to finish the update the of internal flood risk analysis,
- to update of the PSA models to reflect design changes induced by gradual implementation of the post-Fukushima measures, with main focus on:
  - additional back-up feedwater supply into SG from both fixed and external mobile equipment using external connecting interfaces,
  - additional back-up coolant supply into depressurised RCS, sprays and spent fuel pool with additional multiple large sources of coolant,
  - another fixed SBO diesel generator/unit (Temelín is two-unit plant) to enhance safety level in case of „station blackout“ scenario,
  - fixed SBO power supply lines allowing power supply cross-tie to any of the plant 6kV/0.4 kV switchgears/buses,
  - alternate measures for batteries recharging in case of SBO conditions and provisions to extend batteries discharge time,
  - alternate means of power supply from external sources in case of SBO (dam turbines – three additional external power supply sources)
  - **reinforcement of passive autocatalytic hydrogen recombiners inside containment.**
  - **improvements against external events and threads (extreme weather)**
  - **to include modified procedures (EOPs, SAMGs, EDMGs, etc.) reflecting use of newly introduced modifications into the plat design**

In case of NPP Dukovany, the co-operation on further development and update of PSA model and applications of PSA will be driven by the conclusions of IAEA TSR PSA (IPSART) mission, which was organised in June 2016 on request of NPP Dukovany and Czech regulatory body. Eight experts on various areas of PSA from IAEA spent two weeks on revision of complete scope of NPP Dukovany multi-unit PSA covering all plant operational modes, all sources of possible radioactivity releases, including spent fuel pool, Level-1 and Level-2 PSA, five important internal hazards (fires, floods, missiles, heavy load drops and explosions) and a broad set of external hazards, both natural as well as man-made.

It is supposed that the next phase of co-operation on further development of NPP Dukovany PSA will follow the recommendations of the mission and the general conclusion of it, which was that the processes of addressing of all changes in NPP Dukovany design and operation work perfectly, but it is necessary to support them by further development and know-how transfer of the most up-to-date methodology reflecting current known specific challenges in PSA development and applications.

In case of NPP Temelín, it is supposed that broad update of PSA for this plant will continue and will be finished in 2017 in co-operation of Temelín PSA team and UJV experts contracted for specific areas of PSA. IAEA TSR PSA mission is planned for NPP Temelín to be organised in 2018.

9. INTERNATIONAL ACTIVITIES

Within the time period 2011-2015, UJV PSA specialists took part in broad range of international activities. Some of these activities were listed and commented in previous parts of this document, in particular in Section 5, if they were connected with specific methodological development. Some additional activities are presented below.

The UJV specialists have been actively acting in the European 7th Framework project ASAMPSA-E.

Identification, screening and analysis of external hazards for the purposes of risk analysis were the matter of continuing consultations of UJV experts with the experts from EPRI. In January 2014, UJV and CEZ company experts on external hazards were awarded by EPRI for innovative elaboration and using of methodology of identification and screening of external hazards.

The UJV specialists took part in the activities of newly established NEA ad hoc expert group on the impact of climate changes on safety and economics of NPP operation (NUCA). In the work of NUCA, UJV specialists share the knowledge related to the methods of safety analysis (particularly PSA) of NPP operation and discus the potential challenges, climate changes can generated for external events risk analysis.

A broad area of research and development topics has been discussed and planned in connection with NUGENIA platform. The possible activities in the risk and safety management area were currently oriented in the area of human reliability and human factors analysis. The most promising topic for broad international co-operation is simulator data collection and analysis, which was transferred in the project proposal HRA RDM for the Horizon 2020 call.

Several other bilateral projects were under way in 2015, where the UJV experts provided transfer of know-how to the international partners. The most important in 2015 were the following two projects:

- an EuropeAid project CH3.01/10
- the project of co-operation with TAEK.

The EuropeAid project is a broad project oriented to know-how transfer from EU to China covering various safety relevant aspects of NPP operation. From the PSA area, Task 4.1 of the project has been focused on methodological development of fire risk analysis methods. In addition, the subject of co-operation within Task 3.1 was safety analysis of the decommissioning, where the UJV experts were developing an integrated methodology combining and integrating deterministic and probabilistic approach, hazards analysis (including external hazards) and graded approach to safety.

The aim of the project of UJV co-operation with Turkish regulatory body (TAEK) was to develop a knowledge base and tools for licensing safety documentation of new NPP and to use the developed products in evaluation of safety documentation provided by NPP supplier. The area of PSA was completely covered in this project in 2015 by development of a set of more than 700 criteria based on IAEA, Russian and Turkish legislative, presentations of them to the project beneficiary and training the TAEK experts, how to use them.

Last but not the least, UJV experts made presentations on various subjects in top international conferences – PSAM and a number of other events. A list of examples of presentations from last three years is included below.

Husťák, S., Jaroš, M., and Kubíček, J. “Spent fuel pool risk analysis for the Dukovany NPP”, paper presented at EUROSAFE Forum 2013, www.eurosafe-forum.org/eurosafe-2013-seminar-1.

Holy J., Hustak S., Hladky M., Mlady O., Kolar L., Jaros M. “External events analysis in PSA studies for Czech NPPs”, paper presented at OECD International Workshop on PSA of Natural External Hazards including Earthquakes, 17-19 June 2013, Prague, Czech Republic.

Holy J., Hladky M., Mlady O., Kolar L., Jaros M. “Estimation of frequency of occurrence of extreme natural external events of very high intensity on the base of (non)available data”, paper presented at OECD International Workshop on PSA of Natural External Hazards including Earthquakes, 17-19 June 2013, Prague, Czech Republic.

Kolář L, Štván F., The Fire on Turbine Generator as Dominant Fire Risk at NPP Dukovany (VVER-440), OECD NEA Internal Workshop on Fire PRA, Garching, Germany, 28-30 April 2014

Husťák S., Jaroš M., Kubíček J., Spent Fuel Pool Risk Analysis for Dukovany NPP, International review journal, Progress in Nuclear Energy“, ISSN:0149-1970, Elsevier, 2014

Husťák S., Experience gained from the Living PSA project for NPP Dukovany, 22th Conference on Nuclear Engineering ICONE-22 (organised by ASME), 7-11 July 2014, Prague

Demjančuková K, Procházková, Probabilistic Safety Assessment in the Countries with Low Seismicity, 2014 ASME Pressure Vessels and Piping Conference, 19-25 July 2014, Los Angeles

Holý J., The Current PSA Approaches and Results of PSA in Czech Republic, Subtask 4.1 workshop of the EuropeAid project CH3.01/10 „Enhancing the Capabilities of National Nuclear Installations to Ensure Safe Nuclear Power Programmes, 27 October 2015, China Nuclear Power Engineering, Beeing, China

Husťák S., Kubíček J., Criteria and Guidelines for PSA Evaluation, presented for Turkish Regulatory Body (TAEK), 14 October 2015, Ankara

Husťák S., EUR rev.E, CH. 2.17 –PSA Methodology, EUR TCG#6 Meeting, 9-11 June 2015, Rez, Czech Republic

Holý J., Treatment of External Events in PSA Studies and Related Activities in UJV Rez, NUGENIA Forum 2015, Ljublana, 13-15 April, 2015

FINLAND

1. INTRODUCTION

Here, no contribution is expected from the participants.

2. PSA FRAMEWORK AND ENVIRONMENT

In Finland, PSA is a licensing document and the use of PSA is mandatory. The general requirement on the use of PSA is set forth in the Nuclear Energy Decree. It requires that the design phase PSA shall be submitted in connection with the construction licence application of a new nuclear facility and an updated PSA shall be submitted in connection with the operating licence application. PSA is used extensively by the licensees in risk-informed safety management of nuclear power plants and other major nuclear facilities and in risk-informed regulation by the Radiation and Nuclear Safety Authority – STUK.

The development of PSA was started in mid-1980s. From the first, the goal was set at Level 1 and Level 2 PSAs covering a wide range of internal and external initiating events for all operating states. PSA requirements have been gradually extended and implemented in legislation and in the regulatory YVL Guides issued by STUK. The main requirements on PSA and its applications are set forth in the Guide YVL A.7 Probabilistic risk assessment and risk management of a nuclear power plant [1]. The Guide YVL A.7 published in 2013 is an updated version of the previous Guide YVL 2.8 [2] which was first issued in 1987 and updated several times.

The consensus was that PSAs for the operating units should be conducted in-house by the licensees. The goal was also to improve personnel's understanding of the risks in the plants and to facilitate the use of PSA in safety-related decision making and to ensure continuous updating of the PSAs. External consultants were used only for special topics, such as seismic PRA.

For new NPP projects the PSA is typically developed by the vendor but the licensees are involved in the development starting from the early stages of the projects.

During the operating phase PSA shall be updated continuously to include plant modification and new reliability data. STUK reviews PSA updates continuously and a more detailed review is carried out in connection with licence renewals and other periodic safety reviews.

The licensees submit to STUK also the PSA computer model in addition to the documentation. STUK uses the model developed by the licensee in risk-informed regulation and the PSA model provides a common basis for discussions on safety issues. To compensate for the lack of independence, STUK carries out fairly detailed regulatory review of the model.

Analysis of external hazards is a well established part of the Finnish PSAs and there were no need to develop new PSA practices due to the Fukushima accident, changes were mainly in the deterministic requirements. However, decision making was expedited by the accident on some PSA-based plant modifications which were already under discussion before the accident.

3. SAFETY CRITERIA

Level 1 and 2 design phase PSA is required in connection with a Construction License application for a new NPP and the construction phase level 1 and 2 PSA is required in connection with an Operating License application (new unit or renewal of a fixed term licence). Regulatory Guide YVL A.7 Probabilistic risk assessment in safety management of nuclear power plants [1] specifies the following probabilistic design objectives:

- The design of a nuclear power plant unit shall be such that the mean value of the frequency of reactor core damage is less than 10–5/year.
- A nuclear power plant unit shall be designed in compliance with the principles set forth in Section 10 of STUK Regulation Y/1/2016 [3] in a way that

  a the mean value of the frequency of a release of radioactive substances from the plant during an accident involving a Cs-137 release into the atmosphere in excess of 100 TBq is less than $5{\cdot}10^{-7}$/year;
  b the accident sequences, in which the containment function fails or is lost in the early phase of a severe accident, have only a small contribution to the reactor core damage frequency.

Release assessments shall take into account all of the nuclear fuel located at the plant unit. A spent nuclear fuel storage external to the plant unit is considered a separate nuclear facility for whose analysis the aforementioned criteria apply.

The above requirements are applied as such to new NPP units. For the operating units the requirements are considered as target values and the principle of continuous improvement is applied. For major nuclear facilities other than NPPs, the requirements are applied where relevant.

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

4. STATUS AND SCOPE OF PSA PROGRAMMES

In 1984 STUK formally required the Finnish licensees to perform PSA studies and the first internal event PSAs were submitted to STUK in 1989. At present, 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 life.

PSA models have been developed by the licensees for the operating units at the Olkiluoto and Loviisa NPPs. The PSAs include Level 1 and Level 2 models. Level 1 studies cover internal events, internal hazards (fires, floods), and external hazards (harsh weather conditions, high seawater, impurities in seawater and seismic events) for power operation and shutdown states. The Level 2 studies include the same classes of initiating events.

Recent developments for the operating units include unit specific PSAs for Loviisa 1 and 2 as well as for Olkiluoto 1 and 2. Although the units at each site are almost identical, some differences exist especially in a few auxiliary systems. When plant modifications are scattered in time, temporary differences can exist between units. Another example of recent developments are outage specific shutdown PRAs which are nowadays conducted to facilitate work planning and risk minimisation during annual outages.

An updated PSA of Olkiluoto 3 was submitted to STUK in connection with the operating licence application in April 2016 and the review is ongoing.

Spent fuel pools at the plant units have been included in the PSAs. PSA has been carried out for the Olkiluoto interim storage for spent fuel, for the Loviisa interim storage a PSA will be conducted in the near future.

PSA has been carried also for the spent fuel encapsulation plant to be built in Olkiluoto by Posiva. The construction licence was granted in 2015. In this case, the study covered also moderate releases of radioactive substances due to mechanical damage of the fuel rod as the melting of the fuel is highly improbable after the long interim storage period.

The results of external events PRAs were used after the Fukushima accident in the national assessments and in the EU stress tests. The basic procedures or scope of PSAs have not been changed after the Fukushima accident, but some parts were updated, for example, an extensive the hazard studies for high sea water level was conducted for the Loviisa site.

5. PSA METHODOLOGY AND DATA

The requirements on the use of PSA for the risk-informed regulation derive from the Government Decree level,

STUK’s mandatory regulations and regulatory YVL Guides. According to the Nuclear Energy Decree the applicant for an operating licence has to submit a PSA to STUK. Detailed requirements on the use of PSA for risk-informed regulation and safety management have been set forth in the Regulatory Guide YVL A.7. In addition, requirements on the application of PSA in various fields are given in several other YVL Guides.

The Finnish requirements on PSA focus on what the licensees should do in each phase of the life cycle of a plant. The use of any specific standards, guides or methods is not required. The licensees can select the methods they use in their PSA projects. STUK reviews the methods in connection with the PSA review. In new NPP projects, methods descriptions are submitted to STUK at an early phase.

The Finnish licensees have developed their own PSA guidance independently from each other, based partially on international experience and PSA guidance since the late 1980s, and partially on their own research and on Finnish national research activities.

A requirement on peer review has been added in the new Guide YVL A.7, but so far only partial independent peer reviews have been carried out.

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 have been considered. 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 or calibration, 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 analysed, 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 and the newer FinPSA software automatically ensure 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. For example, 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 for taking dependencies into account in Loviisa PSA. In order to recognise 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 recognised as follows:

- Statistical dependency: In order to recognise 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),
- 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 modelled 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 recognised.

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 plant information system contains all failure history files since 1989 and provides all necessary raw data to the reliability data processing 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 (ageing, learning) is made for failure rates, the processing of data involves an automatic comparison between plant-specific and generic data. In a 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 releases. 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 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 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 modularisation procedures are slightly different. Finally, the user friendliness, the capabilities to solve large fault trees, and the computational speed are different for the various codes. However, the benchmarks results have shown that identical fault trees have resulted in sound results independent of the code used.

6. NOTABLE RESULTS OF PSAs

Loviisa 1 and 2 PSA

Loviisa 1 and 2 unit specific PSA results (end of 2015)

	Loviisa 1			**Loviisa 2**		
	Power operation	Shutdown	Total	Power operation	Shutdown	Total
Level 1 CDF [1/year]						
Internal	1.5E-6	6.2E-6	7.7E-6	2.9E-6	6.7E-6	9.6E-6
Fires	3.7E-6	2.3E-6	6.0E-6	4.1E-6	2.5E-6	6.6E-6
Int. flooding	6.5E-7	1.4E-7	7.8E-6	6.8E-7	1.6E-7	8.4E-7
Seismic	8.5E-8		8.5E-8	8.0E-8		8.0E-8
Other external hazards (weather etc)	1.9E-6	5.1E-7	2.4E-6	1.9E-6	9.6E-7	2.8E-6
Total	7.8E-6	9.2E-6	1.7E-5	9.7E-6	1.0E-5	2.0E-5
Level 2 LRF [1/year] Frequency of Cs 137 release exceeding 100 TBq						
All initiating events	2.4E-6	6.9E-6	9.3E-6	2.6E-6	7.7E-6	1.0E-5

Major risk-informed plant and procedural changes at the Loviisa plant

Internal Initiators

Several problem areas were identified in connection with the first PSAs conducted for the Loviisa plant. In some cases the risks were so obvious that actions for risk reduction were taken immediately although it was also understood that the analyses were quite conservative. The implemented measures are still good examples significant risk reduction with cost effective plant modifications.

The first results of the Loviisa level 1 PSA (internal initiators) submitted to STUK in 1989 resulted in immediate measures at the plant, since one initiating event caused 73 % of the total core melt frequency (1.7E-03 1/a).

In the first level 1PSA the dominating event was a loss of cooling of I&C room. The ventilation system of this room had only one train equipped with a cooling unit. The assumption that the control of whole plant is lost, if the temperature exceeds the design limit of I&C equipment 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 hot 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 feed water system could be manually operated even though the automatic control would be lost. hese corrections updated the core melt probability of the respective initiating event to 3.3E-04 1/a, and the total core melt probability to 9E-04 1/a.

Instead of further analysis, immediate actions were taken to redesign the air cooling system and to install an additional 100 % capacity diverse cooling unit. The modifications decreased the core damage frequency due to the loss of instrument room cooling to 1.2E-05 1/a and the total core damage estimate to 6.0E-04 1/a. Improvements have been made in several other systems causing high probability core damage frequencies such as primary circulation pump seal system service water system minimum circulation of ECC system. All the aforementioned systems suffered from design flaws which could be eliminated by cost effective modifications. The redesigned back-rotation prevention system and a new stop signal activated by low flow in seal cooling system for primary circulation pumps (PCP) and improved operator instructions for avoiding seal LOCA decreased the frequency of the respective accident sequence from 2E-04 1/a to about 1.0E-05 1/a.

The redundancy of the service water system was improved by changing base states of a few valves. This change eliminated the total loss of service water system in case of a pipe break and decreased the core damage frequency caused by the loss of service water from 1.3E-04 to 1.9E-05 1/a. An important design flaw was found in ECC system leading to high frequency accident sequence. If the closing valves in the minimum circulation lines failed to close on demand, the sump line valves and suction line valves could have shifted back and forth due to the suctions cycling between water tank and sump. The closing valves in the minimum circulation lines were replaced by more reliable type of valves in order to prevent the ECC water backflow to ECC tank. This change reduced the CDF from 5.4E-05/a to 1.4E-05/a in LOCA cases.

The 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 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 due to 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

Several fire safety improvements implemented during the 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 rotating band screen strainers due to high-pressure difference over the strainer screens and to prevent the consequent access of algae to the main circulating and service water system an automatic system for the reduction of water flow and reactor power has been installed in mid-1990s
- 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 intake 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.

Recent risk reducing plant modifications include:

- a radiator cooling system which can be used as an alternative final heat sink as backup for the service water system
- improved protection against extremely high seawater level
- modification of hoisting routes for heavy lifts in the reactor hall (reactor pressure lid, protective tube unit for control rods)

Olkiluoto 1 and 2 PSA

Olkiluoto 1 and 2 unit specific PSA results (end of 2015)

	Olkiluoto 1			**Olkiluoto 2**		
	Power operation	Shutdown	Total	Power operation	Shutdown	Total

Level 1 CDF [1/year]						
Internal	3.8E-6	1.4E-6	5.2E-6	5.3E-6	2.9E-6	8.2E-6
Fires	7.9E-7	1.1E-6	1.9E-6	2.1E-6	1.2E-6	3.3E-6
Int. flooding	1.8E-8		1.8E-8	1.1E-7		1.1E-7
Seismic	1.6E-7		1.6E-7	1.6E-7		1.6E-7
Other external hazards (weather etc)	7.5E-7	5.6E-8	8.1E-7	1.4E-6	6.2E-8	1.4E-6
Total	5.5E-6	2.5E-6	8.1E-6	9.1E-6	4.2E-6	1.3E-5
Level 2 LRF [1/year] Frequency of Cs 137 release exceeding 100 TBq						
All initiating events	1.3E-6	1.2E-6	2.5E-6			2.7E-6

Major risk-informed plant and procedure changes

The results of the first level 1 internal initiators PSA for the Olkiluoto 1 and 2 BWR units was submitted to STUK in mid-1990s. The results had an important role in initiating some plant changes:

- TVO has improved the reactor pressure vessel water level measurement system to prevent boiling of the water in the reference piping and to ease the surveillance test of the system. For example the function of auxiliary feed water system is controlled by water level in reactor vessel and the loss of the measurement would lead to core damage with high probability.
- Mussel capture strainers were installed into the sea water cooling systems in order to prevent blocking the intermediate cooling and diesel generator cooling heat exchangers by mussels growing in the auxiliary seawater channels. However, this modification was mainly based on operating experience rather than PSA results.
- A shutdown risk analysis was conducted in mid-1990s. The results showed that a large bottom leak STUK required that the lower air lock will be kept closed during the refuelling outages when the maintenance of the main coolant pumps is underway, because the maintenance work can results in large bottom LOCA in the reactor tank.
- the connections of the plant to the outside grid are upgraded by installing a new additional start-up transformer and improving the plant connections to nearby hydroelectric power plants.

New emergency operating procedures (EOPs) have been drawn up as follows:

- refilling of the EFW tank and condenser
- cross-connection of the diesel generators of neighbouring plant units
- manual depressurisation of the reactor tank from the relay room.

In 1995 TVO PSA was revised due to two weather related phenomena which took place at TVO plant. In February 1995 a snow storm blocked diesel generator combustion air filters in the air ducts and two diesels running in surveillance tests were stopped. To upgrade the reliability of DG system, dampers opening automatically on pressure difference were installed to enable alternative combustion air intake directly from DG rooms. In January 1995 frazil ice (rapid freezing of sub-cooled seawater) blocked coarse bar screen in the inlet channel and caused partial loss of service water system which is vital to emergency core cooling systems. To reduce the risk due to the frazil ice, a system circulating warm water to the intake of sea water channel has been installed. The system is to prevent fastening of frazil ice crystals on the coarse bar screen and its blocking. In addition, procedures for alternative seawater intake from the outlet side were developed.

Modelling of these two CCF type of phenomena contributed to TVO PSA core damage frequency an increment of 1.9E-5/year. The total core damage frequency including all identified initiating events and changes made due to the regulatory review was 3.34E-5/year. When the measures for managing the aforementioned type of external initiators were introduced the core damage frequency was reduced almost back to the preceding level.

The seismic risk analysis conducted in the late 1990s resulted in several plant modifications. 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 have been adequately anchored to solid structures.

Recent modifications

In connection with the EU Stress Tests following the Fukushima Daiichi accident it was pointed out that Olkiluoto 1 and 2 as well as some other BWRs are sensitive to the total loss of AC power and the loss of the ultimate heat sink (loss of the seawater cooling). These points could also be seen in the PSA results, but the total risk was relatively small and decisions on additional measures were taken only after the Fukushima accident.

In order to remove the sea water cooling dependence in the high-pressure emergency cooling system (also called auxiliary feed water system), the system arrangement was modified: Originally, when the emergency cooling water supply line to the reactor was closed, the flow was directed to a closed loop recirculation line instead of stopping the piston pumps. The recirculation line has a heat exchanger that cools the water to prevent the pump to heat up and fail. In the modified arrangement, the recirculation line injects the water back to the cooling water tank that has a high heat capacity. This way no sea water cooling is necessary for a long time in case the heat removal is lost. According to PSA-calculations, the modification reduced the core damage frequency by approximately 38 % (from 1.4E-5/year to 8.6E-6/year). However, abnormal vibration and pressure oscillations in the recirculation line have been observed during the testing of one subsystem and the reasons are under investigation. The modification will be implemented at Olkiluoto unit 2 when the issue has been resolved [24].

Olkiluoto 3

The design phase level 1 and 2 PSAs and the PSA applications required by the Guide YVL Guides (see Ch. 7) were submitted in connection with the construction licence application at the end of 2003. Some development areas were identified in STUK's review but in general the design phase PSA fulfilled the regulatory requirements. The updated PSA and the required applications were submitted in connection with the operating licence application in April 2016. STUK is expected to complete the review of the PSA during 2017.

7. SA APPLICATIONS

STUK has actively promoted the use of PSA in risk-informed safety management for more than 30 years. Several PSA applications have been required in Regulatory Guides as a condition for construction and operating licences. Based on development efforts and experience, more requirements have been set forth to extend the use of PSA to various risk-informed applications. Many of the these PSA applications have been examined through pilot studies initiated by STUK. Examples of new applications include a so-called "Security PSA"for vital area identifications, assessment of the coverage & balance of the commissioning tests, management of risks arising from the commissioning tests, and decommissioning risk assessment.

The use of PSA covers the whole life cycle of an NPP from the design phase to the decommissioning phase as long as there is spent fuel at the unit. The requirements have been focused on NPP units, but they are applied to other nuclear facilities when relevant. The use PSA in NPP safety management is summarised in the following table.

USE OF PSA IN FINLAND **NPP Safety Management**	
Design, Construction and Commissioning	**Plant operation, maintenance and decommissioning**
• Resolutions in Early Design Process • Compliance with Safety Objectives • D&EO Procedures • Programme for online PM • Programme for Systems Testing • Safety Classification and Graded QA of SSC • Review of Tech Specs • Assessment of the coverage and balance of the commissioning tests • Management of risks arising from the commissioning tests • Preliminary Decommissioning Risk Assessment • Strategic SAM Planning	LONG TERM • Main risk contributors • Plant Changes and Backfitting • In-Service Inspection (ISI) • In-Service Testing (IST) • Analysis of Tech Specs • Maintenance Planning • Personnel Training • D&EOP Improvements • Outage planning • Graded QA • "Security" PRA – vital area identification • PRA-based event analysis (incl. Risk. Follow-up) • Strategic SAM Planning • Decommissioning Risk Assessment SHORT TERM • Exemption from Tech Specs • Analysis of Safety Margins during Incidents (incl. emergency preparedness)

The licensees have well adopted the risk-informed safety management practices in accordance with regulatory YVL guides. In recent years STUK has also put more effort on developing risk-informed applications for regulatory use. In 2015, STUK initiated a process for implementing a framework for risk-informed decision making in the management system. The aim is to have a well documented formal approach, which enables grading of regulatory reviews and activities based on safety significance. The risk-informed graded approach is in pilot use and further development of guidance and risk metrics for various regulatory applications is ongoing.

Examples of Regulatory Use of PSA in Finland

- Targeting of regulatory inspections and reviews based on risk significance
    - Has been utilised in STUK on case by case basis
- Assessment of the Risk Impact of Plant Modifications
    - Identify need for potential modifications
    - STUK has requested licensees to perform assessments and to present action plans
- Assessment of the risk significance of operating events and incidents
    - To gain risk insights for decision making
    - Used also in INES classification
    - Risk insights may be used to assess the scope and content of licensee event reports
- Analysis of OLC (Tech Specs) Related Issues
    - Exemptions, Changes, AOTs, especially risk of continued operation vs. shutdown
- Annual evaluation of outage (shut down) risks (e.g. risk levels during the outage, outage arrangements, and scheduling of tasks)
- Sensitivity studies and Verification Calculations
    - Updated PSA models and documentation sent to STUK regularly
    - Emergency Preparedness planning at STUK
    - PSA has been used to develop a tool to easily assess possible accident progression and the magnitude path and content of a potential radioactive release
- PSA Info System (PSAIS)
    - Presents the PSA documentation and summary of main results and risk significance of SSCs in clear terms to be used by all experts
    - Needs more promoting and development for more effective use
- STUK has also developed a powerful and versatile PSA code (FinPSA) for model development, calculations and review purposes
    - Further development of FinPSA transferred to VTT

8. FUTURE DEVELOPMENTS AND RESEARCH

Research related to PSA is done mainly in the national nuclear safety research programmes (SAFIR). In the ongoing programme SAFIR2018 programme (2014 – 2018) the topics include

- HRA for advanced control rooms. From 2017 onward, focusing on hybrid control rooms with digital and analogue (as backup) technology
- HRA outside PSA

- Site-level PRA (former multi-unit PRA). Development of site-level PRA including several units and other possible radiation sources, like fuel pools, intermediate storages and repositories.
- FinPSA code development, especially related to dynamic IDPSA models
- Level 3 PSA
- Risk analysis of organisations and operations, including defence in depth in organisations
- Modelling of digital I&C in PRA
- In addition, SAFIR2018 includes topics relevant for both the deterministic and probabilistic approach, such as severe accident phenomena, behaviour of concrete under impact, modelling of fires, integrated safety assessment and justification of NPP automation, extreme weather phenomena, and extreme sea water level including the effects of climate change.

The previous programme period SAFIR 2014 (2010 – 2014) [26] included, for example, projects on

- human reliability analysis
- passive systems reliability
- dynamic Level 2 PSA
- Level 3 PSA
- imprecise probabilities in PSA
- risk communication
- development and use of fire-HRA method
- assessment of defence in depth in fire protection
- sea level scenarios for the Finnish coast
- further development of the FinPSA programme.

The revision of YVL Guides, especially Guide YVL B.1, has increased the weight of failure tolerance analyses, diversity and CCF analyses, and other failure analyses in safety demonstration for an NPP. Significant part of such analyses is naturally linked to review of PSA, in addition to traditional FMEA. These analyses offer significant support to review of PSA model, and PSA model can be used to review the analyses. Thus, the work of PSA teams at utilities and at STUK is including more and more other elements of defence-in-depth analysis. STUK is actively developing new methods to utilise PSA in the review of failure analyses and new methods to utilise failure analyses in the review of PSA.

9. INTERNATIONAL ACTIVITIES

Finland participates, for example, in the following international PSA-related activities:

IAEA Activities: Guide Development, Technical Committee Meetings, ISSC Extrabudgetary projects on seismic events, seismic hazard and other external hazards and related risk analysis

Western European Nuclear Regulators Association (WENRA): use of PSA in regulatory oversight

NEA Activities :WGRISK, other groups WGEV, WGIAGE (Seismic subgroup, CompPSHA), WGOE, WGHOF, MDEP (EPR PRA Technical Group); Projects FIRE, ICDE, Workshops

VVER Forum PSA Group (leader until 2013)

Risk Based Event Analysis meetings in Belgium

Nordic co-operation NKS Reactor Safety Projects, Nordic PSA Group (licensees, STUK is an associate member),

T-Book Nordic reliability data

EU Projects with PSA tasks, e.g, in Armenia, Ukraine, Byelorussia, Brazil

EU Research projects

The international PSAM11 conference was arranged in Helsinki, Finland in 2012 with STUK as the local organiser.

References

1. Current Regulatory YVL Guides are available at www.stuk.fi/web/en/regulations/stuk-s-regulatory-guides/regulatory-guides-on-nuclear-safety-yvl-

2. 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), Helsinki 2003.

3. Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2016). STUK Regulations are available at www.stuk.fi/web/en/regulations/stuk-regulations

4. 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, 29 September-3 October 1996.

5. 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, 28 November-1 December 2000, Osaka, Japan.

6. 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.

7. 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, 24-28 June 1996, Crete, Greece.

8. 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, 29 September-3 October 1996.

9. European Commission. "Report on Risk-Informed In-Service Inspection and In-Service Testing", NRWG, EUR 19153, June 1999.

10. NUREG-1602, “Use of PSA in Risk Informed Applications”. US NRC, 1998.

11. ASME Code Case N-560 "Alternative Examination Requirements for Class 1", 1996.

12. ASME Code Case N-577 "Risk-Informed Requirements for Class 1, 2 and 3 Piping , Method A, 1997.

13. ASME Code Case N-578, "Risk-Informed Requirements for Class 1, 2 and 3 Piping , Method B, 1997.

14. Mononen J, Julin A et al., "A Pilot Study on Risk Informed In-Service Inspection", PSA'99, August 1999.

15. Gosselin SR, "EPRI's new in-service inspection programme" Nuclear News, November 1997.

16. NRC Regulatory Guide 1.178 " An Approach For Plant-Specific Risk-informed Decisionmaking Inservice Inspection of Piping", July 1998.

17. Simola K, Pulkkinen U. "Expert Panel Approach to Support RI-ISI evaluation", December 1999.

18. Simola K, Pulkkinen U et al., "Expert Panel Approach for Supporting RI-ISI Evaluation", PSAM5, November 2000.

19. 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. 1 July 2007.

20. Bergroth N, Jänkälä KE & Ovcienko S. Oil spill risk assessment for Loviisa power plant. Proc. Probabilistic Safety Assessment and Management, PSAM 8, 15-19 May 2006, New Orleans, United States.

21. Marjamäki M, Lehto M, Sandberg J. Recent Experiences In Risk Informed Regulation In Finland. In the proceedings of 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13). Seoul, Korea. 2-7 October 2016.

22. Jänkälä K. Analysing And Decreasing External Event Risks Of Loviisa NPP. In the proceedings of 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13). Seoul, Korea. 2-7 October 2016.

23. Sandberg J, Laitonen J. The Role of PSA in the Fukushima Related Safety Assessments in Finland. In PSAM Topical Conference: In light of the Fukushima Dai-ichi Accident. Tokyo, Japan. 15-17 April 2013.

24. Finnish report on nuclear safety, Finnish 7th national report as referred to in Article 5 of the Convention on Nuclear Safety. Available at /www.julkari.fi/bitstream/handle/10024/130945/stuk-b205.pdf?sequence=1

25. Routamo T (ed.). European Stress Tests for Nuclear Power Plants, National Report - Finland. Available at www.ensreg.eu/sites/default/files/EU_Stress_Tests_-_National_Report_-_Finland.pdf

26. Hämäläinen J. and Suolanen V. (eds.) SAFIR2014 – The Finnish Research Programme on Nuclear Power Plant Safety 2011-2014, VTT Technical Research Centre of Finland, Espoo, Finland, 2015.

FRANCE

1. INTRODUCTION

* Note, the Executive Summary and Section 1 – Introduction will be written after the rest of the report has been compiled so that no contributions are expected from the member countries.

PSA FRAMEWORK AND ENVIRONMENT

The safety of French nuclear reactors is based essentially on a deterministic approach. The first PSAs have been performed out of the regulatory framework. PSAs were originally not required by the Safety Authority and were carried out as an aid for safety analysis.

Although it was not a regulatory requirement, partial probabilistic studies have been carried out since 1980 By EDF (Électricité de France – the French utility) and IPSN9 (Institute for Nuclear Protection and Safety - technical support of the Safety Authority), and two global PWR L1 PSAs were completed in 1990.

The first of these studies (PSA 900) concerned 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 1 300 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 reviews by EDF and IPSN were beneficial in assessing the exhaustiveness of the PSAs, as well as the validity of the assumptions made. Since PSAs were not a regulatory requirement, the relations between EDF and IPSN were more a co-operation and a technical dialogue than a classical safety analysis process.

The results of these studies have confirmed the importance of plant modifications designed to address Design Extension Conditions.

Presently French PSA activities are mainly carried out in 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 et aux Energies Renouvelables). These activities concern the development of PSA models and methods, as well as PSA applications for various safety analysis problems. Moreover, in the frame of new plants (e.g. EPR), a PSA is developed and utilised by the designers (AREVA and EDF) from the beginning of the design process.

PSAs have been recognised as useful tools for safety analyses in France and it became apparent the necessity for EDF and for the Safety Authority to define a more precise framework for PSA developments and applications. A Safety Rule dedicated to PSAs was issued in 2002.

[9] Now IRSN - Institut de Radioprotection et de Sûreté Nucléaire

Today, accordingly to the French order issued in 2012 (see articles 3.3 and 8.1.2 respectively), the regulatory safety demonstration shall include level 1 and level 2 PSAs for all relevant initiating events. In addition, internal events level 1 PSA is required to define the “Design Extension Conditions”.

2. NUMERICAL SAFETY CRITERIA

Generally speaking, the French Safety Authority (ASN) considers PSA as a useful 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, ASN is 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 approach is adopted in particular for the EPR project and in some particular cases during the Periodic Safety Review process, in accordance with the Numerical Safety Criteria defined by IAEA (INSAG 12).

3. STATUS AND SCOPE OF PSA PROGRAMMES

PSA developments in IRSN

Level 1 PSA for 900 MWe NPP

The level 1 PSA for 900 MWe plant series (CPY series) was updated in year 2010 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. The study will also be used to develop the fire, internal flooding, internal explosion and seismic PSAs.

Level 1 PSA for 1 300 MWe NPP

The level 1 PSA for the 1 300 MWe standardised PWRs is finished and a publication of the main reports (for P4 and P’4 1 300MWe plant type PSAs) has been updated in 2014. The study was 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.

Level 1 PSA for 1 450 MWe (N4) reactors

In the framework of the preparation of the 2nd Periodic Safety Review of the 1 450 MWe plant series (foreseen in 2016), the first version of the level 1 internal events PSA was updated in 2015.

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 (French Power Reactors Permanent Group meeting, early 2014). The study is now under updating to incorporate the latest design information, and will be used in the frame of the assessment of the commissioning application of the FA3 EPR reactor. The study is also used to develop the IRSN Level 2 PSA.

Level 1 PSA for EPR spent fuel pool

The draft version of the PSA study of the EPR spent fuel pool was finalised in 2011 and integrated to the EPR reactor PSA in 2014. The study will be mainly used to analyse the similar study which will be presented by EDF in the frame of the application for FA3 EPR reactor commissioning (French Power Reactors Permanent Group meeting beginning of 2016).

Fire PSA for 900 MWe NPP

A version of the fire PSA for 900 MWe was performed in 2007 taken into account the event oriented operating procedures.

The results obtained in the framework of the Fire PSA activities were used for the review of 900 MWe fire protection improvements. The study is now under updating.

Fire PSA for 1 300 MWe NPP

The first version of the study was finalised and was used for the third Periodic Safety Review of these plants. The summary reports (for P4 and P'4 trains) were issued in 2013. This first version has been updated in 2015.

Explosion PSA for 900 MWe NPP

The preliminary version of the internal explosion 1 PSA for 900 MWe reactors was finalised.

The study will be used for the fourth Periodic Safety Review of 900 plants (foreseen in 2017) to ensure that prevention and mitigation measures proposed by EDF are suitable and sufficient to ensure safety with regards to explosion risk.

Level 2 PSA for 900 MWe and 1 300 MWe NPP

Level 2 PSA for 900 MWe PWR series (internal events, power and shutdown reactor states): 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. A new update is now ongoing before the 4th PSR reviews activities which are planned in 2017. **Level 2 PSA for 1 300 MWe PWR series (internal events, power and shutdown reactor states)*:*** a first version of a level 2 PSA has been developed and used the conclusion during the preparation of the third Periodic Safety Review of these plants (2010-2013). This study is being updated.

Level 2 PSA for EPR Flamanville (internal events): a level 2 PSA has been initiated but stopped temporarily for other tasks

Extended L2 PSAs

Extension of L2 PSA to internal and external hazards is ongoing: simplified seismic probabilistic analysis of the containment function, a fire L2 PSA and site risk screening (for containment function).

PSA developments in EDF

900MWe NPP

The level 1 and 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) and plants modifications decided after the 3thd periodic safety review.

In the framework of the preparation of the 4th Periodic Safety Review, a new update of the 900MWe NPP level 1 and level 2 internal PSA has been issued in 2016.

Furthermore, the scope of PSAs is extended to:

- internal hazards : fire, flooding and explosion (analysis focused on the frequency of generating an explosive atmosphere).
- external hazards (site specific) : earthquake and flooding.

At last, EDF has developed and transmitted to the regulator in 2013 a screening methodology, which aims at identifying the relevant external hazards that should be subject to a probabilistic analysis. This methodology has been applied to each site ; as a result, simplified probabilistic analysis will be developed for other hazards than mentioned above.

1 300MWe NPP

The level 1 internal events PSA for 1 300 MWe NPP was updated in 2008. It takes into account the plant modifications decided during the 2nd periodic safety Review of the EDF 1 300 MWe plant series and the most recent experience feedback. This model was extended to Level 2 in 2008.

In the framework of the preparation of the 3thd Periodic Safety Review of the 1 300 MWe plant series, the level 1 and level 2 PSA were updated and extended (level 1 PSA only) to internal fire, internal flooding and earthquake (a feasibility exercise for Saint ALBAN power plant) in 2010.

Those PSA were discussed with the technical support organisation (IRSN) in the frame of this 3thd Periodic Safety Review of the 1 300 MWe plant series. Following the technical discussions, the internal event level 1 and level 2 PSA the internal fire and internal flooding level 1 PSA were updated and transmitted to the regulator in 2013. A last update of level 1 and level 2 PSA was achieved and transmitted to the regulator in 2014. This update takes into account the plant modifications decided during the 3thd periodic safety review of the EDF 1 300 MWe plant series.

1 450MWe NPP

Last update of Level 1 PSA for 1 450 MWe NPP was achieved in 2007. It takes into account the plant modifications decided during the 1st periodic safety Review of the EDF 1 450 MWe plant series and the most recent experience feedback.

In the framework of the preparation of the 2nd Periodic Safety Review of the 1 450 MWe plant series, the level 1 internal events PSA was updated and extended to level 2 in 2015.

Futhermore, the level 1 PSA will be extended to internal fire. Extension to internal flooding will be addressed as well by considering whether the existing 1 300 MWe internal flooding level PSA 1 can be usefully credited. Besides, the screening methodology produced for the 900 MWe plants will also be implemented for the 1 450 MWe sites.

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. The Level 1 PSA was used in particular to define the “Design Extension Conditions”.

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). Particular studies in order to respond to technical queries brought by IRSN or to assess the sensitivity to certain assumptions and input data were also performed.

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

On the other hand, specific studies related to the practically elimination of core melt sequences with containment bypass or induced by heterogeneous dilutions scenarios were performed.

Those PSA were transmitted to the regulator from 2009 to 2013 with updates of most recent design, including state of the installation, for the anticipated instruction. The internal fire and internal flooding level 1 PSA for the spent fuel pool were developed and transmitted to the regulator in 2013. Following regulator’s assessment, all those PSA studies were updated and transmitted to the regulator in 2014. A full update of all PSAs and particular studies is planned in the framework of the operational PSA development in consistency with the as-built plant state (to be accomplished in 2016).

4. PSA METHODOLOGY AND DATA

5. 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 studies were performed by two independent teams (IRSN and EDF), with a very detailed mutual review, contributing to an important improvement of PSA quality.

The current PSA Safety Rule issued in 2002 presents, in general terms, the acceptable methods for PSA developments and their applications, but it is limited to internal events and to level 1 PSAs.

For internal and external hazards PSAs as well as the extension to level 2 PSAs, EDF has developed its own methodologies, based on international available state of the art. IRSN uses mainly international available guidelines for level 1 PSA and has developed tools and methodologies for level 2 PSA.

For PSA applications, a detailed technical dialogue between EDF and IRSN is continuously carried out, including the discussion of methods in case of new developments. Periodic Safety reviews are a key part of this dialogue.

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 mainly to functional assumptions.

Level 2 PSA

In order to evaluate the risk of off-site releases, the EDF level 2 PSA covers the level 1 PSA accident sequences leading to core uncovering, both in reactor and in the spent fuel pool. This evaluation is divided in three main parts: an interface between level 1 and level 2 (definition of Plant Damage States), an accident progression analysis modelled by an event tree and a releases categorisation. 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.

In the IRSN L2 PSA, a particular effort has been done to obtain as far as possible “best estimates” results (with uncertainties assessment), avoiding conservative assumptions. This has led to the following features:

- A detailed level 1/level 2 interface: ~ 200 PDS.
- A specific software (KANT) for APET development and quantification and results presentation.
- A significant number of accident progression calculations with ASTEC (integral code) completed by MC3D (steam explosion), CAST3M (containment behaviour, mechanics),
- Detailed studies for each physical phenomena.
- Use of response surface method and grid method for physical modules of APET and uncertainties assessment.
- Automatic generation of Release Categories from the APET quantification with KANT (more than 1 000) associated to radioactive release calculations ; specific procedure for results presentation.
- A very fast-running code for consequences assessment (amplitude and kinetics of radioactive release, off-site radiological consequences).

Hazard PSAs

For both internal and external hazards, EDF has mainly adapted the existing EPRI/NRC or AMSE methodologies to the French context and specific needs. This is particularly the case for internal fire, internal flooding, earthquake and external hazards screening.

For internal explosion, EDF has developed its own approach. Besides, whatever the hazard to be assessed from a probabilistic perspective, EDF has developed approaches which are graduated and proportionate to safety issues. As a result, the depth of hazard PSA studies differs between hazards and between sites.

Common cause failures

The Multiple Greek Letter method and recently the alpha method for EDF are 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).

A common EDF/IRSN technical committee is in place in order to discuss methodological aspects related to CCF quantification and modelling.

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 based on Event-Oriented procedures.

Following the implementation of the State-Oriented procedures, the HRA models were updated, according to the new procedures logic and to simulator observations.

In the years 2000, in order to take into account the computerised emergency operating procedures of a new series of reactors, EDF developed a second generation HRA method (MERMOS), which is now the reference method for the internal events PSAs. The MERMOS method assumes that the emergency operation missions are assigned not to one operator, but an operating system that includes the control room team, the emergency operating procedures and the man-machine interface. The general approach of the MERMOS method consists in identifying all the scenarios for failure of the 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.

To model the actions of the SAMG for level 2 PSAs, both IRSN and EDF developed a dedicated HRA model: HORAAM for the IRSN and MEPEM for EDF.

- MEPEM is a second generation HRA model derived from MERMOS; a fourth failure mode concerning the prognostic of degradation has been added to the SAD model. MEPEM is made of three levels. More conservative results can be obtained (MEPEM 1 or MEPEM2) when there is a lack of information due to the grouping of level 1 sequences into PDS.
- HORAAM is a decision tree HRA model based on the observation of nuclear crisis exercises.

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.

Another point to be noted is the analysis as a specific study of long duration sequences (long-term loss of off-site power and of heat sink for EPR).

Section 6 – 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: CMF = 5. 10^{-5}/reactor x year

1300 MWe plant: CMF = 1. 10^{-5}/reactor x year

The most outstanding result was the high contribution of shutdown modes (32% for the 900 MWe plant and 56% for the 1 300 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 (see section 4). The updated studies take into account all the plant modifications in design and operation, as well as the evolution of knowledge and data (in particular success criteria were revised and new sequences were identified). For these reasons the results of the updated studies are not directly comparable to previous results.

For the recently updated EDF PSA (internal events, all plant operating modes), the order of magnitude for CMF is less than 10^{-5}/ry and for LERF is close to 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.

Section 7 – PSA Applications

Use of PSA during Periodic Safety Reassessments

The periodic safety reassessment, applicable to existing reactors, is a periodic process implemented for a given reactor type, which incorporates recent operating experience and updated knowledge.

Upstream of the safety reassessment, PSAs are updated in order to take into account the more recent operating experience and support studies (thermo-hydraulic, neutronic, aeraulic, hazard propagation …). They are used to identify and rank the main contributions to the core damage or abnormal releases frequencies. Thus, modifications of the design and the general operating rules can be proposed and studied in the frame of periodic safety review. Moreover, safety benefits of planned modifications are evaluated as well as their cost (direct and indirect costs related to operating). All modifications can be ranked accordingly to a dedicated approach developed by EDF.

Downstream of the safety reassessment, PSAs are updated in order to be consistent with all modifications decided during the periodic process and to evaluate their benefits with constant assumptions.

Design Extension Conditions

PSA results highlighted the need for additional dispositions in case of multiple failures situations ("Design Extension Conditions"). Internal events level 1 PSA is used to define the list of "Design Extension Conditions", and PSA insights are used in the demonstration of the acceptability of the additional dispositions and in the definition of requirements associated to these dispositions.

Operating Technical Specifications (OTS)

Typically, SSCs unavailabilities are classified into two groups in the OTS, depending on their importance in the Safety Demonstration. Nevertheless, for the SSCs dedicated to Design Extension Conditions, internal events PSAs can be used to optimise their classification in the OTS.

Furthermore, internal events PSAs can be used, as a complement of the safety analysis, to derogate to OTS, for exemple in the case of maintenance operations which duration could be longer than that initially expected in the OTS.

Probabilistic analysis of Operating Events

The probabilistic analysis of operating events occurring on the French fleet is performed by EDF for all events, and by IRSN for some representative examples. An operating event is considered as a "Precursor" when the conditional probability of core meltdown due to this event is higher than 10-6/event. Moreover, for the most important events (conditional probability of core meltdown higher than 10-4), the Safety Authority has required from EDF 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 programme since 1993. This analysis consists firstly in using a screening method to select events to be analysed. Secondly, the outstanding events are analysed using PSA models in order to imagine and assess degradation scenarios.

With this approach, the potential consequences of events are highlighted and corrective actions are adapted to their importance. The results of the event analysis programme are periodically presented to the French Safety Authority.

Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs)

PSA insights are used to optimise EOPs as well as SAMGs, in consistency with WENRA safety reference level O3.2 (PSA shall be used to identify the need for modifications to the plant and its procedures, including for severe accident management measures, in order to reduce the risk from the plant).

Training of operators

PSA insights are used in the frame of operators training, in consistency with WENRA safety reference level O3.5 (Insights from PSA shall be used as input to development and validation of the safety significant training programmes of the licensee, including simulator training of control room operators).

Risk-informed design for new reactors

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

- designing and optimising the facility during the design phase and life of the site,
- broaden the deterministic design scope of systems, with specific beyond-design analysis (multiple failures conditions),
- justify the maintenance planning,
- support the severe accident analysis,
- confirm the protections from external and internal hazards,

- assess the safety level increase compared to existing plants.

During commissioning of Flamanville 3, PSA is used essentially to demonstrate the compliance of the NPP with the assigned safety objectives and to support some PSA applications (like the contribution to the development of technical specifications).

Post-Fukushima Complementary Safety Assessments (CSA)

Until now Post-Fukushima Complementary Safety Assessments (CSA) were carried out mostly on a deterministic basis. PSA was not used explicitly, although knowledge of accident sequences was advantageous. The role of probabilistic insights will be further considered in the future (NPPs modifications will be included in the future PSAs). The development of the external events PSA will also contribute to the assessment of the effectiveness of the post-Fukushima plant modifications.

Section 8 – Future Developments and Research

PSA developments in EDF

In the future, EDF will continue to update and extend the scope of the PSAs accordingly to the French order issued in 2012 (see section 2).

In parallel, research and development works are in progress on subjects such as tools to optimise and facilitate PSAs developments and dynamic models coupled with codes calculations.

PSA development IRSN

Level 2 PSAs development and updating

L2 PSA for 900 MWe will be updated for the 4th generic PSR (2014-2016) and will take into account post-Fukushima action plans.

L2 PSA for 1 300 MWe will be updated after the 3rd generic PSR (2014-2015).

First version of L2 PSA for EPR will be available around 2016.

L2 PSA extension to hazards is seen as an important step for the future

Ageing PSA

Investigations are in progress in IRSN for introducing ageing effects in PSA models. A feasibility study and a pilot study were done. Based on the conclusions of these studies, a study limited to the incorporation of the maintenance data and the operating experience in the existing 900 MWe plants PSA model was performed.

Hazards PSA

For the internal flooding PSA, a feasibility study was done. The development of a first internal flooding PSA is ongoing.

For the seismic PSA a preliminary feasibility study was done. The development of a seismic PSA pilot study for 900 MWe plants is ongoing.

Regarding the external hazards PSA for external hazards, others than seismic, the following activities can be mentioned:

- ongoing development of screening method of external hazards,
- ongoing development of a “long-term” PSA (methodology and pilot study),
- recently started external flooding PSA (methods and pilot study).

PSA for new designs

In 2010, the CEA decided to perform PSA studies in collaboration with EDF and AREVA NP in support to the design of ASTRID (Advanced Sodium Technological Reactor for Industrial Demonstration), the French GEN IV Sodium Fast Reactor prototype.

At the end of 2013, a first PSA level 1, limited to the study of 8 initiating events occurring at nominal power, has been performed based on the static fault trees/event trees methodology on a period of time of 168 hours. The objective of this first model was to compare different designs of decay heat removal systems to orientate or to reinforce design decisions of these systems. This model was updated in 2015 in accordance with design progress.

Nevertheless, the conventional FT/ET approach initially developed for PWRs (Wash 1400), which is binary and static and does not permit the consider of the repair of failed components, appears to be unsuitable for SFRs PSA to assess the global risk over long periods of time, whereas several months are necessary for the thermal leakage to be equivalent to decay heat.

Therefore, dynamic PSA approaches have been investigated to extend the conventional PSA to longer periods of time by taking into account the specific characteristics of a sodium reactor such as its high thermal inertia – allowing operator intervention – and the fact that sodium circuits present risks of irreversible and temperature-sensitive failures.

Concurrently with reliable modelling by Petri nets and BDMP, an original combined methodology for probabilistic safety assessment is being developed by the CEA and its partners, AREVA NP and EDF at the conceptual design stage of ASTRID. This methodology, based on one hand on the results of the static level 1 PSA with the FT/ET approach and, on the other hand, on the dynamic analyses of long-term sequences with random failures and repairs of the DHR systems and support systems, allows quantitative evaluation of exceedance risk of safety criteria. Its goal is to demonstrate that the loss of DHR function can be practically eliminated in the long term. In the framework on this demonstration, influent parameters, as the study period of time, are to be justified and subjected to sensitivity analysis.

At this stage of the project, the modelling is based on numerous assumptions and doesn’t pretend to give results comparable directly with a probabilistic target: the main objective of PSA modelling is to give design orientations and move towards a trustworthy version in 2017.

PSA data

EDF has established a specific organisation on site and at corporate level in order to regularly update PSA data (reliability data, system unavailability, duration of standard plant states). The aim is to support not only living PSA programmes but also to support maintenance and safety management activities.

PSA Methodology

- In the last five years, methodologies have been developed by EDF on various subjects ; e.g. Fire PRA: EDF adapted the EPRI/NRC methodology to the French context and specific needs. It was applied for 1 300 MWe series Fire PSA. The feedback 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 1 300 MWe PSA.
- Modelling of I&C in PSA: in the frame of EPR PSA development, some new developments were carried out to improve the EDF reference approach; the so-called “compact model”. These developments include the modelling of initiating events induced by spurious actuation of I&C, of human-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 is to develop a method able to cover all possible situations including those when EDF Operational Experience show no evidence of common-cause events.
- HRA: advances in methodology have been developed in different areas such as Fire PRA, Level 2 PRA, pre-accidental HRA, enlarging the scope of the 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 by EDF with this new methodology show that the impact may be negligible in comparison to intra-system CCF. However the method is under discussion with IRSN.
- Some work is also being performed on the integration of all initiating events (including hazards) in the PSA model with a medium-term objective of enabling a modular PSA, facilitating further updates and collaborative work of different teams on the same model.

International activities

Most of the EDF methodological developments were presented to different PSA conferences (PSA 2008, PSAM 9, PSAM 10, PSA 2011 and PSAM 11).

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 harmonisation of practices. This includes participation to IAEA PSA safety guides, WGRISK activities (DICREL, ICDE, ...), EPRI scope and quality group. EDF was also one of the organisations 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 oversees the standard development for PSA in the United States. In 2011 a common team EDF/NNB was established for developing a PSA for supporting operation of the future Hinkley Point EPR.

IRSN develops mainly methodological aspects for the treatment of external hazards in the PSA, like the treatment of sequences with long study periods and site-wide sequences in case of total loss of electrical sources and/or of ultimate heat sink.

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

- CSNI/WGRISK workshops and task groups
- PSA 2008, 2011 and 2013 Meetings
- PSAM 9, PSAM 10, PSAM 11 and PSAM 12 meetings

IRSN has ensured the co-ordination of the ASAMPSA2 project of EC 7th FP, aiming at drafting the best-practice guidelines for development and applications of Level 2 PSAs. These guidelines, which are standardised for acceptance by a large number of organisations, have been available since 2013. A second European project, ASAMPSA_E, a collaboration of 30 organisations (extended PSA), now provides a framework to examine the methodologies available to extend the scope of PSAs as far as possible (internal and external hazards, L1 and L2 for all reactor states and SFP). Information on these projects is available on www.asampsa.eu.

IRSN is a member of ETSON PSA group and of MDEP/EPR/PSA group. In the frame of MDEP (Multinational Design Evaluation Programme) a working group is dedicated to EPR PSA (leaded by STUK). Presently a L1 EPR PSA comparison exercise was finalised between Finland, France, the United Kingdom and the United States.

Section 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 2010
- PSAM 11 – Helsinki (Finland) – 25-29 June 2012
- PSA 2013, Columbia, SC, United States, 22-26 September 2013

Appendix: Overview of the Status of EDF PSA Programmes

Figure 1

Plant Name	Plant type	Scope of the PSA carried out				PSA usage		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Standardized 900 MW plant	PWR	Level 1 Level 2	Internal events + Fire (only for IRSN Level 1) ongoing for EDF: internal fire, internal flooding, internal explosion, earthquake	All plant operating states	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	Yes - updated for 10 yearly PSR	Original: 1990 Last revision in 2010 New revision in2013 released in the framework of the fourth periodic safety review	No regulatory requirement Safety Assessment	Design review PSR PSA-based event analysis Review of Tech Specs
Standardized N4	PWR	Level 1	Internal events ongoing for EDF: internal fire	All plant operating states	Yes – updated for 10 yearly PSR	Original: 2001 Last revision in 2014	Carried out as part of the initial design and licensing	Design review PSR PSA-based event analysis Review of Tech Specs

EPR	PWR	Level 1+	Internal events	All plant operating states	Design PSA	Original: 2001 Revised: 2006	Carried out as part of the initial design and licensing	Design review AOT and IST
EPR Flamanville 3	PWR	Level 1 Level 2	Internal events, internal fire, internal flooding, internal explosion, simplified seismic PSA	All plant operating states	Construction PSA	Last update 2014 PSA updates taking into account design evolution and state of installation		

GERMANY

Use and Development of probabilistic safety assessment

An Overview of the situation at the end of 2015

1. INTRODUCTION

To be written later

2. PSA FRAMEWORK AND ENVIRONMENT

According to the Atomic Energy Act /ATG 16/, PSA is mandatory to be performed in the frame of the (Periodic) Safety Reviews (SR).

PSA is also addressed in the recent "Safety Requirements for Nuclear Power Plants" /BMU 15/ requiring ….

For enhancing the state of the art and considering insights from post-Fukushima investigations, a variety of R&D activities have been carried out. Details can be found in Chapter 5.

PSA is mainly developed by GRS as Federal German TSO (including nuclear research) and by the licensees together with their consultants in charge for carrying out PSA.

PSA users are the licensees, at least for PSA to be performed within the mandatory SR, and, to some extent, in the frame of regulatory findings or intended plant modifications. Other PSA users are TSOs and reviewers working on behalf of the regulatory authorities. The German regulators themselves use PSA only indirectly by contracting TSOs and other expert organisations for reviews or other analyses in the frame of regulatory decision making.

3. SAFETY CRITERIA

The Federal German regulatory body has recently promulgated a set of mandatory safety criteria, the so-called "Safety Requirements for Nuclear Power Plants" /BMU 15/ covering also requirements for PSA. These include only qualitative criteria, requiring PSA methods up to Level 2 PSA for full power (FP) as well as low power and shutdown states (LPSD) covering also PSA for internal and external hazards. The assessment shall also cover the spent fuel pool (SFP). Multi-unit aspects shall be taken into account; however, so far no detailed risk metrics are available.

Quantitative threshold values and criteria are not provided in Germany.

Detailed guidance is provided in the German PSA Guide /BMU 05/ and the supporting technical guidance documents /FAK 05/, /FAK 05a/, /FAK 16/.

In addition, as a minimum the requirements of WENRA, and IAEA, typically /IAE 10/, /IAE 10a/, /IAE 01/, /IAE 02/, /IAE 06/, are considered as well.

PSA for research reactors is up to now not mandatory in Germany. Probabilistic safety criteria as well as PSA methods and data need to be adapted to the specifics of research reactors.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

Progress has been made for the operating PWR as well as for BWR in the deterministic and probabilistic accident analyses for low power and shutdown states, and with respect to external hazards.

For accidents in a spent fuel pool a set of deterministic simulations has been performed, and a related set of source terms has been defined for different scenarios.

A comparative probabilistic study of two different types of emergency fuel element cooling has been performed for an older BWR in the post-commercial safe shutdown phase /TUE 15/. …

5. PSA METHODOLOGY AND DATA

For nuclear power plants in Germany, PSA is required by the mandatory “Safety Requirements for Nuclear Power Plants” /BMU 15/ and the German PSA Guide /BMU 05/.

The relevant German guidance documents on PSA Methods and Data /FAK 905/, /FAK 05a/ have been updated by provision of an additional technical guidance document /FAK 16/. PSA methods and data cover PSA up to Level 2 for FP as well as LPSD. Internal and external hazards are at least covered in Level 1 PSA.

CCF estimation methods have been improved to consistently include the different sources of estimation uncertainties applying Bayesian statistical methods /STI 14/, /STI 14a/, /STI 14b/. Applying these methods, generic CCF probabilities have been estimated based on recent operating experience of German NPP up to 2010, which has been analysed qualitatively and quantitatively in a common effort of GRS and the German utilities /STI 11/.

With regard to Level 2 PSA no significant changes occurred.

A modernised GRS source term prediction software with an underlying probabilistic approach to predict potential radioactive releases to the environment during a severe accident has been developed. By combining user answers concerning the status of the NPP and a basic Level 2 PSA by using a Bayesian Belief Network (BBN), the software predicts the most probable accident scenario and the corresponding release. The fast-running GRS source term prediction software has recently been improved to provide a user interface for input of observations and output of source term prognoses /HAG 16/. The final source terms can be provided as an already formatted report and as a code, which can be instantly read by decision-support programmes used by the corresponding authorities dealing with contamination in the environment and plant external measures. The prediction software is a tool to support the crisis team at the nuclear power plant during a severe accident. This enables the national authorities to be better prepared for decision making on external emergency procedures such as evacuations or the distribution of iodine to the public.

In order to enhance the completeness of PSA models and tools, an automated approach /BER 16/ has been developed to provide generic functionalities required to efficiently integrate the impact of internal and external hazards into PSA models. The approach enables PSA analysts to systematically model failure modes of nearly arbitrary complexity in a reasonable time frame while the thereby applied modifications remain traceable within the PSA data base. Moreover, the modelling of complex patterns and correlations between components, e.g. fire spreading between compartments, indicates limitations of commonly used software tools. In this way, the new tool pyRiskRobot may help to identify reasonable adaptations of established PSA tools in order to satisfy the increasing need to model hazard impacts as accurately as possible.

A methodological approach for systematic consideration of dependencies in case of internal and external hazards and their combinations in the probabilistic plant model for nuclear power plants was developed concerning site-specific Level 1 PSA taking into account the entire risks. In a first step, all the hazards which may occur at the site under investigation have to be identified. This requires a compilation of the potential hazards and their possible combinations. In a second step, the hazards to be considered for the specific site have to be classified with respect to the depth of the probabilistic analyses to be carried out. This classification covers three categories: hazards with a negligible contribution to the overall risk, hazards with such a low risk contribution that a rough quantitative assessment is sufficient, and hazards which need in-depth probabilistic analysis. Based on the available Level 1 PSA model for internal events, a systematic approach for in-depth probabilistic analyses of hazards and their combinations is proposed. In this context, lists of those systems structures, and components (SSC), which can be impaired in their required function resulting in a risk increase, are provided. One of these lists contains the equipment, the other one the dependencies to be considered for the corresponding hazard. In addition to the general approach for performing site-specific PSA, a procedure for modelling dependencies in the behaviour of structures, systems and components of a nuclear power plant according to failures caused by hazards has been developed. A generic dependency model has been built.

GRS is developing a tool called “Library HAZARDS” for comprehensively collecting internal and external hazards and combinations of events involving hazards in lists. In a first step, the entire hazards are included in this library. In a second step, information based on the internationally available operating experience with events from internal and external hazards is included. In a final step, the generic list is reduced in order to derive a site and plant-specific one. This list also covers event combinations involving internal and/or external hazards to be credited for the site under investigation.

Accident propagation after initiating events is a time-dependent process in which aleatory (stochastic) uncertainties affect the system and process behaviour in a way difficult to anticipate even for experts. For consideration of the manifold time dependencies and interactions between system and process behaviour, human actions and stochastic influences in an as far as practical realistic manner, advanced approaches for an improved probabilistic safety analysis have been recently developed /KLO 12/, /KLO 12a/, /KLO 12b/.

One of the advanced methods is MCDET (Monte Carlo Dynamic Event Tree) which is a combination of Monte Carlo simulation and the discrete Dynamic Event Tree approach. The aim of the MCDET approach is to integrate DSA and PSA to perform an Integrated Deterministic Probabilistic Safety Analysis (IDPSA) in order to derive more detailed and valid probabilistic results which can be used for risk-informed decision making. IDPSA with MCDET /KLO 12/, /KLO 14/, /KLO 14a/ allows modelling and analysing inherent interactions of complex systems in more detail while relevant aleatory as well as epistemic uncertainties can be taken into account much more comprehensively than in the classical PSA approach. MCDET was implemented as a tool which can operate in tandem with any deterministic dynamics code simulating the process and system dynamics.

An essential element of system safety is the reliable performance of human activities under a variety of different conditions. For modelling situations where plant personnel has to respond to process or system conditions an approach (Crew-Module) was developed which can be combined with MCDET /PES 12/. The Crew Module in combination with MCDET allows simulating human actions as a dynamic process depending on stochastic events and process states while interacting with the system and process dynamics in the course of time. MCDET in combination with the Crew Module was applied to perform an IDPSA for a fire scenario with fire fighting by plant personnel /PES 14/, /KLO 15/.

SUSA (Software for Uncertainty and Sensitivity Analyses) is a powerful software tool for uncertainty and sensitivity analyses and an important part of the GRS code system for nuclear reactor safety analyses /KLO 15a/, /KLO 16/. It provides support to quantify input uncertainties in terms of probability distributions, correlations and other appropriate dependence structures. For Monte Carlo simulation, the simple random and the Latin Hypercube sampling procedure are available. To prepare and launch computer code runs, a selection of code interfaces are implemented. Rather comfortable are the interfaces to selected codes in the field of nuclear reactor safety analyses. Many options exist for quantifying the uncertainty of a computational result. Options for performing a sensitivity analysis are implemented as well. SUSA combines well established methods from probability calculus and statistics with a comfortable graphical user interface (GUI). The GUI guides through the main analysis steps, requests input data where necessary, checks for input errors and performs all other actions up to the final representation of results. SUSA has been extended by new analysis options and updated according to the needs of an advanced IT environment in order to make it permanently usable for future uncertainty and sensitivity analyses.

6. NOTABLE RESULTS OF PSAs

The methods for implementation of Level 1 PSA are described in the German PSA Guide and the associated technical guidance documents. Despite the guidance specified therein for PSA implementation, the generic analysis of PSAs for the entire operating German nuclear power plant units, which had been carried in the frame of the mandatory (Periodic) Safety Reviews, has shown differences with regard to the methodology, the level of detail and the verification of the results.

The areas for enhancing probabilistic methodology identified are related to improving the completeness of PSA models, to insufficiencies in probabilistic assessment approaches, and to enhancements of assessment methods. Generic findings and review results for generic aspects found for Level 1 PSA mainly concern the safety assessment of the spent fuel pool (SFP), the consistent use of emergency measures, in particular for low power and shutdown (LPSD) operational states, the spectrum of initiating events for LPSD operational states as well as neglecting potential initiating events. With respect to hazards, the generic aspects mainly concern the necessity of enhancing PSA models for systematically assessing the risk resulting from internal and external hazards respectively including event combinations involving hazards.

Regarding the SFP safety assessment differences concern the spectrum of initiating events to be investigated in the course of plant nominal full-power (FP) operation and LPSD operation. Moreover, the failure of the SFP cooling has not been analysed in detail in all of the PSA analysed. Partly, the ultimate end-states for undesirable event sequences are defined differently. Differences between the individual PSAs also exist with regard to the systems under consideration for SFP cooling and the recovery of failed components to restore SFP cooling. Consequently, the results differ in the range of up to two orders of magnitude.

Inconsistencies exist in the consideration of emergency measures during the transition from hazard states to core damage states. The event-specific request of the available emergency response is not uniform in the PSAs for FP and LPSD operation states. Accordingly, a comparative analysis of CDF frequencies is more difficult since the extent to which emergency measures are taken into account in the PSAs strongly varies.

Event sequences due to mini leaks in the primary circuit are not considered in the PSAs. These event sequences differ significantly from the event sequences of larger leaks in the primary circuit. Also, initiating events with low occurrence frequencies are frequently examined qualitatively or within the frame of probabilistic assessments respectively, e.g. ATWS incidents. The explicit inclusion of these events in PSA would provide a methodological improvement.

The use of obsolete data for the occurrence frequencies of initiating events and for the reliability of system components and of human actions in the PSAs move the balance of PSA results, thus affect the assessment of the balance of the actual security concept of the system. In addition, minimum requirements to be applied for safety functions should be determined under realistic conditions and should match the specific conditions of FP and LPSD operation states.

A large number of events with cross-cutting impacts were not investigated or were assessed only qualitatively. With respect to cross-cutting impacts, the generic aspects mainly address the necessity of enhancing and completing PSA models for assessing the risk resulting from internal and external hazards and hazard combinations. The consideration of uncertainties by means of uncertainty analysis has so far not yet been performed consistently.

Level 2 PSA for German PWR consistently show that the containments provide a rather reliable barrier in case of core melt scenarios after they had been backfitted by means of filtered venting systems and with passive autocatalytic combiners. The most relevant negative aspects are related to missing discussions of combustion-caused damage to venting systems and failures of the venting filter, to realism versus conservatism of the analyses, and to considerations concerning a general metrics in order to better characterise Level 2 PSA results.

7. PSA APPLICATIONS AND DECISION MAKING

PSA in Germany is mainly used in the frame of the (Periodic) Safety Reviews (SR), which are obligatory to be performed every ten years for NPPs under commercial operation. During the reporting period of this report, no SR had to be carried out for the operating reactors units, however, updates of the existing PSAs for some of the reactor units considering post-Fukushima analytical results and actual improvements have been carried out. The activities for enhancing the regulatory framework in Germany can be found in /BER 13/.

Such analyses have been carried out for the following regulatory examples:

- Potential internal flooding due to a beak of a fire water pipeline (occasional assessment/review, followed by an intended plant modification):
  The fire water supply of an NPP electrical building was done by a fire water main from the building basement routed via the staircase to the different building levels supplying the different fire extinguishing systems. The fire water line was under permanent pressure, a valve for isolating the line was installed in the basement (in open position). In case of a leakage in the pipeline the valve had to be manually closed. Investigations in the frame of the SR indicated that it could not be excluded that a leakage would be recognised and located only when the basement was already flooded making the closing of the valve impossible. The licensee proposed a modification by replacing the manually operated open valve in the basement of the electrical building by a motor-operated closed one, which automatically opens in case of a fire in the electrical building for ensuring the fire water supply. For prevention of pressure surges (water hammer) in the fire water pipeline in case of opening the valve, which may endanger the integrity of the fire water pipeline the pipeline in front of the valve should be connected to the one behind valve by a bypass pipeline with small diameter and orifice to ensure that the pressure is maintained. The reassessment of the scenario with respect to the frequency of damage states taking into account the intended changes gave the result that the overall plant risk could be significantly reduced by the proposed plant modification. Therefore, the regulator decided that the proposed modification could be realised as intended.

8. FUTURE DEVELOPMENTS AND RESEARCH

Past and current research projects were and are devoted to CCF exceeding CCF groups presently modelled in PSA. An extensive analysis of German operating experience has demonstrated that such CCF occur quite frequently. For most component types modelled in PSA such CCF have been observed, even CCF affecting components of different types (e.g. due to common piece parts) /LEB 15/. New modelling and quantification approaches to include such CCF have been developed. A first exemplary application suggests that such CCF have a significant influence on quantitative PSA results/STI 15/, /STI 16/. Future research on this subject, which also is important to multi-unit PSA, is intended.

Further PSA research activities concern the extension, completion and improvement of PSA methods for the entire spectrum of internal and external hazards including event combinations with hazards in order to address these systematically in PSA – Level 1 and Level 2 – for all plant operational states (full power as well as low power and shutdown, including the longer term post-commercial safe shutdown phase).

Another important aspect of research is dynamic PSA including, as a result from investigations of the Fukushima Daiichi accident, the implementation of knowledge based human actions and consideration of stress affecting human action, particularly in hazard scenarios.

In addition, research and development activities on better addressing multi-unit issues in PSA have been started.

Moreover, GRS has started to develop and validate a graded PSA approach for research reactors.

9. INTERNATIONAL ACTIVITIES

Germany is actively participating in nearly all WGRISK tasks. Moreover, PSA-related work is also performed by GRS in the NEA Database projects, in particular ICDE and OECD FIRE. Results of the German participation in ICDE with respect to CCF can e.g. be found in /BRU 16/, on OECD FIRE e.g. in /NEA 16/, /BER 16a/, and /ROE 16/.

References

/BER 13/ Berg, H.-P., M. Röwekamp: Current Activities to Enhance PSA and Update the Corresponding Nuclear Regulatory Framework in Germany, Paper 227, in: Proceedings of ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis, Columbia, SC, 22-26 September 2013, on CD-ROM, American Nuclear Society, LaGrange Park, IL, United States, 2013, http://toc.proceedings.com/21106webtoc.pdf.

/BER 16/ Berner, N.:, 2016.

/BER 16a/ Berg, H. P., E. Armañanzas Albaizar, N. Fritze, M. Röwekamp: Consideration of Event Combinations of Fires and Other Events in Fire PRA – Insights from the OECD FIRE Database, Paper in: Proceedings of 13th International Probabilistic Safety Assessment and Management Conference (PSAM13), Seoul, Korea, Oktober 2016.

/ATG 16/ Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz - AtG) vom 15. Juli 1985 (BGBl. I S. 1565) zuletzt geändert durch Gesetz vom Art. 1 G v. 26.7.2016 I 1843, 2930, 2016; English version: Act on the Peaceful Utilisation of Atomic Energy and the Protection against its Hazards (Atomic Energy Act) Edition 12/16 (bilingual), 2016, www.bfs.de/SharedDocs/Downloads/BfS/EN/hns/a1-english/A1-12-16-AtG.pdf?__blob=publicationFile&v=11.

/BMU 05/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU): Sicherheitsüberprüfung für Kernkraftwerke gemäß §19a des Atomgesetzes - Leitfaden Probabilistische Sicherheitsanalyse, 31. January 2005, Bekanntmachung vom 30. August 2005, Bundesanzeiger, Jahrgang 57, Nummer 207a, ISSN 0720-6100, 3. November 2005; English translation Safety Review for Nuclear Power Plants pursuant to § 19a of the Atomic Energy Act - Guide Probabilistic Safety Analysis - of 30 August 2005, Edition 08/05, 2005, www.bfs.de/SharedDocs/Downloads/BfS/EN/hns/a1-english/A1-08-05.pdf?__blob=publicationFile&v=4.

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB): Sicherheitsanforderungen an Kernkraftwerke, Bekanntmachung vom 3. März 2015, BAnz AT 30.02.2015 B2, www.bfs.de/SharedDocs/Downloads/BfS/DE/rsh/3-bmub/3_0_1.pdf?__blob=publicationFile&v=6; English version: Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety, Safety Requirements for Nuclear Power Plants as amended and published on 22 November 2012 and revised version of March 3, 2015, www.bfs.de/SharedDocs/Downloads/BfS/EN/hns/a1-english/A1-03-15-SiAnf.html.

/BRU 16/ Brück, B., et al.: Expanding the Scope of ICDE: Systematic Collection of Operating Experience with Cross Component Group CCFs, in: Proceedings of the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM13), Seoul, Korea, October 2016.

/FAK 05/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, Oktober 2005, in German, http://doris.bfs.de/jspui/handle/urn:nbn:de:0221-201011243824.

/FAK 05a/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BfS-SCHR-38/05, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, Oktober 2005, in German, https://doris.bfs.de/jspui/handle/urn:nbn:de:0221-201011243838.

/FAK 16/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden und Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: Mai 2015, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany, BfS-SCHR-61/16, September 2016, in German, https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221.../3/BfS-SCHR-61-16.pdf.

/*HAG* 16/ Hage, M., et al.: A Probabilistic Approach for Source Term Prediction in Case of Severe Accidents, in: Proceedings of the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM13), Seoul, Korea, October 2016.

/IAE 01/ International Atomic Energy Agency (IAEA): Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2, IAEA-TECDOC-1229, Vienna, July 2001, www-pub.iaea.org/MTCD/publications/PDF/te_1229_prn.pdf.

/IAE 02/ International Atomic Energy Agency (IAEA): Review of Probabilistic Safety Assessments by Regulatory Bodies", Safety Reports Series No. 25, Vienna, November 2002, www-pub.iaea.org/MTCD/publications/PDF/Pub1139_scr.pdf.

/IAE 06/ International Atomic Energy Agency (IAEA): Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1511, Vienna, July 2006, www-pub.iaea.org/MTCD/publications/PDF/te_1511_web.pdf.

/IAE 10/ International Atomic Energy Agency (IAEA): Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-3, IAEA Safety Standards Series, STI/PUB/1430, ISBN 978-92-0-114509-3, Vienna, April 2010, www-pub.iaea.org/MTCD/publications/PDF/Pub1430_web.pdf.

/IAE 10a/ International Atomic Energy Agency (IAEA): Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide No. SSG-4, IAEA Safety Standards Serie, STI/PUB/1443, ISBN 978–92–0–102210–3, Vienna, May 2010,, www-pub.iaea.org/MTCD/publications/PDF/Pub1443_web.pdf.

/KLO 12/ Kloos M., J Peschke, W. Pointner: Advanced Method for Considering Epistemic and Aleatory Uncertainties in Integrated Deterministic Probabilistic Safety Analyses, Technical Meeting on Combining Insights from Deterministic and Probabilistic Safety Analyses, OECD Nuclear Energy Agency (NEA), Pisa, Italy, 11–15 June 2012.

/KLO 12a/ Kloos M.: Sensitivity analyses supplemented to epistemic uncertainty analyses for PSA results, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5**,** Curran Associates, Inc., Red Hook, NY, United States, 2012.

/KLO 12b/ Kloos M., J. Peschke: MCDET Approach for Considering Epistemic and Aleatory Uncertainties in Accident Simulations, NUTHOS-9 Conference, Kaohsiung, Chinese Taipei, September 2012

/KLO 14/ Kloos M., et al.: Insights from an Integrated Deterministic Probabilistic Safety Analysis (IDPSA) of a Fire Scenario, in: Proceedings of 12th International Probabilistic Safety Assessment and Management Conference (PSAM12), Honolulu, HI, United States, June 2014.

/KLO 14a/ Kloos, M., J. Peschke, J. Scheuer: Weiterentwicklung der MCDET-Methode und des zugehörigen Rechenwerkzeugs für probabilistische Dynamikanalysen, Technischer Fachbericht, GRS-330, ISBN 978-3- 944161-10-5, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Germany, June 2014 (in German), www.grs.de/publikation/grs-330.

/KLO 15/ Kloos M., J. Peschke: Improved Modelling and Assessment of the Performance of Fire Fighting Means in the Frame of a Fire PSA, Science and Technology of Nuclear Installations, Vol. 2015, Article ID 238723, 2015.

/KLO 15a/ Kloos M.: Main features of the tool SUSA 4.0 for uncertainty and sensitivity analyses, in: Proceedings of Annual European Safety and Reliability Conference 2015 (ESREL 2015), Zürich, Switzerland, 6-10 September 2015, CRC Press, 2015.

/KLO 16/ Kloos, M.: SUSA Version 4.0, Software for Uncertainty and Sensitivity Analyses, User's Guide and Tutorial, GRS-P-5, Rev. 2, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Garching, Germany, 2016.

/LEB 15/ Leberecht, M., et al.: Entwicklung fortschrittlicher Methoden zur Identifizierung von Gruppen von Komponenten mit GVA-Potenzial und zur Bewertung von teilweiser Diversität, Technischer Fachbericht, GRS-328, ISBN-978-3-944161-08, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH, Köln, Germany, Mai 2015 (in German), www.grs.de/publikation/grs-328.

/NEA 16/ Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA), Committee on the Safety of Nuclear Installations (CSNI):
Combinations of Fires and Other Events - The Fire Incidents Records Exchange Project Topical Report No. 3, NEA/CSNI/R(2016)7, Paris, France, (July 2016), www.oecd-nea.org/documents/2016/sin/csni-r2016-7.pdf.

/PES 12/ Peschke J., M. Kloos: Options to Consider Reliability Information in a Dynamic PSA with the MCDET Method, in: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012 (PSAM11 ESREL 2012), ISBN: 978-1-62276-436-5, Curran Associates, Inc., Red Hook, NY, United States, 2012.

/PES 14/ Peschke, J., et al.: Methodenentwicklung zur Analyse von Personalhandlungen im Rahmen probabilistischer Dynamikanalysen am Beispiel von Brandereignisabläufen mit Brandbekämpfung, Technischer Fachbericht, GRS-331, ISBN 978-3-944161-11-2, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Garching, Germany, June 2014 (in German), www.grs.de/publikation/grs-331.

/ROE 16/ Röwekamp, M., et al.: Experiences from the OECD FIRE Database and Intended Future Extensions, Paper in: Proceedings of 13th International Probabilistic Safety Assessment and Management Conference (PSAM13), Seoul, Korea, October 2016.

/STE 13/ Steinrötter, T.: Spent Fuel Pool Analyses for German NPPs using the MELCOR Code, OECD SFP Project Seminar 2013, Paris, France, 22-23 October 2013.

/STI 11/ Stiller, J. C., et al.: Development of an integrated program and database system for the estimation of CCF probabilities, 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, United States, 2011.

/STI 14/ Stiller, J., A. Kreuser, C. Verstegen: Further Development of the GRS Common Cause Failure Quantification Method, in: Proceedings of 12th International Probabilistic Safety Assessment and Management Conference (PSAM12), Honolulu, HI, United States, June 2014,

/STI 14a/ Stiller, J. C., et al.: Weiterentwicklung des Quantifizierungsverfahrens für GVA zur Vermeidung von Schätzfehlern aufgrund vereinfachender Modellannahmen, Technischer Fachbericht, GRS-322, ISBN 978-3- 944161-02-0, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Juni 2014 (in German), www.grs.de/publikation/grs-322.

/STI 14b/ Stiller, J. C., et al.: Methodenentwicklung zur konsistenten Berücksichtigung epistemischer Unsicherheiten probabilistischer Kenngrößen in PSA-Rechnungen, Technischer Fachbericht, GRS-327, ISBN 978-3-944161-07-5, Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Köln, Juni 2014 (in German), www.grs.de/publikation/grs-327.

/STI 15/ Stiller, J. C., et al.: Common Cause Failures Exceeding CCF Groups, in: Proceedings of the International Topical Meeting on Probabilistic Safety Assessment and Analysis, Sun Valley, Idaho, United States, April 2015.

/STI 16/ Stiller, J. C., et al.: Common Cause Failures Exceeding CCF Groups, in: Proceedings of the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 3), Seoul, Korea, October 2016.

/TUE 15/ Türschmann, M., M. Röwekamp, S. Babst: Concept for Comprehensive Hazards PSA and Fire PSA Application, Progress in Nuclear Energy, Volume 84, Special Issue: EUROSAFE 2013, S. 36-40, 2015, www.sciencedirect.com/science/journal/01491970/84.

/WEN xy/ Western European Nuclear Regulators' Association (WENRA), Reactor Harmonization Working Group (RHWG): WENRA Reactor Safety Reference Levels for Existing Reactors, Issue S: Protection against Internal Fires, September 2014, www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

HUNGARY

1. INTRODUCTION

2. PSA FRAMEWORK AND ENVIRONMENT

The Hungarian legislative framework of the peaceful application of nuclear energy is predominantly defined by the Act No. CXVI/1996 on Atomic Energy and the subsequent Governmental Decree No. 118/2011 (VII. 11.). None of these legal items contain explicit requirements on performing and/or application of probabilistic safety assessment for the safety evaluation of existing and new nuclear power plants in Hungary.

Ten volumes of Nuclear Safety Codes (NSC) were issued as appendices to the Governmental Decree No. 118/2011 (VII. 11.) on the Nuclear Safety Requirements of the nuclear installations and related regulatory activities. These volumes contain a very detailed set of technical requirements on nuclear safety. All requirements in the volumes of NSC are obligatory to meet byr 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, NEA, EUR[10], 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 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 apply other means to meet the nuclear safety requirements.

The nuclear safety requirements related to an existing or a new nuclear power plant are collected in the first four volumes of NSC. Volume 3 deals with the design requirements of an existing nuclear power plant, Volume 3a deals with the design requirements of a new nuclear power plant, and these contain several prescriptions in relation to PSA. Regarding the PSA, these volumes contain 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 and initiating events. It is stated that best-estimate approaches shall be followed in PSA, and where this requirement cannot be fulfilled, there reasonable assumptions shall be considered. General requirements are given related to data, modelling of human failure events and consideration of common-cause failures in PSA. According to the requirements, uncertainty and sensitivity analysis are mandatory. Other than that, there are no specific requirements on PSA quality.

As defined in the requirements of the NSC, use of PSA should be made or can be envisioned in the following areas:

- Support to safety management: the licensee is obliged to use probabilistic safety assessment and PSA information in support of safety management.

[10] European Utility Requirements

- Evaluation of plant safety: PSA has to be applied to evaluate and justify that the plant design is balanced, and the analysis results must be used to show that the defences against beyond-design-basis accidents are appropriate.
- Support to design: the requirements prescribe the use of PSA to justify the design and to review the design.
- Support to plant modifications: PSA should be applied to evaluate the necessity of plant modification and to identify modifications, if seen necessary from risk point of view.
- Safety classification of systems, structures and components: it is generally described that deterministic and probabilistic considerations should be used together, although detailed requirements on applying PSA are not specified.
- Support to maintenance: acceptance criteria for PSA must be met by modelling maintenance of plant systems and equipment "as planned" in a design stage PSA and "as practised" in a PSA valid during plant operation. The maintenance programme is supposed to be set up by seeking balance between improvement in equipment reliability due to maintenance and risk increase caused by maintenance related equipment unavailability.
- Configuration control: the PSA of an NPP is supposed to be performed by giving appropriate considerations to all kinds of plant operational states and system configurations. This requirement calls for an adequate coverage of all plant and system operating modes in the PSA, but it does not in itself establish a basis for configuration control.
- In-service inspection and testing: the intervals for in-service inspection and testing have to be based on dedicated analysis. Also, reference is made in the requirements to the need to consider risk aspects. However, this requirement is related to the surveillance test intervals of active plant systems rather than inspection frequencies of passive systems.
- Support to establishing and reviewing Technical Specifications: safety analysis is required to determine the allowed outage times and the surveillance test intervals of safety-related plant systems and components. There is no requirement or regulatory guidance in place concerning the methods to be used in this safety analysis.
- Monitoring maintenance effectiveness: this is required by safety regulations to ensure that safety functions are fulfilled with high reliability, and corrective measures are determined and implemented to avoid deteriorating safety performance of active plant equipment.
- Support to training: use has to be made of the PSA results to underpin the development of the training programme of the plant personnel and also to validate the programme.
- Analysis of operational events: the need for safety evaluation and for the assessment of degradation in safety margins appears. However, probabilistic safety assessment are not referred to explicitly.

Nuclear Safety Guideline No 3.11 version 2. was issued in 2014 with recommendations on the quality of PSA and on how to prepare PSA models and tools for internal initiating events and internal hazards in all operational states for existing power plants. Nuclear Safety Guideline No 3a.11 version 1. was issued in 2015 with specific requirements for a new nuclear power plant. The specific recommendations cover PSA model development, containment analysis, analysis of internal and external hazards, uncertainty, sensitivity and importance analyses, and documentation.

During the decision making in all of its regulatory areas the Hungarian Atomic Energy Authority (HAEA) 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 has been continuously making efforts to make explicit uses of risk information, PSA results and PSA insights in its decision-making processes. The HAEA has decided to implement and follow good international practices in that respect. The most important areas of regulatory risk-informed decision making have recently been as follows:

- licensing plant modifications including measures for severe accident management;
- analysis of operational events;
- supervision of maintenance planning and licensing changes to maintenance strategy including the introduction of online maintenance at NPP Paks.

The HAEA directly support research and development activities to make advancement in PSA methods and PSA applications as well – see Chapter 7 and 8 for details.

The HAEA has a limited staff for PSA and it relies on Technical Support Organisations to help PSA-related activities. The Paks NPP, as the major licensee for nuclear installations in Hungary, has a dedicated PSA team within its own organisational unit for technical support, although the PSA models of the plant are developed and maintained in co-operation with external support organisations and PSA experts. The licensee also support R&D as necessary to meet PSA-related regulatory requirements and to make advancement in PSA applications.

3. SAFETY CRITERIA

In the NSC there are several acceptance criteria for safety analyses. In Volume 3 it is prescribed that with consideration to all designed operating conditions and postulated initiating events, excluding sabotage, the frequency of core damage shall not exceed 10-4/year. For all initial operating conditions and effects, excluding sabotage and earthquake, the cumulative frequency of severe accident event sequences resulting in large or early releases shall not exceed 10-5/year, but with every reasonably practicable modification and intervention 10-6/year shall be targeted. The fulfilment of criteria shall be demonstrated by level 2 PSA.

For new power plants the total frequency of events resulting in a partial or full core meltdown for an event sequence originating from all assumed initiating events, except for sabotage, shall not exceed 10-5/year. Events resulting in large or early releases shall be practically eliminated. The total frequency of event sequences resulting in large or early releases summarised for all initiating operating conditions and effects, excluding sabotage, shall not exceed 10-6/year. The fulfilment of the requirements shall be demonstrated by evel 2 PSA.

Other numerical criteria are given in Volume 3 of the NSC, which serve basically for ranking initiating events and for exclusion of initiating events from the scope of assessments for existing nuclear power plants.

The following can be excluded from the scope of postulated initiating events of the design basis:

- an internal initiating event due to the failure of a system, structure or component, and/or human error, if the frequency of occurrence is less than 10^{-5}/year;
- event resulting from external human activity typical of the site, if the frequency of the occurrence is less than 10^{-7}/year, or if the hazard factor is at such a distance, that it can be justified that it will not have an effect on the nuclear power plant unit;
- initiating events occurring due to a recurring external impact of natural origin, with a median frequency of less than 10^{-4}/year, or external effects of natural origin for which it can be demonstrated that they are not able to induce loads that are challenging to the power plant.

The following can be excluded from the scope of initiating events assumed in the definition of the design basis:

- internal initiating events occurring due to the failure of systems, structures or components or human error or both if their frequencies are less than 10^{-6}/year;
- an event resulting from external human activities characteristic to the site, the frequency of which is less than 10^{-7}/year, or if the hazard factor is at a distance that it can be demonstrated that it is not expected to have an effect on the nuclear power plant unit;
- all initiating events triggered by a recurring external effect of natural origin, with a frequency of less than 10^{-5}/year.

For new nuclear power plants there are other criteria in Volume 3a. It shall be ensured that the residual heat is transferred to the ultimate heat sink in such a way that the frequency of the loss of the heat removal function should be lower than 10-7/year.

For new nuclear power plants at least the following events shall be practically excluded by design solutions or the implementation of preventive accident management capabilities, i.e. it shall be demonstrated that their occurrence is physically impossible or the frequencies of their occurrence are less than 10-7/year with high certainty:

- rupture of the reactor vessel;
- reactivity accidents with prompt criticality, including the cases of heterogeneous boric acid dilution;
- all loads appearing in the short and long run, which may jeopardise the integrity of the containment, in particular, the dropping of a heavy load, steam and hydrogen explosion, interaction between the molten core and concrete loadbearing structures, and containment overpressurisation;
- loss of cooling during the storage of irradiated fuel elements, which may lead to damage to the fuel elements;
- loss of coolant with open containment, which may cause core dry out.

Volume 7 of the NSC is regulates site investigation and evaluation for nuclear installations. There are numerical criteria for event frequencies in this volume as well:

- The probability of exceeding the safety earthquake properties annually shall not be higher than 10^{-5}/year. The uncertainty of the data shall be evaluated. In order to avoid the cliff edge effect, the site-specific properties shall be modified appropriately.
- For the identification of the operational basis earthquake, the hazard shall be determined within an occurrence frequency range from 10^{-1}/year to 10^{-3}/year.
- The earthquake hazard exposure and the hazard curve of the earthquake related phenomena shall be determined up to an occurrence frequency of 10^{-7}/year, at least. The uncertainties in the determination of the hazards shall be assessed and the hazard curve, taken for mean value, shall be used.
- If the site is exposed to geotechnical hazard for which no proven engineering solutions or measures can be taken to improve the characteristics of the site, then the probability of the hazard shall not be higher than 10^{-6}/year, taking into account the cliff edge effect.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

NPP Paks, Level 1 PSA

In general, PSA developments have recently been focused on extending the scope of the analyses and on ensuring that PSA models and results adequately represent the actual status of the nuclear installations analysed. The scope of PSA has been broadened primarily by extending the range of initiating events covered. First of all, this extension included PSA for a wider range of external initiating events. Modelling of modifications has been the key part of keeping PSA models and results up-to-date in Hungary. In addition and in a more general sense, there is a living PSA programme in place for the Paks NPP to incorporate the effects of changes and new knowledges into PSA – see further details below under living PSA.

Unit specific level 1 PSA models and results are available for the four VVER/440-213 type reactor units (old reactors) of the Paks NPP. The PSA covers full power, as well as low power and shutdown states. The initiating events analysed include

- internal events;
- internal fires and internal flooding as internal hazards, where the PSA for internal flooding encompasses high energy line breaks too;
- seismic events, extreme weather events (wind, snow, rainfall, ice formation, lightning) and blockage of water intake from the river Danube as external events.

As compared to the previous report, extreme weather events and blockage of water intake have been added to the list of initiating events analysed. Four separate unit specific analyses are at hand for internal events and internal hazards, while PSA for external events has been performed for unit 3 as a reference unit of the analysis.

The four reactors and the four spent fuel pools, as sources of potential large releases, have been subject to PSA modelling in the level 1 PSA for Paks. The scope of plant operational sates and initiating events is identical in the reactor PSA and in the spent fuel pool PSA for the plant.

NPP Paks, Level 2 PSA

The main objectives of the level 2 PSA study carried out for a reference unit were to provide a basis for

- the development of plant-specific accident management strategies;
- the plant-specific backfit analysis and evaluation of risk reduction options;
- the resolution of specific regulatory concerns.

Unit 1 is the reference unit of the level 2 PSA for NPP Paks, except for seismic events where the reference unit is unit 3. The scope of the analysis is comparable to that of the level 1 PSA. Full power, as well as low power and shutdown states are included. Internal events, internal fires, internal flooding and seismic events have been considered. Other external events are not within the scope of level 2 PSA at present.

Similarly to level 1 PSA, reactor as well as spent fuel pool accidents have been considered in the level 2 PSA. However, the treatment of spent fuel pool accidents is simplified as fuel damage in the pool is considered a large release because the spent fuel pool is outside the hermetic area. (Analysis is ongoing to refine this assumption – see Chapter 8.)

In the early 2000s level 2 PSA was used in support of outlining a strategy of severe accident management and developing proposals for the associated accident management measures. Most of these measures have been implemented, and guidelines for severe accident management have been introduced at the plant. The most important measures include the installation of hydrogen recombiners in the containment and external cooling of the reactor pressure vessel by flooding the reactor cavity to prevent vessel failure and installation of severe accident measurements and instrumentation. A recent update of the level 2 PSA covered modelling of the implemented severe accident management measures and guidelines.

NPP Paks, living PSA and post-Fukushima developments

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. As necessary, these updates include modelling of implemented post-Fukushima measures as well. Since most post-Fukushima modifications aim at improving the effectiveness of severe accident management, rather than accident prevention, mainly level 2 PSA needs to be updated. This update will be a future task because the level 2 analysis is renewed less frequently than the level 1 PSA.

There is no living PSA programme in place for the level 2 PSA of NPP Paks. However, the effects of important plant modifications on level 2 PSA results have always been evaluated an example being the power upgrade of the plant.

The Fukushima accident gave momentum to advance in the analysis of external events, although these efforts had started before Fukushima as a result of findings from periodic safety reviews.

PSA for Modular Vault Dry Storage

There is a Modular Vault Dry Storage (MVDS) dry spent fuel storage next to the site of the Paks NPP. PSA is available for this facility too, which quantifies the frequency of accident scenarios related to the facility as well associated dose for the operational personnel and the public (basically a simplified level 3 PSA). The PSA consists of 183 event trees separated into three areas according to the operational features of the facility. PSA results include the frequencies of the different dose rate categories. Modifications to the MVDS are regularly modelled in PSA so that it can be considered a living PSA. It is noted that there are several dose rate criteria in the nuclear safety requirements, but no numerical criteria regarding dose rate frequencies for nuclear storage facilities in Hungary.

5. PSA METHODOLOGY AND DATA

There are no national standards developed in the area of PSA, but there is a regulatory guide on PSA for existing and a separate guide for new nuclear power plants – see Chapter 2.

The requirements on the use of PSA for demonstrating the safety level of the operating nuclear units and the operational/design changes are involved on a general level within the Nuclear Safety Codes as described in Chapter 2. Volume 3 of the codes contains regulatory requirements for existing NPPs, and Volume 3a for new nuclear power plants. Sub-sections of these Volumes summarises requirements to be met by PSA.

No specific international PSA standards and guides have been selected to be strictly followed for the PSA of nuclear installations in Hungary. As PSA studies requiring different types of methodology have been performed for the Paks NPP, the actual analysis procedure was set up and the methodologies to be applied for the main tasks of a given study were defined during the course of the study. For this purpose numerous reference documents have been used, first of all, IAEA procedure guides, NEA documents, ANS PRA Standards, NUREG reports, WENRA and EUR requirements have been considered.

As stated above, the methodologies followed during the level 1 and level 2 PSA for Paks were generally 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, and the needs of PSA for internal hazards and external events. The major analysis steps can be briefly summarised as follows.

Definition of plant operational states: This initial analysis was important for the purposes of the shutdown PSA. The plant operating modes described in the Operating Procedures and Technical Specifications of Paks were decomposed into 24 distinct plant operational states (POSs) that represent a PSA driven breakdown of a complete shutdown-refuelling-start-up process. Within a POS the availability and configuration of plant systems, the system success criteria related to a given initiating event (plant transient), as well as the means and conditions of operator responses to a transient can be considered constant. This approach enabled the development of POS dependent PSA sub-models. A similar approach was used in the spent fuel pool PSA for NPP Paks with the definition of 6 POSs.

Identification of initiating events: For internal 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.

For external events, a multi-step screening analysis was performed to determine those events that required detail PSA modelling. Screening included a combination of qualitative considerations (e.g. screening by relevance) and frequency screening in view of the corresponding regulatory requirements. Events that were found important were subject to probabilistic hazard assessment.

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 Fire-Induced Vulnerability (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.

The commonly followed method of probabilistic seismic hazard assessment was applied to determine seismic hazard curves at various confidence levels. The theory of extreme value distributions was used to determine hazard curves for most extreme weather events (wind, snow, rainfall and ice formation). Lightning frequencies were assessed in a simplified manner on the basis of applicable lightning protection standards and recorded data on lightning.

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 in the level 1 PSA. 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. A similar modelling approach was followed to delineate accident sequences for external events were the transient initiating failures (internal PSA events) and failures in mitigating systems, structures and components were determined on the basis of plant response analysis.

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.

Failures due to external events were added to the internal events fault trees in view of the results of plant response and fragility analysis for seismic as well as extreme weather events.

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 â factor approach. Parametric common-cause failure analysis and quantification was based on internationally accepted methods and on generic data.

Multiple failures due to loads induced by internal hazards as well as external events were explicitly considered as physical dependence.

Human reliability analysis: Human reliability analysis was aimed at selection and quantification of those human failure events 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 using a dedicated method that integrates the results of simulator observations, field experience and expert judgement into a context based 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.

The likelihood of failures induced by internal fires and internal flooding was determined by using specific dedicated analyses.

Seismic failures of SSCs were assessed by seismic fragility analysis using the separation of variables approach. The probability of failures induced by extreme weather events was determined by performing structural reliability analyses.

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.

Separate quantification methods and tools were applied to convolute hazards curves and fragility curves in the external events PSA in order to determine core damage frequency.

The most important methodological features of the level 2 PSA for NPP Paks are highlighted below.

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. 189 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 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.

Plant damage states were determined independently for internal and seismic events. The plant operational states of the level 1 PSA were grouped into full power, shutdown and open reactor states. Important plant damage states were selected by the use of frequency ranking. For example, in case of seismic events, 9 plant damage state were selected for normal operation and 19 for low power and shutdown states. As a result, 46 plant damage states were subject to further detailed analysis, including 17 damage states for power operation and 29 damage states for low power and shutdown modes, 4 of which characterised by an open reactor vessel.

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 22 branch points to model accident progression and the resulting containment damage state. Most importantly, the headings in the CET are concerned with:

- closing the open containment in case of shutdown states;
- primary system depressurisation (by the operators or by an induced break);
- water injection into the vessel before and after core melt, melt retention by melt arrest;
- process of flooding the cavity and long-term water supply;
- recovery of failed containment spray in early or late phase;
- external reactor vessel cooling;
- containment failure due to fast (hydrogen burning, steam explosion, fast steam production, high-pressure melt ejection) and slow overpressurisation in different phases of accident progression;
- filtered venting of the containment;

- containment failure due to temperature loads from severe accident;
- operation of different ventilation systems in the reactor hall.

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 states and the release into the environment. The results of obtained were used for calculating the containment pressure loads due to hydrogen burn. Pressure loads from hydrogen combustion were determined for spontaneous ignition and ignition caused by recombiners for design-basis accidents and for severe accidents. The probability of the ignition was used to express the containment pressure loads in the form of probability distribution. The pressure load curves were convoluted against the fragility of the containment to obtain the probability of containment failure.

The probabilistic pressure capacity and 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, while 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 time windows for recovery. Separate recovery analysis was performed for each dominant plant damage state.

Human failure events were taken into account for recovery of the emergency core cooling systems and containment spray, and for taking severe accident management actions. The environmental conditions (number of failures – fire, fission product release, earthquake magnitude), the complexity of the decision, available time for the quality of the specific guideline in the severe accident management guidelines determines the probability of human error.

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.

Containment damage states and categories of releases: The containment damage states were grouped into different release categories. The containment damage states include a range of containment states, for example basemat melt-through or initially open containment. The release categories take into account only the timing and amount of atmospheric release to the environment. As an example, the initially open containment with successful reactor vessel cooling and the early containment failure due to hydrogen burn with core-concrete interaction yield to basemat failure belonging to different containment damage states but the same release category. The following main release categories were used for the purpose of CET modelling:

1. Catastrophic containment failure;
2. Containment By-pass (B);
3. Early Containment Failure, Rupture (ECF) – Break size of 0.5 m^2 or higher;
4. Early Containment Enhanced Leakage (ECL) – Leak size of 0.05 m^2;
5. Late Containment Failure, Rupture (LCF);
6. Late Containment Enhanced Leakage (LCL);
7. Early Containment Failure, Rupture with Spray (ECFS);
8. Early Containment Enhanced Leakage with Spray (ECLS);
9. Late Containment Failure, Rupture with Spray (LCFS);
10. Late Containment Enhanced Leakage with Spray (LCLS);
11. Intact containment (I);
12. Intact containment with Spray (IS);
13. Partial Core Damage (PDC) – no excessive core melt;
14. Shutdown State, Open Containment Before Refuelling (SDOC_BR);
15. Shutdown State, Open Containment After Refuelling (SDOC_AR).

The source terms and frequencies of the release categories were used to determine large release frequency. A simplified method was applied for the determination of the environmental impact of the release categories. The method is based on the European Utility Requirements for LWR Nuclear Power Plants, Appendix B. Large release means that the environmental impact exceeds the following criteria:

- no Emergency Protection Action beyond 800 m from the reactor during the first 24 hours;
- no Delayed Action at any time beyond about 3 km from the reactor during the first 4 days;
- no Long Term Action at any distance beyond 800 m from the reactor.

Each criterion was verified independently for each release category, according to the following methodology:

- The released activity of 9 reference isotope groups was calculated.
- These releases were combined and compared with one criterion.

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 as 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.

6. NOTABLE RESULTS OF PSAs

Level 1 PSA for the Paks NPP

The latest results from the living level 1 PSA for NPP Paks using unit 3 as a reference are as follows.

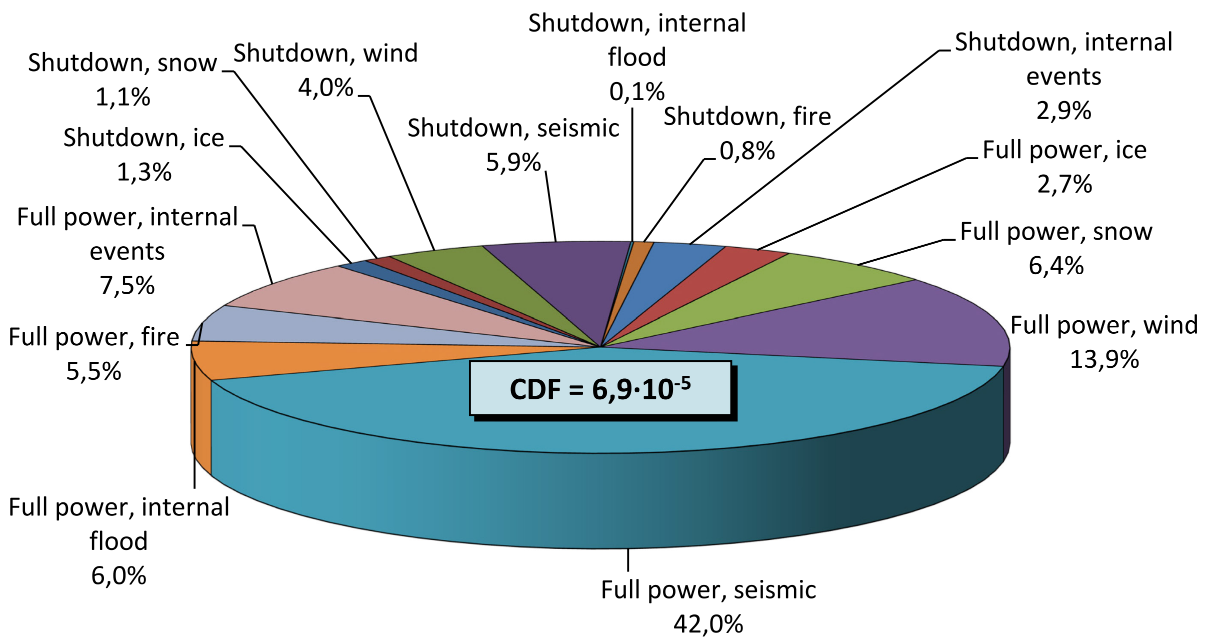
Full power

- CDF from internal events: 5%: $2.10 \cdot 10^{-6}$/year, mean: $5.75 \cdot 10^{-6}$/year, 95%: $1.58 \cdot 10^{-5}$/year;
- CDF from internal fires: mean: $4.21 \cdot 10^{-6}$/year;
- CDF from internal flooding: mean: $4.61 \cdot 10^{-6}$/year;
- CDF from seismic events: 5%: $1.51 \cdot 10^{-6}$/year, mean: $3.23 \cdot 10^{-5}$/year, 95%: $9.07 \cdot 10^{-5}$/year;
- CDF from strong wind: 5%: $1.12 \cdot 10^{-7}$/year, mean: $1.07 \cdot 10^{-5}$/year, 95%: $2.95 \cdot 10^{-4}$/year;
- CDF from extreme snowfall: 5%: $4.53 \cdot 10^{-8}$/year, mean: $4.90 \cdot 10^{-6}$/year, 95%: $3.05 \cdot 10^{-5}$/year;
- CDF from ice formation: 5%: $1.94 \cdot 10^{-7}$/year, mean: $2.07 \cdot 10^{-6}$/year, 95%: $3.83 \cdot 10^{-5}$/year.

Low power and shutdown modes

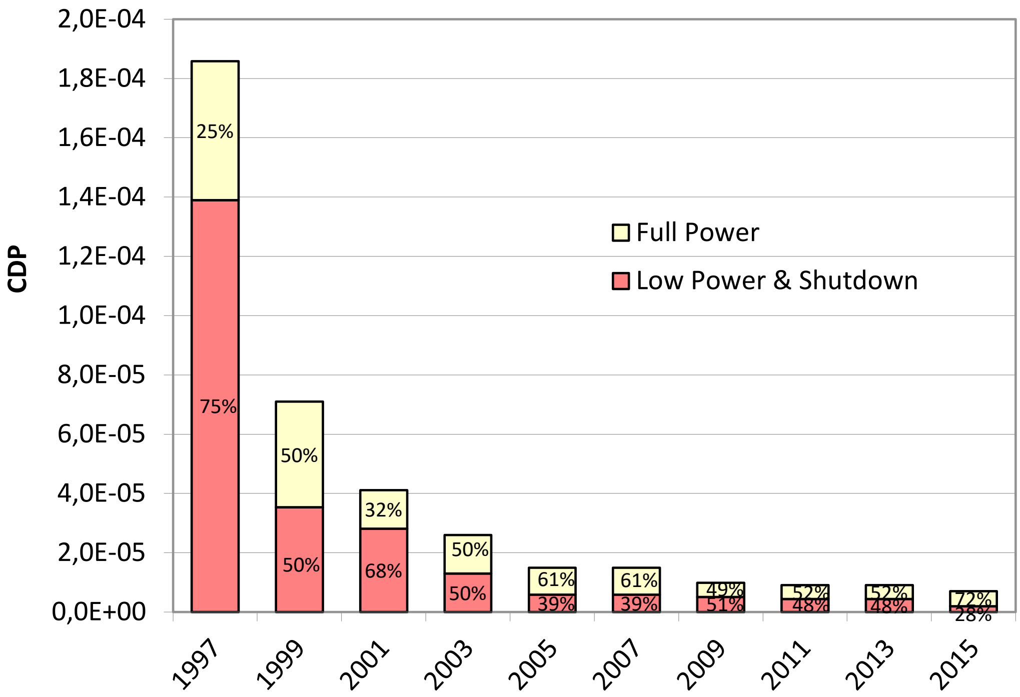
- CDP from internal events: 5 %: $1.15 \cdot 10^{-6}$/outage, mean: $1.98 \cdot 10^{-6}$/outage, 95 %: $4.23 \cdot 10^{-6}$/outage;
- CDP from internal fires: mean: $5.49 \cdot 10^{-7}$/outage;
- CDP from internal flooding: mean: $7.74 \cdot 10^{-8}$/outage;
- CDP from seismic events: 5 %: $1.15 \cdot 10^{-7}$/outage, mean: $4.06 \cdot 10^{-6}$/outage, 95 %: $1.35 \cdot 10^{-5}$/outage;
- CDP from strong wind: 5 %: $2.88 \cdot 10^{-8}$/outage, mean: $2.75 \cdot 10^{-6}$/outage, 95 %: $5.01 \cdot 10^{-5}$/outage;
- CDP from extreme snowfall: 5 %: $7.23 \cdot 10^{-9}$/outage, mean: $7.82 \cdot 10^{-7}$/outage, 95 %: $4.87 \cdot 10^{-6}$/outage;
- CDP from ice formation: 5 %: $8.67 \cdot 10^{-8}$/outage, mean: $9.24 \cdot 10^{-7}$/outage, 95 %: $1.71 \cdot 10^{-5}$/outage.

The following Figure demonstrates the relative contributions of the various risk factors to the yearly average CDF.



Distribution of CDF over Major Contributors, NPP Paks, Unit 3

The Figure below shows the changes in CDF from internal events over time. The risk decrease is mostly attributable to the implemented safety improvements.



Time History of CDF from Internal Events, NPP Paks, Unit 2

Spent fuel pool

- mean FDF (Fuel Damage Frequency) from internal events and internal hazards: $6.89 \cdot 10^{-7}$/year;
- mean FDF from seismic events: $1.64 \cdot 10^{-5}$/year;
- mean FDF from strong wind: $2.04 \cdot 10^{-5}$/year;
- mean FDF from extreme snowfall: $7.63 \cdot 10^{-6}$/year;
- mean FDF from ice formation: $6.69 \cdot 10^{-6}$/year.

Level 2 PSA for the Paks NPP

The results of the level 2 PSA for unit 1 of NPP Paks after the implementation of measures and guidelines for severe accident management can be summarised as follows.

Full power

- Internal events and internal hazards:
  - Mean large release frequency, LRF (including early and late releases): $9.62 \cdot 10^{-7}$/year;
  - Mean frequency of beyond-design-basis releases not exceeding the EUR criteria for limited impact: $1.30 \cdot 10^{-5}$/year.
- Seismic events:
  - Mean LRF: $1.36 \cdot 10^{-5}$/year;
  - Mean frequency of beyond-design-basis releases not exceeding the EUR criteria for limited impact: $2.48 \cdot 10^{-5}$/year.

Low power and shutdown modes

- Internal events and internal hazards:
  - Large release probability, LRP (including early and late releases): $1.86 \cdot 10^{-6}$/outage;
  - Probability of beyond-design-basis releases not exceeding the EUR criteria for limited impact: $6.8 \cdot 10^{-7}$/outage.
- Seismic events:
  - Large release probability, LRP (including early and late releases): $3.95 \cdot 10^{-6}$/outage;
  - Probability of beyond-design-basis releases not exceeding the EUR criteria for limited impact: $2.0 \cdot 10^{-7}$/outage.

Implementation of severe accident management has helped to reduce the frequency of large releases by more than an order of magnitude for internal events and by a factor of 4 for seismic events at full power. The introduction of hydrogen management (passive catalytic recombiners) has remarkably lowered the frequency of early containment rupture due to hydrogen burn. The introduction of severe accident management guidelines (SAMG) was another important modification which decreased the frequency of large release. It was found that new guidelines introduced for primary system depressurisation at the transition between the use of emergency operating procedures and SAMG and also in the SAMG markedly reduced the probability of the high-pressure melt ejection (that would lead to catastrophic containment failure). The external cooling of the reactor vessel with flooding of the reactor cavity reduced the frequency of basemat melt-through type containment failure for internal events by more than an order of magnitude.

7. PSA APPLICATIONS AND DECISION MAKING

For NPP Paks living PSA helps to follow changes in the safety level of the plant, and it also ensures that safety-related decisions can be supported by up-to-date risk models and data. Living PSA enables a range of PSA applications and it provides a precondition for the usefulness and credibility of results gained from the applications. The living PSA models and results for NPP Paks have been used in a number of PSA applications. Both utility and regulatory activities have been supported by these applications.

The most important PSA applications by the Paks NPP have been as follows:

- development of recommendations for safety improvement and use of PSA during design and implementation of plant modifications;
- evaluating the safety level of the plant and trends in safety performance from PSA point of view, identifying vulnerabilities and issues of potential safety concern during periodic safety reviews required in every 10 years by nuclear safety regulations,
- PSA-based analysis of operational events;
- unique PSA applications (analyses) to support recovery from the consequences of the ex-core fuel damage event at Paks in April 2003;
- use of PSA to determine probabilistic performance indicators and criteria for safety systems and components in support of monitoring maintenance effectiveness;
- assessment of plant vulnerability to external events and safety margin beyond the design basis during the post-Fukushima targeted safety reassessment (stress test) of the plant;
- dedicated probabilistic analyses to support modifications to limiting conditions of operation laid down in Technical Specifications;
- selection of severe accident sequences from level 2 PSA for training the Technical Support Centre staff;
- dedicated analyses performed by using the plant-specific risk monitor to support the introduction of online maintenance for selected safety systems;
- developmental efforts to better exploit the capabilities of the plant-specific risk monitor (ongoing – see Chapter 8).

The role of PSA in underpinning plant modifications/upgrades at NPP Paks has to be emphasised. Use of PSA in support of severe accident management is of particular importance due to lessons learnt from the Fukushima accident. Severe accident analyses performed prior to the level 2 PSA for Paks had already outlined potential severe accident management measures for the plant. Subsequently, the level 2 PSA results were used to:

- prioritise measures from risk reduction point of view;
- select feasible and effective measures;
- develop technical requirements for certain measures.

After implementing measures for severe accident management at the plant, level 2 PSA was further applied to:

- determine risk reduction (probability of large release) and compare risk level with criteria, thus demonstrate the safety level of the plant;
- check the adequacy of the plant modifications, the severe accident management measures;
- identify residual vulnerabilities in the mitigation of severe accidents and outline options for further risk reduction (still ongoing).

The four units of NPP Paks have undergone a continuous upgrade process since start-up. This is why PSA-based analysis of plant modifications that supports this upgrade process has become the most important PSA application. According to the regulatory approach and requirements, it should be proved that each modification maintains or increases the safety level. In order to gain the most complete insights not only deterministic principles but also probabilistic evaluations are 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 plant modifications it is to be shown and reviewed by the HAEA that the calculated overall risk impact (in terms of changes in level 1 and level 2 PSA results) is favourable or, at worst, negligible. In many cases the design of plant modifications have been customised based on calculated risk characteristics.

PSA-based analysis of licensee events has been going on for about 20 years at the HAEA to evaluate risk significance of events and identify precursors to severe accidents. The objectives of the precursor event analysis programme using probabilistic methods are as follows:

- determination of the risk significance of the operational events, identification of the most significant ones and their ranking;
- early signalisation of negative trends in performance;
- drawing conclusions based on the risk significance of operational events and identification of necessary corrective actions by the licensee and/or the safety authority;
- feedback to the PSA model and data used.

A computerised tool has been developed and used for precursor event analysis. Licensee Event Reports are evaluated quarterly and the summarised results are used as risk-based indicators of operational safety at the Paks NPP. In addition to analysing precursors to severe accident, the effect of system and/or component unavailability (as reported in the licensee event reports) on the instantaneous core damage frequency is determined by using a dedicated regulatory analysis tool that is a simplified risk monitor of the plant.

A so-called risk prediction system is available at the HAEA, which can be used in an emergency at the Centre for Emergency Training and Awareness of the authority to assess the likelihood of a severe accident. This computerised tool uses the plant-specific

PSA models and additional data specified by the user during the evolution of an event to calculate the occurrence probability of a severe accident.

8. FUTURE DEVELOPMENTS AND RESEARCH

Ongoing and planned PSA developments in Hungary aim mostly at:

- extending the scope of the analysis to better cover risk contributors and to better understand the role of various risk factors;
- improving modelling methods, adequacy and input data to enhance credibility and usefulness of PSA results;
- making advancement in PSA applications in a risk-informed decision-making framework.

The most important developmental areas of current interest are briefly characterised below.

PSA for external events

Continued efforts are made to improve the available PSA for external events. Ongoing and planned improvements include developments in analysis scope, methodology and data. The scope of the analysis will be extended with events that could not be screened out decisively from the scope of detailed modelling for NPP Paks. In particular, extremes in ambient temperature and tornadoes are currently subject to analysis. Concerning methodology and data, the technical areas to be addressed further cover probabilistic hazard assessment for a wide range of hazards, analysis of plant response and fragility of SSCs by considering loads induced by different types of external events, and human reliability analysis. How to perform a PSA for external events that is appropriate for use in site level risk assessment is also in the focus of interest and ongoing development. Developments for an adequate treatment of combined external hazards from the point of view of both hazards assessment and consequence analysis is on the agenda of research for a longer term.

Site level risk assessment and multi-unit PSA

A pilot study has recently been conducted on developing an initial site risk model for the Paks NPP. Loss of off-site power was the reference initiating event in that study. Further to the pilot study, follow-on analysis is in preparation to perform a multi-unit level 1 PSA for the four units of the Paks plant to the extent reasonably practicable. The ultimate goals of the follow-on analysis are to

- quantify and evaluate level 1 PSA measures (core damage and fuel damage risk) for the whole site;
- identify analysis areas and associated technical issues in need of improvement or refinement to yield credible risk estimates;
- examine how the level 1 PSA for the site can be developed into a level 2 PSA.

PSA data update

The data base for component reliability and initiating events used in the PSA for the Paks NPP is planned to be updated. In general, reliability data in the Paks PSA represent a combination of generic and plant-specific data with preference to the use of plant-specific data to the greatest possible extent. The planned data update will be primarily based on making use of plant statistics from the past 10 years in a Bayesian data analysis framework.

Support to severe accident management

Based on the available level 2 PSA for Paks, parametric studies have been performed in support of the design of an active containment cooling system to prevent long term overpressurisation of the containment during a severe accident. Detailed design, construction and installation of this system is planned for the next phase. PSA is supposed to be used as a tool to ensure adequacy of the design from risk point of view.

Improvements in spent fuel pool PSA

Analysis has started to refine the level 2 PSA for the spent fuel pool of the Paks NPP. Release paths have been defined and modelled with considerations to the operating mode of the pool and to the availability and operating modes of ventilation systems in the reactor hall as a function of scenario dependent system failures and human interventions. Deterministic analyses of source term for the different possible operational states of the pool and for the different paths will be performed in the next step. Finally, release magnitude and conditional release probability will be assessed in a path dependent manner.

Research activities within the Sustainable Nuclear Energy Platform in Hungary

Research and development activities under the auspices of the Sustainable Nuclear Energy Platform in Hungary include developments in the following areas of PSA for nuclear installations:

- better integration of deterministic and probabilistic safety analysis, including treatment of uncertainties;
- human reliability analysis;
- common-cause failure analysis;
- dynamic PSA.

In addition, there is a dedicated research task on the agenda of the Platform to develop PSA for the planned demonstration reactor, called ALLEGRO, for a Generation IV gas-cooled fast reactor.

PSA applications at NPP Paks

Development is ongoing at the plant to advance in risk-informed applications based mostly on the use of the plant-specific risk monitor that is available for the four units. First of all, the risk monitor is to be applied as a risk management tool in the area of outage planning, configuration control and refinement of Technical Specifications.

9. INTERNATIONAL ACTIVITIES

The nuclear safety authority, the licensees and the technical support organisations from Hungary take part in PSA-related activities of the NEA and the IAEA. The Paks NPP as a licensee contributes to the work of WANO as well, although PSA is not explicitly present in WANO work.

Within the framework of the so-called VVER Forum, which is a forum of state nuclear safety authorities of the countries operating VVER type reactors, there is a PSA Workgroup. The goal of the group is to compile and compare the legal and regulatory framework of the member countries in the field of PSA in order to find the best practices and to use the accumulated information as a reference or input for further improvements and amendments for the national frameworks. Currently the PSA Workgroup plans to collect information from the member countries in the following fields:

- lessons learnt after Fukushima;
- comparison of current EE PSA approaches and regulations;
- risk-informed inspection;
- risk-informed decision making;
- reliability-centred maintenance and monitoring maintenance effectiveness;
- annual evaluation of outage (shut down) risks;
- use of RIRIS – an indicator system developed in order to visualise the changes in the PSA framework on a long term in the different member countries, in order to help the regulatory bodies to find the most relevant areas of possible improvements to keep up with the scientific and technological development.

There is participation from Hungary in the European ASAMPSA_E project that aims at describing good practices for safety analysis, evaluation of safety level (including identification of vulnerabilities) and decision making by developing and making use of an “extended PSA” with particular emphasis on external events (see www.asampsa.eu for more details on this project).

Hungarian technical support organisations of the Hungarian Atomic Energy Authority have recently joined the European Technical Safety Organisations Network (ETSON), and members have been delegated from Hungary into the Expert Group on PSA of ETSON.

The V4G4 Centre of Excellence as a legal entity, established with participation of technical support organisations from the Czech Republic, Hungary, Poland and the Slovak Republic, is in charge of co-ordinating design of the ALLEGRO demonstration reactor. The so-called Design and Safety

Roadmap of ALLEGRO integrates PSA and the use of PSA for safety demonstration and feedback to design into the whole design process. PSA activities for ALLEGRO are in an early phase, mostly preparatory studies have been performed up-to-date on order to develop PSA methodology applicable to this reactor design.

APPENDIX: Overview of the status of PSA programmes in Hungary

Overview of the PSA Programmes in Hungary								
Plant Name	**Plant type**	**Scope of the PSA carried out**				**PSA usage**		
		Level of PSA	**Initiating events**	**Plant Operating States**	**Living PSA**	**Date of original PSA/ revisions**	**Reason for carrying out PSA**	**PSA applications**
Paks, unit 3	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1994 Revision: annually	AGNES project and regulatory requirements	*
Paks, units 1 and 2	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1995 Revision: annually	Periodic safety review	*
Paks NPP, unit 2	VVER-440/213	Level 1	Internal events	Low power and shutdown states of a refuelling outage	Yes	Original: 1997 Revision: annually	Regulatory requirements	*

Paks, unit 4	VVER-440/213	Level 1	Internal events	Full power	Yes	Original: 1998 Revision: annually	Periodic safety review	*
Paks, unit 1	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 1999 Revision: annually	Regulatory requirements	*
Paks, unit 2	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 2001 Revision: annually	Regulatory requirements	*
Paks, units 3 and 4	VVER-440/213	Level 1	Internal fires, internal flooding	Full power	Yes	Original: 2002 Revision: annually	Regulatory requirements	*
Paks, unit 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, units 1, 3 and 4	VVER-440/213	Level 1	Internal events, internal fires, internal flooding	Low power and shutdown states of a refuelling outage	Yes	Original: 2011 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 3	VVER-440/213	Level 1	Extreme weather events	Full power, as well as low power and shutdown states of a refuelling outage	No	Original: 2012 Revision: ongoing	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: 2006 Revision: annually	Regulatory requirements	*
Paks, unit 3, spent fuel storage pool	VVER-440/213	Level 1	Extreme weather events	All planned plant operational states	No	Original: 2013 Revision: no	Regulatory requirements	*
Paks, unit 3, spent fuel storage pool	VVER-440/213	Level 1	Seismic events	All planned plant operational states	No	Original: 2014 Revision: no	Regulatory requirements	*
Paks, unit 1, reactor and spent fuel storage pool	VVER-440/213	Level 2	Internal events, internal fires and internal flooding	Full power, Low power and shutdown states of a refuelling outage for reactor, all planned plant operational states for spent fuel storage pool	No	Original: 2003 Revision: 2008 for power upgrade. A large revision of	Regulatory requirements	*

						the analysis due to severe accident management lead to a whole new study listed as original in two rows below.		
Paks, unit 3	VVER-440/213	Level 2	Seismic events	Full power	No	Original: 2006 Revision: a large revision of the analysis due to severe accident management lead to a whole new study listed as original in the next row.	Regulatory requirements	*

Paks, unit 1 (unit 3 for seismic)	VVER/440/213	Level 2	Internal events, internal fires, internal flooding and seismic events	Full power, Low power and shutdown states of a refuelling outage	No	Original: 2015 Revision: no	Plant modifications (severe accident management)	*
Paks, spent fuel storage pool	VVER/440/213	Level 2	Internal events, internal fires and internal flooding	All planned operational states	No	Ongoing	Plant modifications and new deterministic calculation method	*

*The models and the associated results form the basis of PSA applications for NPP Paks as listed in Chapter 7.

INDIA

1. INTRODUCTION

2. PSA FRAMEWORK and ENVIRONMENT

Use of PSA in NPP regulation - Historical Perspective

In India the regulatory body is the Authorised agency by the Government for the regulation of Nuclear Power Plants (NPPs), radiation facilities and fuel cycle facilities (FCF) in India. As a part of regulatory practices, the regulatory body enforces standards and issues authorisation for siting, design, construction, commissioning, operation and decommissioning of above-mentioned facilities ensuring safety. It also conducts periodic safety review for reauthorisation during the operating life of a plant based on plant performance, revised safety reports submitted by utility to account for modifications carried out during the period, if any, and updated plant-specific data. The Research and Development organisations provide technical support (TSO) to the regulatory body. The utility is the responsible organisation for design, construction, commissioning, operation and decommissioning of Nuclear Power Plants.

In the early days, the NPPs were licensed by the regulatory body 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 analysis reports. In line with international practices and PSA developments, PSA studies have been performed by TSO and utility. Presently utility performs Level-1 PSA for all its operating stations as well as the projects at design stage.Level-2 PSA has also been carried out for a typical PHWR. The regulatory body utilises the information provided by these studies as a complementary tool to traditional deterministic methods into regulatory decision-making. Currently, Level 1 PSA is mandatory requirement for licensing and reauthorisation as risk-informed approach is being followed in the regulation.

Regulatory Requirements for PSA

The assessment of system reliabilities was one of the regulatory requirements for the application for renewal of authorisation (AERB/SG/O-12, 2000). In 2008, the regulatory body made it mandatory for utility to submit Level-1 PSA (internal events, full power) for all new NPPs before the first approach to criticality (AERB/NPP/SC/O, 2008). For NPPs in operations, as per the regulatory body requirements, AERB/NPP/SC/O (Rev. 1) the PSA studies shall be updated as a part of periodic safety review report . 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. Considerations arising from Fukushima event have been included in the relevant regulatory requirements.

3. NUMERICAL SAFETY CRITERIA

Safety target for level 1 PSA (i.e. system reliability targets, core damage frequency, large early release frequency) have been defined in the regulatory documents. Presently, risk-informed approach is being followed and outcome of PSA studies are appropriately considered. The PSA study provides 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. The quantitative targets are also defined in both new and revised regulatory safety documents of AERB (e.g. AERB/NPP-LWR/SC-D, 2015, AERB/NF/SC/S, Rev.1, 2014, etc.).

PSA standards and Guidance

Regulatory safety codes establish the objectives and set minimum requirements that shall be fulfilled to provide adequate assurance of safety. The regulatory body 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 for NPPs and research reactors. This document gives comprehensive coverage on various elements of PSA, guidance on regulatory review and quality assurance in PSA.

Few PSA 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, the regulatory body prepared a compendium on generic component reliability database (AERB/NPP/TD/O-1, 2006) based on various generic data sources available. 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. The regulatory body prepared a compendium on HRA for PSA of NPPs (AERB/NPP/TD/O-2, 2008). 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.

The regulatory body has published safety guide on ‘Regulatory Review of Level-1 Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors (AERB/NPP&RR/SG/G-10, 2015) which provides guidelines for regulatory review of Leve-1 PSA.

4. STATUS AND SCOPE OF PSA PROGRAMMES

The Level-1 PSAs considering the internal events at full-power operation stage are performed for all Indian NPPs (design stage and operation stage). These PSAs are reviewed and assessed by the regulatory body. PSAs are also revised every 5 years based on the plant-specific data for the reporting period as a part for relicensing. These PSAs are reviewed by the regulatory body

The latest regulatory documents call for full-scope PSA at design stage itself. Full-scope PSA is in various stages of completion for all operating plants. Development of external event PSA (i.e. flood, seismic), internal hazards (i.e. fire, flood) and low power and shutdown PSA has been completed for a representative NPP and are in progress for all the NPPs. Level-2 PSA study for a representative NPP was completed by the utility, reviewed by the regulatory body and subsequently revised by the utility. Currently, this revised version of the Level-2 PSA is undergoing regulatory review. This study was used to identify the severe accident scenarios for development of Severe Accident management Guidelines (SAMG) by utility. India is actively participating in the benchmark studies related to PSA of multi-unit sites (MUPSA). The methodology developed for MUPSA is being implemented on a representative site.

5. 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 international documents such as IAEA and USNRC. 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. Utility has developed Procedure for conducting Level-1 PSA-based on IAEA guidelines. The methods to be used for various PSA tasks are described in this to standardise the methodology for all the NPPs.

Common Cause Failure Analyses are done using multi-parameter models described in NUREGs using generic parameters. Human Reliability Analysis (HRA) is performed first generation methods such as THERP, ASEP, HCR etc with generic parameters/coefficients. A judicious mixture of plant-specific and generic data is used in PSAs for operating stations'

Low Power and Shut down PSAs are performed based on the methodology given in IAEA TECDOC 1144. Procedure has been developed for the same by the utility.

Fire PSA is performed based on methodology outlined in NUREG 6850. Internal Flood PSA is performed based on methodology outlined in the procedure developed by utility which is in line with EPRI guidelines (Report 1019194, 2009).

A major task in external Events PSA is the development of the Hazard such as seismic Hazard analysis in case of seismic PSA, Flood Hazard (Rainfall, dam break, Tsunami, Storm surge as applicable). Hazard development is done based on standard methodology and the base case Internal Events level-1 PSA model is analysed for quantification of CDF.

The Level-2 PSA considering the internal events at full-power operation stage for Indian NPP was performed as per the procedure given international documents such as IAEA and USNRC.

The PSA study is subjected to a Peer Review by an independent team at the utility. The PSA report after Peer Review and appropriate approvals is further reviewed by regulatory body for acceptance for PSA Applications.

6. RESULTS AND INSIGHTS FROM THE PSAs

- Confirmation of well balanced designed and the contribution from individual Initiating Events to the CDF

- 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 revealed to be an important step during reactor start-up to ensure their desired position after maintenance.

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, inputs to development of SAMG and Periodic Safety Review .

8. FUTURE DEVELOPMENTS 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. Digital System Reliability Assessment

B. Human Factor development and Human Reliability prediction

C. Simulator studies for development of plant-specific parameters for HRA

D. Structural System Reliability modelling

E. Passive System Reliability modelling

F. Multi-Unit PSA

G. Dynamic PSA

H. Development and Application of improved Methods for Reliability modelling

I. Ageing PSA

J. Integration of Probabilistic and Deterministic Approaches

References

[1] Atomic Energy Regulatory Board, AERB Safety Code on Nuclear power Plant Operation, AERB/NPP/SC/O (Rev. 1), 2008.

[2] Atomic Energy Regulatory Board, Renewal of Authorization for Operation of Nuclear Power Plants, AERB/NPP/SG/O-12, August 2000.

[3] Atomic Energy Regulatory Board, Probabilistic safety assessment for nuclear power plants and research reactors, AERB/NPP&RR/SM/O-1, March 2008.

[4] Atomic Energy Regulatory Board, AERB Safety Code on Design Of Pressurised Heavy Water Reactor Based Nuclear Power Plants, AERB/NPP-PHWR/SC/D (Rev. 1), 2009.

[5] Atomic Energy Regulatory Board, AERB Safety Code on Design Of Light Water Reactor Based Nuclear Power Plants.(AERB/NPP-LWR/SC/D), 2015.

[6] Atomic Energy Regulatory Board, AERB safety regulatory review of level-1 probabilistic safety assessment for nuclear power plants and research reactors (AERB/NPP&RR/SG/G-10).

[7] International Atomic Energy Agency, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, SSG-3, 2010.

[8] International Atomic Energy Agency, Deterministic Safety Analysis for Nuclear Power Plants, SSG -2, 2009.

[9] International Atomic Energy Agency, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, TECDOC-1200, February 2001.

[10] Generic CANDU Probabilistic Safety Assessment – Methodology, 91-03660-AR-001, Rev.-1, July 2002.

[11] American Society for Mechanical Engineers, Standard for PRA for NPP applications, ASME RA-Sb-2005.

[12] International Atomic Energy Agency, A framework for a quality assurance programme for PSA, IAEA-TECDOC-1101, Vienna, 1999.

[13] International Atomic Energy Agerncy, Generic Component Reliability Data for Research Reactor PSA**,** IAEA-TECDOC-930, Vienna.

[14] International Atomic Energy Agency, PSA for Shutdown Mode for Nuclear Power Plants, TECDOC-751, IAEA, Vienna, 1994.

[15] International Atomic Energy Agency, Living Probabilistic Safety Assessment (LPSA), TECDOC-1106, August 1999.

[16] International Atomic Energy Agency, Component Reliability Data for Use. In Probabilistic Safety Assessment, IAEA-TECDOC-478, Vienna, 1988.

ITALY

1. INTRODUCTION

To be written later

2. PSA FRAMEWORK AND ENVIRONMENT

In June 2011 Italian people in a national referendum has voted against a return to nuclear power, repealing regulation that allowed for the construction of new reactors. Consequently various PSA-related activities have been devoted, for the most, to research in nuclear safety, addressing specific aspects, such as reliability of passive systems (Italy has participated through ENEA (denominated Italian National Agency for New Technologies, Energy and Sustainable Economic Development) and University of Pisa to the IAEA CRP on "Development of Methodologies for the Assessment of Passive Safety System Performance in Advanced Reactors" (2008-2012) [1], advanced reactors PSA (as the CSNI task on "PSA for New and Advanced Reactors"), including GenIV reactors and Level2 PSA aspects [2], Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) [3]. These activities have been conducted mostly by research organisations (as ENEA) and technical Universities (like Politecnico di Milano and University of Pisa). In addition several initiatives have been undertaken in the aftermath of Fukushima accident.

3. 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. STATUS AND SCOPE OF ONGOING PSA STUDIES

Post-Fukushima actions have been undertaken as domestic projects supported by the Italian Ministry for Economic Development, to reflect lessons learnt from the Fukushima accident in order to maintain the competences in the field of nuclear safety.

They cover some gaps as highlighted by the Fukushima accident such as the analysis of the combination of external events as initiating events, the assessment of risk relative to sites with many units, the examination of accident scenarios involving the performance of safety systems, such as for heat removal, for prolonged periods of time and the risk associated with spent fuel pools, including some aspects related to level2 PSA and SAM implementation.

To this aim, for instance, some foundational notions to develop the PSA models related to specific aspects, such as the wide-site risk (including multi-units and spent fuel pools) events and the hazard combination, e.g. earthquake and tsunami as at the Fukushima accident, are proposed and discussed for their implementation within the risk assessment methodology. [4].

5. PSA METHODOLOGY AND DATA

6. NOTABLE RESULTS OF PSAs

7. PSA APPLICATIONS AND DECISION MAKING

8. FUTURE DEVELOPMENTS AND RESEARCH

Some activities related to Fukushima accident with main focus on risk assessment are foreseen in the upcoming years.

9. INTERNATIONAL ACTIVITIES

ENEA is involved in the European funded project denoted ASAMPSA_E (Advanced Safety Assessment: Extended PSA) from 2013 to 2016, to offer a new framework to discuss, at a technical level, how extended PSA can be developed efficiently and be used to verify the robustness of NPPs, against beyond-design-basis accidents, to address the issues and gaps as emerging from the Fukushima accident (like multi-unit site risk, severe accident studies, Level2 PSA and SAMGs implementation).

In the ambit of CSNI activities ENEA joined the Senior expert group on safety and research opportunities post-Fukushima (SAREF), to identify and follow up on opportunities to address safety research gaps, as regards, specifically, topics like the multi-unit risk issue, external events and loss of ultimate heat sink.

Finally activities in nuclear safety research with respect to PSA aspects, are conducted by Politecnico di Milano, which concern mainly the following subjects:

- Development of new methods for digital Instrumentation&Control (I&C) system reliability analysis [5-6]
- Development of improved methods and models for passive system reliability assessment [7]
- Development of computational methods for fault detection, failure diagnostics and prognostics of NPPs sensors and components [8-24]
- Development of new methods for the identification of prime implicants for system dynamic reliability analysis [25-27]
- Development of new Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) methods for the post-processing of accident sequences [28-29]
- Development of new IDPSA methods for identifying prototypical sequences of different failure domains (FD) [30]
- Development of new methods for efficient Monte Carlo simulation to propagate epistemic and aleatory uncertainties for sensitivity analysis [31-36]

To this respect a lot of scientific articles are referenced in peer reviewed journals.

References

1. IAEA-TEC-DOC-1752, Progress in Methodologies for the Assessment of Passive Safety Systems in Advanced Reactors, March 2012
2. Burgazzi L., Problems facing the use of passive safety systems, proceedings of OECD/NEA Workshop on PSA of new and advanced reactors, Paris, 20-24 June 2011, NEA/CSNI/R(2012)2
3. Zio, E., INTEGRATED DETERMINISTIC AND PROBABILISTIC SAFETY ANALYSIS: CONCEPTS, CHALLENGES, RESEARCH DIRECTIONS, Nuclear Engineering and Design 280 (2014) 413–419
4. Burgazzi L., Implementation of PSA models to estimate the probabilities associated with external event combination, proceedings of International workshop on PSA of Natural External Hazards including Earthquakes, Prague, Czech Republic, 17-19 June 2013, NEA/CSNI/R(2014)9
5. W. Wang, F. Di Maio, E. Zio, “Component- and System-level Degradation of Digital Instrumentation and control systems based on a Multi-State Physics Modelling approach”, accepted, Annals of Nuclear Energy.
6. F. Di Maio, P. Secchi, S. Vantini, E. Zio, “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, Volume 60, Issue 2, June 2011, pages 415-425.
7. F. Di Maio, D. Colli, E. Zio, L. Tao, J. Tong, “A Multi-State Physics Modeling Approach for the Reliability Assessment of Nuclear Power Plants Piping Systems”, Annals of Nuclear Energy, 80, 151–165, 2015.
8. S. Al-Dahidi, F. Di Maio, P. Baraldi, E. Zio, R. Seraoui, “A novel ensemble approach for clustering operational transients of a NPP turbine”, International Journal of Prognostics and Health Management, Vol 6 (Special Issue Nuclear Energy PHM), ISSN 2153-2648, (open access), pages: 21, 2015.
9. P. Baraldi, F. Di Maio, D. Genini, E. Zio, “Comparison of data-driven reconstruction methods for fault detection“,DOI 10.1109/TR.2015.2436384, IEEE Transactions on Reliability, Vol. 64 (3), pp. 852-860, 2015.
10. P. Baraldi, P. Turati, F. Di Maio, E. Zio, “Robust signal reconstruction for condition monitoring of industrial components via a modified Auto Associative Kernel Regression method”, Mechanical Systems and Signal Processing, 60-61, 29–44, 2015.
11. P. Baraldi, F. Di Maio, E. Zio, M. Rigamonti, R. Seraoui, “Clustering for unsupervised fault diagnosis in nuclear turbine shut-down transients”, Mechanical Systems and Signal Processing, Volumes 58–59, Pages 160–178, June 2015.
12. Y. Hu, P. Baraldi, F. Di Maio, E. Zio, “A Particle Filtering and Kernel Smoothing-based Approach for New Design Component Prognostics”, Reliability Engineering and System Safety, Vol. 134, 19-31, February 2015.

13. P. Baraldi, F. Di Maio, D. Genini, E. Zio, “Reconstruction of missing data in multidimensional time series by fuzzy similarity”, Applied Soft Computing, Vol. 26, 1–9, January 2015.

14. P. Baraldi, F. Di Maio, E. Zio, M. Rigamonti, R. Seraoui, “Unsupervised clustering of vibration signals for identifying anomalous conditions in a nuclear turbine”, Journal of Intelligent and Fuzzy Systems (JIFS), 28, 1723–1731, DOI:10.3233/IFS-141459.

15. S. Al-Dahidi, F. Di Maio, P. Baraldi, E. Zio “Ensemble Clustering for Fault Diagnosis in Industrial Plants”, Chemical Engineering Transactions, Vol. 43, pp. 1225 - 1230.

16. S. Al-Dahidi, P. Baraldi, F. Di Maio, E. Zio, A novel fault detection system taking into account uncertainties in the reconstructed signals”, Annals of Nuclear Energy, Volume 73, Pages 131–144, 2014.

17. F. Di Maio, P. Baraldi, E. Zio, R. Seraoui, “Fault Detection in Nuclear Power Plants Components by a Combination of Statistical Methods”, IEEE Transactions on Reliability, 62 (4) , pp. 833-845, 2013.

18. P. Baraldi, F. Di Maio, F. Mangili, E. Zio,“A Belief Function Theory Method for Prognostics in Clogging Filters”, Chemical Engineering Transactions, 33, pp. 847-852, 2013.

19. P. Baraldi, F. Di Maio, E. Zio, D. Genini, “A fuzzy similarity based method for signal reconstruction during plant transients”, Chemical Engineering Transactions, 33, pp. 889-894, 2013.

20. P. Baraldi, F. Di Maio, M. Rigamonti, E. Zio, R. Seraoui, “Transients Analysis of a Nuclear Power Plant Component for Fault Diagnosis”, Chemical Engineering Transactions, 33, pp. 895-900, 2013.

21. P. Baraldi, F. Di Maio, E. Zio, “Unsupervised Clustering for Fault Diagnosis in Nuclear Power Plant Components”, International Journal of Computational Intelligence Systems, Vol. 6, No. 4, pp. 764-777, 2013.

22. F. Di Maio, E. Zio, “Failure Prognostics by a Data-Driven Similarity Based Approach”, International Journal of Reliability Quality and Safety Engineering, Vol 20 (2), No.1, pp.1-17, 2013.

23. P. Baraldi, F. Di Maio, L. Pappaglione, E. Zio, R. Seraoui, “Condition Monitoring of Electrical Power Plant Components During Operational Transients”, Proceedings of the Institution of Mechanical Engineers, Part O, Journal of Risk and Reliability, 226(6) 568–583, 2012.

24. E. Zio, F. Di Maio, “Fault Diagnosis and Failure Mode Estimation by a Data-Driven Fuzzy Similarity Approach”, International Journal of Performability Engineering, Vol. 8, No.1, pp. 49-66, 2012.

25. F. Di Maio, S. Baronchelli, E. Zio, “Hierarchical Differential Evolution for Minimal Cut Sets Identification: Application to Nuclear Safety Systems”, European Journal of Operational Research, Volume 238, Issue 2, Pages 645–652, 2014.

26. F. Di Maio, S. Baronchelli, E. Zio, “A Visual Interactive Method for Prime Implicants Identification”, IEEE Transactions on Reliability, 64, Issue 2, 539-549, 2015.

27. F. Di Maio, S. Baronchelli, E. Zio, “A Computational framework for Prime Implicants Identification in non-coherent Dynamic Systems”, Risk Analysis, Vol. 35, No. 1, 142–156, 2015.

28. F. Di Maio, M., Vagnoli, E. Zio, “Transient Identification by Clustering based on Integrated Deterministic and Probabilistic Safety Analysis Outcomes”, Annals of Nuclear Energy, Volume 87, pp. 217–227, 2016.

29. F. Di Maio, M., Vagnoli, E. Zio, “Risk-based clustering for near misses identification in integrated deterministic and probabilistic safety analysis”, Article ID 693891, 29 pages, doi:10.1155/2015/693891, Science and Technology of Nuclear Installations (STNI), Special Issue on IDPSA (open access), 2015.

30. F. Di Maio, A. Bandini, E. Zio, A. Alfonsi, C. Rabiti, “An Approach Based on Support Vector Machines and a K-D Tree Search Algorithm for Identification of the Failure Domain and Safest Operating Conditions in Nuclear Systems“, Progress in Nuclear Energy, Volume 88, pp. 297–309, 2016

31. F. Di Maio, G. Nicola, E. Borgonovo, E. Zio, “Invariant Methods for an ensemble-based Sensitivity Analysis of a Passive Containment Cooling System of an AP1000 Nuclear Power Plant”, Reliability Engineering and System Safety, Volume 151, pp. 12–19, 2016.

32. F. Di Maio, A. Bandini, E. Zio, S. Carlos Alberola, F. Sanchez-Saez, S. Martorell, “Bootstrapped Ensemble-based Sensitivity analysis of a TRACE thermal-hydraulic model based on a limited number of PWR large Break LOCA simulations”, accepted, RESS.

33. F. Di Maio, A. Rai, E. Zio, “A Risk informed safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis”, Reliability Engineering and System Safety, Volume 145, pp. 9–18, 2016.

34. M. Hoseyni, F. Di Maio, M. Vagnoli, E. Zio, M. Pourgol-Mohammad, “A Bayesian ensemble of sensitivity measures for Severe Accident modeling”, Nuclear Engineering and Design, Vol. 295, pp. 182–191, 2015.

35. F. Di Maio, G. Nicola, E. Zio, Y.Yu, “Finite Mixture Models for sensitivity analysis of Thermal Hydraulic Codes for Passive Safety Systems safety Analysis”, Nuclear Engineering and Design, 289, 144–154, 2015.

36. F. Di Maio, G. Nicola, E. Zio, Y.Yu, “Ensemble-based sensitivity analysis of a best estimate thermal hydraulic model: application to a Passive Containment Cooling System of an AP1000 Nuclear Power Plant”, Annals of Nuclear Energy, 73, 200–210, 2014.

JAPAN

1. INTRODUCTION

Here, no contribution is expected from the participants.

2. PRA FRAMEWORK AND ENVIRONMENT

To ensure a transparent separation of regulation and utilisation, the former Nuclear and Industrial Safety Agency (NISA) was decoupled from Ministry of Economy, Trade and Industry, and the Nuclear Regulation Authority (NRA) was established based on the Act for Establishment of the Nuclear Regulation Authority (Act No.47 of 27 June 2012) in 2012. The Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors (issuance: Act No. 166 of 10 June 1957, revised: Act No. 82 of 22 November 2013) (hereinafter called "the Reactor Regulation Act") has revised in 2013.

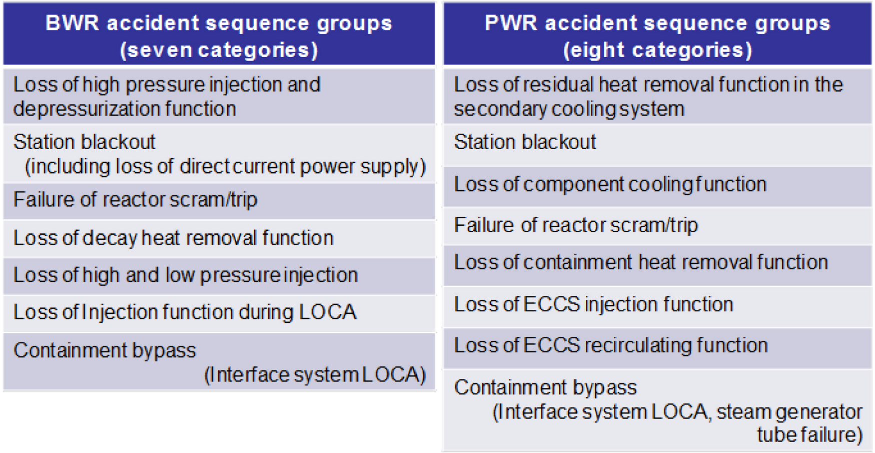
Japan Nuclear Energy Safety Organization (JNES) was merged into NRA in March 2014, and activities of JNES were succeeded by NRA.

The Reactor Regulation Act requires the effectiveness evaluations of countermeasures, and the countermeasures include the measures to prevent core damage and the measures to prevent containment vessel failure. Fig.1. shows the image of differences between previous and new regulatory requirements.

In the new regulation introduced in July 2013, severe accident countermeasures were included in the regulatory requirements. Licensees are obliged to install severe accident management facilities and to implement effectiveness evaluation of those facilities. Regarding accident sequence groups and containment vessel failure modes assumed in effectiveness evaluation process of severe accident management facilities, it is required that licensee shall consider additional accident sequence groups based on the PRA on individual plant, in addition to those designated by NRA. Table 1 shows the designated accident sequence groups, and table 2 shows the designated containment vessel failure modes.

Based on the lessons learnt from the Fukushima Daiichi Accident, Japanese Electric Utilities recognise nuclear risks as the top corporate management issue and decided to improve nuclear safety beyond the regulatory requirement. As a part of industry-wide effort, CRIEPI (Central Research Institute of Electric Power Industry) established NRRC (Nuclear Risk Research Center) on October 1,2014, to conduct R&D for common technical issues (technologies to evaluate the risks of low-frequency high consequence events, application of risk information, etc.)

Table 1. Accident sequence groups for BWR and PWR



BWR accident sequence groups (seven categories)	PWR accident sequence groups (eight categories)
Loss of high pressure injection and depressurization function	Loss of residual heat removal function in the secondary cooling system
Station blackout (including loss of direct current power supply)	Station blackout
Failure of reactor scram/trip	Loss of component cooling function
Loss of decay heat removal function	Failure of reactor scram/trip
Loss of high and low pressure injection	Loss of containment heat removal function
Loss of Injection function during LOCA	Loss of ECCS injection function
Containment bypass (Interface system LOCA)	Loss of ECCS recirculating function
	Containment bypass (Interface system LOCA, steam generator tube failure)

Table 2. Containment failure modes for BWR and PWR

Containment Vessel Failure Modes
Quasi-static loads by internal pressure/temperature (damage by containment vessel overpressurisation/over-heating)
High-pressure melt ejection/direct heating of containment vessel atmosphere
Ex-vessel fuel-coolant interaction (FCI)
Hydrogen explosion
Direct contact with containment vessel (shell attack)
Melted core and concrete interactions (MCCI)

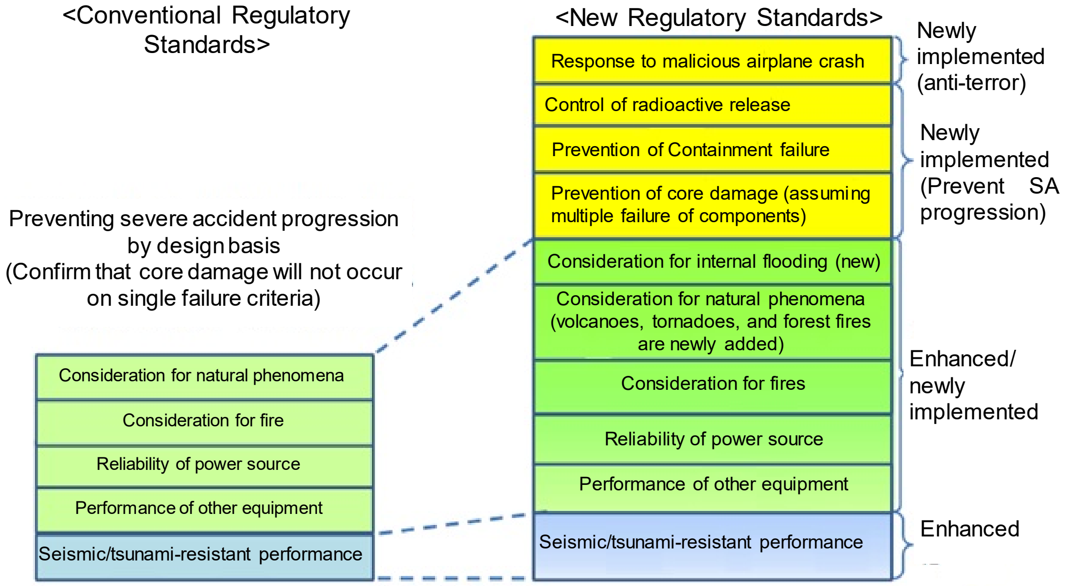

<Conventional Regulatory Standards>
<New Regulatory Standards>
Response to malicious airplane crash
Newly implemented (anti-terror)
Control of radioactive release
Prevention of Containment failure
Newly implemented (Prevent SA progression)
Prevention of core damage (assuming multiple failure of components)
Preventing severe accident progression by design basis (Confirm that core damage will not occur on single failure criteria)
Consideration for internal flooding (new)
Consideration for natural phenomena (volcanoes, tornadoes, and forest fires are newly added)
Consideration for natural phenomena
Consideration for fire
Consideration for fires
Enhanced/ newly implemented
Reliability of power source
Reliability of power source
Performance of other equipment
Performance of other equipment
Seismic/tsunami-resistant performance
Seismic/tsunami-resistant performance
Enhanced

Fig. 1. Previous and new regulatory requirements

Effectiveness evaluations of severe accident countermeasures

The measures to prevent core damage assuming beyond design-basis accidents are required. The assumed beyond design-basis accidents are as follows:

1) ATWS
2) Loss of reactor cooling function (at high pressure)
3) Loss of reactor depressurisation function
4) Loss of reactor cooling function (at low pressure)
5) Loss of UHS System
6) Loss of support function (makeup water, power supply)
7) Others identified by IPE and IPEEE

The measures to prevent containment failure after core damage are required as follows:

1) Cooling and depressurisation of CV, reduction of release of radioactive materials (e.g. CV spray)
2) Heat removal from CV and depressurisation of CV (e.g. filtered venting)
3) Cooling of molten core at the bottom of CV and inside RPV (e.g. water injection)
4) Prevention of DCH (e.g. depressurisation of RPV)
5) Prevention of hydrogen explosion inside CV (e.g. igniter)

Periodic safety assessment of continuous improvement

The Reactor Regulation Act requires the licensees to submit an updated safety assessment report on safety improvement to the NRA, at least every five years and to make it available to public. This system was introduced in new regulatory framework after Fukushima Daiichi accident, as Japanese periodic safety review. The first submission of this safety assessment report is set within six months after the date of completion of the licensees' periodic facility inspection based on the new regulatory requirements.

NRA published the regulatory guidance of the periodic safety assessment of continuous improvement, and PRA is conducted as one of the assessment. Licensees are required to conduct PRA covering internal events, seismic and tsunami PRAs for at-power and during plant shutdown condition.

Internal fire, internal flood, other external hazards, multi-hazard, spent fuel pool and multi-unit PRAs are covered in future depending on their maturity of methodology.

NRA is developing guidelines to confirm appropriateness of PRA submitted by licensees, as well as promoting researches on evaluation methods of PRA for new areas in addition to the areas previously developed such as internal events, shutdown stage, earthquakes and tsunamis.

1) Researches on PRA evaluation method
   - Internal fire PRA
   - Internal flood PRA
2) Guideline development for confirmation of appropriateness of PRA
   - Power operation PRA
   - Shutdown PRA

- Earthquake PRA
- Tsunami PRA
- Internal fire PRA
- Internal flooding PRA

Voluntary efforts and continuous improvement of nuclear safety

Japanese Electric Utilities give their full attention to nuclear risks honestly, by applying the risk information, strengthen their capability to cope with nuclear risks and improve nuclear safety continuously. NRRC assists such kind of continuous safety improvement efforts of Japanese Nuclear Industries by conducting R&Ds and applying R&D results.

3. SAFETY CRITERIA

Safety Goals

The former Nuclear Safety Commission did not make final decision on safety goals that is aimed to achieve through regulation. The NRA decided on the following position of Safety Goal in April 2013:

(i) The conclusion of Committee on Safety Goal under former Nuclear Safety Commission is a good basis for the NRA's discussion, which includes:
- Core damage frequency: approximately 10^{-4}/year
- Containment functional failure frequency: approximately 10^{-5}/year

(ii) The frequency of the release of Cs137 larger than 100 TBq during nuclear emergency should be less than once in one million years (excluding those due to security events).
(iii) Safety goals should be applied to all nuclear power plants equally.
(iv) Safety Goal is the goal that NRA should achieve through implementing its regulation over nuclear facilities.
(v) Plan to have further discussion on Safety Goal with a view to continue the enhancement of safety.

4. STATUS AND SCOPE OF ONGOING PRA STUDIES

Common elements among Level 1, Level2 and Level 3 PRA

✓ Main objectives of PRA development

One of the main objectives of PRA development is to prepare the knowledge of internal and external PRAs for reviewing "Periodic safety assessment of continuous improvement for NPP" which licensees are required to conduct.

Another main objective of PRA development is to support the safety regulation. For example, the NRA provided several accident sequence groups and containment vessel failure modes for which licensees shall conduct "effectiveness evaluations of countermeasures," and the NRA prepared these accident sequence groups and containment vessel failure modes using PRA information.

✓ Incorporation of countermeasures against severe accidents

The reactor regulation act requires the countermeasures for severe accidents, and the licensees have installed new equipment including the mobile equipment. The equipment is incorporated in the Level 1 and level 2 internal and seismic PRA models.

- ✓ Multi-unit PRA

  Using SECOM2-DQFM code developed by JAEA, assessments for two-unit site have been performed. Special features of SECOM2-DQFM can perform seismic PRA by directly quantifying combined FT using Monte Carlo sampling method, for either single unit or multi-unit, considering correlation of both seismic response and capacity among SSCs inside single unit or across multi-unit.

<u>Level1 PRA</u>

NRA has developed the methodology of level 1 PRA and PRA models, and NRA performed PRA for representative plants which are categorised into following 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 containment (4 loop PWR)
- 1100 MW class PWR with ice-condenser containment (4 loop PWR)

Appendix A shows the status of PRA development for each PRA models.

- ✓ Internal fire PRA

  Assessment flow and related technical elements of fire PRA including evaluation of severity factors, progression of accident scenarios and estimation of fire occurrence frequencies have been developed. In parallel, a methodology of the detailed fire modelling for single-compartment has been developed. Fire dynamic simulator (FDS) is used for the detailed fire modelling. Fire propagation analysis in the relevant compartments of actual plant size is started.

- ✓ Internal flood PRA

  Assessment flow and related technical elements of flood PRA including evaluation of flood progression of accident scenarios and estimation of flood occurrence frequencies have been developed.

  Flood propagation analyses using APROS® which is a computer code developed by VTT Technical Research Centre of Finland and Finnish energy company Fortum are started.

- ✓ Internal event PRA for SFPs

  The licensees are required to implement countermeasures against severe accidents for spent fuel pool/pit. The licensees are required to conduct assessment of safety enhancement of their NPPs periodically including plant-specific PRA reflecting the effectiveness of severe accident measures.

  NRA has developed the PRA methodology and PRA models with the countermeasures against severe accidents for the SFPs of PWR and BWR.

✓ Other external hazards PRAs

NRA is developing the methodology for other external hazards PRAs such as external flood, high wind, tornado, volcanoes and thunder.

Level 2 PRA

NRA has developed the methodology for level 2 PRA. MELCOR code is used to simulate and to accumulate knowledge for plant situations under severe accident progressing conditions. In addition to that, several dedicated codes and ROAAM application has been established to qualify behaviour of physical and chemical phenomena in the containment. Since the countermeasures against severe accidents have been installed in accordance with requirements of the Reactor Regulation Act, internal and seismic level2 PRA should be considered the effect of system unavailability for those countermeasures involving the mobile equipment.

JAEA has developed numerical codes applicable to level 2 PRA, including THALES2/KICHE code for analyses on severe accident progression and source term, and JASMINE code for those on fuel/coolant interactions and ex-vessel debris coolability relating to the evaluation of loads on containment vessels.

Level 3 PRA

NRA has developed the methodology for level 3 PRA, and MACCS-2 code is used to analyse the off-site radiological consequences for internal and seismic events at typical BWR and PWR plants in Japan.

JAEA has developed level 3 PRA code, OSCAAR, capable of analysing the environmental transportation of radionuclides, subsequent radiation exposure and health effects on the public, and economic impacts. The OSCAAR code has been applied to evaluating to the effectiveness of emergency preparedness and response.

State-of-practice PRA

In order to achieve continuous safety improvement by applying risk information, Japanese Electric Utilities chose KK-6/7 of TEPCO and Ikata-3 of Shikoku-Epco as pilot plants for improving PRA model to state-of-practice level. TEPCO and Shikoku-Epco are improving their PRA model and NRRC assists their activities.

5. PSA METHODOLOGY AND DATA

AESJ PRA standard

Japanese PRA standards are established by AESJ (Atomic Energy Society of Japan) and are revised every 5 years. As of today, established Japanese PRA standards are below;

✓ Level 1 PRA: At power state and internal event, Shutdown state and internal event, internal flooding, internal-fire, Seismic, Tsunami

✓ Level 2 PRA: At power state and internal event

✓ Level 3 PRA: At power state and internal event

✓ Ensuring Quality of PRA

Equipment Reliability Data by using NUCIA Database

By analysing NUCIA database which collects incident information of Japanese Nuclear Power plants, JANSI establishes Japanese general equipment reliability data. The latest version which includes 29years experiences of 56 plants in Japan was opened to the public in June, 2016.

Common Cause Failure Data

As with equipment reliability data, NUCIA database is analysed by CRIEPI for assessing parameters of common-cause failure. CRIEPI established CCF database, a guideline for analysing the incident and compiling examples.

6. NOTABLE RESULTS OF PRAs

No notable result can be shown in this moment.

7. PRA APPLICATIONS AND DECISION MAKING

Risk-informed inspection

An international team of senior nuclear and radiation safety experts suggests "increase NRA flexibility to provide for efficient, performance-based, less prescriptive and risk-informed regulation of nuclear and radiation safety" on the Integrated Regulatory Review Service (IRRS) mission from 11 to 22 January 2016. The development of PRA models for the risk-informed inspection has been accelerated.

Accident sequence precursor

NRA performs the accident sequence precursor to inform the technical information committee of NRA about the quantitative plant risk (conditional core damage probability) for screening events.

8. FUTURE DEVELOPMENTS AND RESEARCH

Dynamic PRA

NRA has planned to develop the dynamic PRA for better accuracy of core damage risks. The calculation of thermal hydraulics will be done by APROS®, and the calculation of physical and chemical phenomena in the severe accidents will be done by THALES-2 which is developed by JAEA. The dynamic event tree methodology will be developed as the first phase.

Seismically-induced fire and flood

NRA has planned to develop the seismically-induced fire PRA and seismically-induced flood PRA to confirm the residual seismic risks. The combination of the equipment damage from earthquake and fire or flood may be important to consider on the PRA.

9. INTERNATIONAL ACTIVITIES

Activities of NRA

To exchange the information of PRA, NRA has the information exchange meeting based on the bilateral co-operation with the US Nuclear Regulatory Commission (NRC). NRA also has the bilateral co-operation with the French Institute for Radiological Protection and Nuclear Safety (IRSN) to exchange the information about fire PRA as a part of fire projects.

Activities of industries

Japanese Electric Utilities and US Electric Utilities collaboratively exchange information about PRA and application of the risk information under the agreement between JANSI and INPO. Regarding collaboration with European Countries, Japanese BWROG and European BWR Club has information exchange meeting annually.

Besides these things, JANSI contributed to ASAMPSA_E project by providing information about the Fukushima accident and so on.

References

[1] "Act for Establishment of the Nuclear Regulation Authority," Act No. 47 of 27 June 2012.

[2] "Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors," Act No. 166 of 10 June 1957.

[3] International Atomic Energy Agency (IAEA), "Integrated Regulatory Review Service (IRRS) Mission to Japan," IAEA-NS-IRRS-2016, January 2016.

[4] Jari Lappalainen, et al., "Dynamic process simulation as an engineering tool – A case of analysing a coal plant evaporator," VGB Powertech Vol. 92, 2012

[5] Liu Q, et al., “User's manual of SECOM2-DQFM; A Computer code for seismic system reliability analysis,” JAEA-Data/Code 2008-004, Japan Atomic Energy Agency, March 2008.

[6] M.Kajimoto, et al,”Development of THALES2, A Computer code for Coupled Thermal-Hydranlics and Fission Product Transport Analysis for Severe Accident at LWRs and its Application to Analysis of Fission Product Revaporization Phenomena”,Proc.of Int.Mtg.on ANS Thermal Nuclear Reactors, Portlamd, 21-25 July 1991.

[7] Nuclear Regulation Authority, "Convention on Nuclear Safety National Report of Japan for 6th Review Meeting," August 2013.

[8] Nuclear Regulation Authority, "Enforcement of the New Regulatory Requirements for Commercial Nuclear Power Reactors," 8 July 2013.

[9] R.O. Gauntt, et al., “MELCOR Computer Code Manuals, Primer and User’s Guide, Version 1.8.5,” NUREG/CR-6119, US Nuclear Regulatory Commission, December 2000.

[10] Special Committee on Safety Goals, Nuclear Safety Commission, Japan, "Interim Report on Research and Deliberations on Safety Goals," 2003.

[11] Special Committee on Safety Goals, Nuclear Safety Commission, Japan, “Performance Goals for Nuclear Power Plants Equivalent to the Interim Safety Goals,” 2006.

[12] Toyoshi Fuketa, "How PSA Results are to be Utilized in New Nuclear Regulation in Japan," PSAM Topical Conference in Tokyo, 15 April 2013.

[13] The Secretariat of Nuclear Regulation Authority, "Outline of Nuclear Regulation of Japan - Reference documents for the IAEA IRRS Mission -," November 2015.

APPENDIX: Overview of the status of PRA programmes in Japan

PRA of NRA

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
500 MW class BWR	BWR-3	Level 1	Internal events, seismic event	At power and shutdown	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
800 MW class BWR	BWR-4	Level 1	Internal events, seismic event	At power and shutdown	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme, SDP
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
1100 MW class BWR	BWR-5	Level 1	Internal events, seismic event, tsunami event,	At power and shutdown	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme
			Internal events, SFP	At power	No	2015	Review of Periodic safety assessment of continuous improvement	ASP, SDP
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
1300 MW class BWR	ABWR	Level 1	Internal events, seismic event,	At power and shutdown	No	1992/2000,	Review of accident management in 2000,	ASP, Maintenance programme
			Internal events, seismic event , internal fire events, internal flood events	At power	No	2016 (under development)	Review of Periodic safety assessment of continuous improvement	ASP,SDP
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
			Internal events, seismic event	At power	No	2016 (under development)	Review of Periodic safety assessment of continuous improvement	Performance target

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
500 MW class PWR	2 loop PWR	Level 1	Internal events, seismic event	At power and shutdown	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme, SDP
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
800 MW class PWR	3 loop PWR	Level 1	Internal events, seismic event	At power and shutdown	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme
			Internal events, seismic event	At power	No	2016	Review of Periodic safety assessment of	ASP, SDP

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
						(under development)	continuous improvement	
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
			Internal events, seismic event	At power	No	2016 (under development)	Review of Periodic safety assessment of continuous improvement	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
1100 MW class PWR with large dry containment	4 loop PWR	Level 1	Internal events, seismic event, tsunami event,	At power and shutdown	No	1992/2000	Review of accident management in 2000,	ASP, Maintenance programme
			Internal events, seismic event, internal fire	At power	No	2016	Review of Periodic safety assessment of	ASP, SDP

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ revisions	Reason for PRA	PRA applications
			events, internal flood events, SFP			(under development)	continuous improvement	
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site
1100 MW class PWR with ice-condenser containment	4 loop PWR with ice-condenser containment	Level 1	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	ASP, Maintenance programme
		Level 2	Internal events, seismic event	At power	No	1992/2000	Review of accident management in 2000	Performance target
		Level 3	Internal events, Seismic event	At power	No	2005/2006,2013	Decision of a performance target,	Performance target, Risk evaluation outside the site

PRA of licensees

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Tomari Unit 1	PWR(2-Loop)-579MWe	L1,1.5*	Internal events seismic event, Tsunami events	At power and shutdown	Yes	2004/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Tomari Unit 2	PWR(2-Loop)-579MWe	L1,1.5*	Internal events seismic event, Tsunami events	At power and shutdown	Yes	2004/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Tomari Unit 3	PWR(3-Loop)-912MWe	L1,1.5*	Internal events seismic event, Tsunami events	At power and shutdown	Yes	2008/2013	Evaluate effectiveness of AM, Application for the new regulation	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Higashidori Unit1	BWR5-1100MWe	L1, L1.5*	Internal events, Seismic event, Tsunami events	At power and shutdown**	Yes	2003/2014	Evaluate effectiveness of AM Application for the new regulation	Design Review
Onagawa Unit1	BWR4-524MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	1994/2009	Evaluate effectiveness of AM PSR	Design Review
Onagawa Unit2	BWR5-825MWe	L1, L1.5*	Internal events, Seismic event, Tsunami events	At power and shutdown**	Yes	1994/2013	Evaluate effectiveness of AM PSR Application for the new regulation	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Onagawa Unit3	BWR5-825MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	1995/2012	Evaluate effectiveness of AM PSR	Design Review
Fukushima Daini Unit1	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2000/2008	PSR Evaluate effectiveness of AM	Design Review, Evaluate effectiveness of AM
Fukushima Daini Unit2	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2001/2008	PSR Evaluate effectiveness of AM	Design Review, Evaluate effectiveness of AM
Fukushima Daini Unit3	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2002/2010	PSR Evaluate effectiveness of AM	Design Review, Evaluate effectiveness of AM
Fukushima Daini Unit4	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2002/2010	PSR Evaluate effectiveness of AM	Design Review, Evaluate effectiveness of AM
Kashiwazaki-Kariwa Unit1	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2002/2012	PSR	Evaluate effectiveness of AM, Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Kashiwazaki-Kariwa Unit2	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2004/2006	Evaluate effectiveness of AM, PSR	Design Review
Kashiwazaki-Kariwa Unit3	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2004/2006	Evaluate effectiveness of AM, PSR	Design Review
Kashiwazaki-Kariwa Unit4	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2004/2006	Evaluate effectiveness of AM, PSR	Design Review
Kashiwazaki-Kariwa Unit5	BWR5-1100MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	2004/2006	Evaluate effectiveness of AM, PSR	Design Review
Kashiwazaki-Kariwa Unit6	ABWR-1356MWe	L1, L1.5*	Internal events, seismic event, Tsunami events	At power and shutdown	Yes	2002/2013	Evaluate effectiveness of AM, PSR,	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
							Application for the new regulation	
Kashiwazaki-Kariwa Unit7	ABWR-1356MWe	L1, L1.5*	Internal events, seismic event, Tsunami events	At power and shutdown	Yes	2004/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Hamaoka Unit3	BWR5-1100MWe	L1, L1.5*	Internal events, seismic events, Tsunami events	At power and shutdown**	Yes	2002/2015	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Hamaoka Unit4	BWR5-1137MWe	L1, L1.5*	Internal events, seismic events, Tsunami events	At power and shutdown**	Yes	2004/2015	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Hamaoka Unit5	ABWR-1380MWe	L1,L1.5*	Internal events	At power and shutdown	Yes	2003/2014	Evaluate effectiveness of AM, PSR	Design Review
Shika Unit1	BWR5-540MWe	L1, L1.5	Internal events	At power and shutdown	Yes	2004/2015	Evaluate effectiveness of AM, PSR,	Evaluate effectiveness of AM, Design Review
Shika Unit2	ABWR-1358MWe***	L1, L1.5*	Internal events, seismic events,	At power and shutdown**	Yes	2002/2015	Evaluate effectiveness of AM, PSR,	Evaluate effectiveness of AM, Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
			tsunami events				Application for the new regulation	
Mihama Unit3	PWR(3-Loop)-826MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2015	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Takahama Unit1	PWR(3-Loop)-826MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2015	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Takahama Unit2	PWR(3-Loop)-826MWe	L1, L1.5*	Internal-events, Seismic-events,	At power and shutdown	Yes	1994/2015	Evaluate effectiveness of AM, PSR,	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
			Tsunami-events				Application for the new regulation	
Takahama Unit3	PWR(3-Loop)-870MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Takahama Unit4	PWR(3-Loop)-870MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Ohi Unit1	PWR(4-Loop)-1175MWe	L1, L1.5	Internal events	At power and shutdown	Yes	1994/2008	Evaluate effectiveness of AM, PSR	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Ohi Unit2	PWR(4-Loop)-1175MWe	L1, L1.5	Internal events	At power and shutdown	Yes	1994/2008	Evaluate effectiveness of AM, PSR	Design Review
Ohi Unit3	PWR(4-Loop)-1180MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Ohi Unit4	PWR(4-Loop)-1180MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Shimane Unit2	BWR5-820MWe	L1, L1.5*	Internal events, seismic event,	At power and shutdown	Yes	1994/2014	Evaluate effectiveness of AM,	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
			Tsunami events				PSR, Application for the new regulation	
Shimane Unit3	ABWR-1373MWe	L1, L1.5*	Internal events	At power	under construction	2010	Evaluate effectiveness of AM	Design Review
Ikata Unit2	PWR(2-loop)-566MWe	L1, L1.5	Internal-events	At power and shutdown	Yes	1994/2011	Evaluate effectiveness of AM, PSR	Design Review
Ikata Unit3	PWR(3-loop)-890MWe	L1, L1.5*	Internal-events, Seismic-events, Tsunami-events	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Genkai Unit2	PWR(2-Loop)-559MWe	L1, L1.5*	Internal events	At power and shutdown	Yes	1994/2010	Evaluate effectiveness of AM, PSR	Design Review
Genkai Unit3	PWR(4-Loop)-1180MWe	L1, L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR,	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
							Application for the new regulation	
Genkai Unit4	PWR(4-Loop)-1180MWe	L1, L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Sendai Unit1	PWR(3-Loop)-890MWe	L1, L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review
Sendai Unit2	PWR(3-Loop)-890MWe	L1, L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2013	Evaluate effectiveness of AM, PSR, Application for the new regulation	Design Review

Plant Name	Plant type	PRA Scope				PRA usage		
		Level	Initiating events	Plant operating states	Living PRA	Date of original PRA/ latest revisions	Reason for PRA	PRA applications
Tokai Daini	BWR5-1100MWe	L1,L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2014	Evaluate effectiveness of AM, PSR, Application for the new regulation	Evaluate effectiveness of AM, Design Review
Tsuruga Unit 2	4loop PWR-1160MWe	L1,L1.5*	Internal events, Seismic , Tsunami	At power and shutdown	Yes	1994/2015	Evaluate effectiveness of AM, PSR, Application for the new regulation	Evaluate effectiveness of AM, Design Review
Ohma	ABWR-1383MWe	L1, L1.5*	Internal events, seismic event, Tsunami events	At power and shutdown	(Under Construction)	2014	Application for the new regulation	Design Review

* L1.5 PRA is performed only for internal events during power operation.

** Shutdown L1 PRA is performed only for internal events.

*** The current rated electric power outlet is 1206 MW due to installation of the turbine rectification board.

KOREA

1. INTRODUCTION

2. PSA FRAMEWORK AND ENVIRONMENT

As of the end of 2015, PSAs are performed in Korea based on administrative orders under the umbrella of the Severe Accident Policy promulgated by the Korean Nuclear Safety Commission in 2001. The Severe Accident Policy prescribes comprehensive measures against severe accidents including PSA implementation. The main objective of the policy is to assure that the possibility of severe accident occurrence is extremely low, and its risk to the public is sufficiently reduced. The Severe Accident Policy requires taking into account the following aspects:

1. Establishing performance goals to achieve the safety goals (Quantitative Health Objectives);
2. Implementing PSA for NPPs (Nuclear Power Plants);
3. Providing capability for preventing against severe accidents; providing mitigating features;
4. Establishing and implementing SAMP (Severe Accident Management Program).

After the Fukushima Daiichi accident in 2011, the Korean government became aware of an urgent need to establish a substantial regulatory framework for efficiently coping with severe accidents and effectively including PSA-based on the stipulated legislation. Hence, to reinforce the previous regulations, to establish rules to encompass Fukushima action items originally implemented by enforcement orders, and to reflect international efforts to enhance safety of NPPs after Fukushima Daiichi accident, rulemaking efforts were made to revise the current regulatory framework for severe accidents and the PSA.

In 2014, the enforcement ordinance and the enforcement regulations of the Nuclear Safety Act were amended to include PSA as one element in the PSR (Periodic Safety Review) which is performed every 10 years to review the safety of operating NPPs. The purpose of reviewing PSA as a factor of PSR is to confirm the validity of the existing PSA of the NPP, while considering changes of design, operating conditions, PSA methodologies and other technologies.

The Korean National Assembly made an amendment to the Nuclear Safety Act in 2015 to provide legal bases for regulatory control of severe accidents. The amendment of the Nuclear Safety Act requires that the applicant of an operating licence for an NPP shall submit an “Accident Management Program (AMP)” as a legal-binding information package that demonstrates the capacity to cope with a severe accident at the designated NPP in compliance with the regulatory requirements for severe accidents and the PSA stipulated in the NSSC (Nuclear Safety and Security Commission) rules. In addition, all operating licence holders shall submit the “Accident Management Program” within the time window of 3 years after the effective date of the amendment of the Nuclear Safety Act. The effective date of the amendment is 23 June 2016; the NSSC and the KINS (Korea Institute of Nuclear Safety) are developing a draft of the NSSC rules and regulatory standards/guidelines of the KINS for regulatory control of severe accidents and PSA. The amendment work related to NSSC rules and KINS regulatory standards/guidelines is scheduled to be completed before the effective date of the amendment of the Nuclear Safety Act. According to the draft of the NSSC rules and regulatory standards/guidelines of KINS, major changes for PSA are as follows:

1. Include the PSA results in chapter on estimation of accident management capability in "Accident Management Program" which will be submitted at the time of operating licence application;
2. Include the PSA results in chapter on estimation of accident management capability in "Preliminary Accident Management Program" which will be submitted at the time of construction permit application or standard design approval application;
3. Detailed criteria the PSA should meet;

- The scopes of PSA for "Accident Management Program" and "Preliminary Accident Management Program" are specified.
- PSA quality verification process (e.g. peer review) should be implemented with adequate PSA standard.
- PSA results shall satisfy the risk target values (prompt fatality risk (or equivalent performance goal), cancer fatality risk (or equivalent performance goal), frequency of Cs-137 release more than 100 TBq).
- PSA results should be utilised to enhance capability in prevention and mitigation of severe accidents.

4. Use the PSA results in selecting the accidents that shall be analysed via a deterministic approach. An accident evaluated as having a similar frequency and consequence compared to the accident list in the NSSC rules should be selected.

In Korea, PSAs have been carried out by several organisations, including the CRI (Central Research Institute) of the nuclear utility (the Korea Hydro and Nuclear Power Company; KHNP), KAERI (the Korea Atomic Energy Research Institute), and KEPCO E&C (previous KOPEC). Major activities have been focused on the development of PSA models and methods, the use of PSA in the design stage, and PSA applications to operational safety and performance improvement such as risk-informed approaches. The NSSC (governmental nuclear regulatory authority) and the KINS (technical supporting organisation) are responsible for regulatory reviews of NPPs.

3. SAFETY CRITERIA

As of the end of 2015, no quantitative safety criteria in designing plants have been officially used in Korea. However, the Severe Accident Policy promulgated in 2001 addresses the primary quantitative safety goals: "The risk to an average individual in the vicinity of a nuclear power plant of prompt fatality resulting from reactor accidents should not exceed 0.1% of the sum of prompt fatality risks resulting from all other accidents. The risk to the population in the area near a nuclear power plant of cancer fatalities resulting from nuclear power plant operation should not exceed 0.1% of the sum of cancer fatality risks resulting from all other causes." In order to practically implement the above safety goals for NPPs, KINS has been developing surrogate performance goals using risk metrics to prevent damage of the reactor core and to limit radioactive materials release through the containment. The performance goals have been studied by KINS with considerations of several aspects of applications, which include difference in design between PWR and CANDU plants, different safety level of existing and new plants, and so on.

As mentioned in the chapter on the PSA framework and environment, the NSSC and the KINS are developing a draft of the NSSC rules and regulatory standards/guidelines of KINS as a subsequent process for an amendment of the Nuclear Safety Act of 2015. The amendment of NSSC rules and KINS regulatory standards/guidelines is scheduled to be completed before 23 June 2016. According to the draft of the NSSC rules, the following two safety criteria are applied as risk target values the PSA should satisfy. The first criterion is adopted from the quantitative safety goals in the Severe Accident Policy.

The risk to an average individual in the vicinity of a nuclear power plant of prompt fatality resulting from a reactor accident should not exceed 0.1% of the sum of prompt fatality risks resulting from all other accidents. The risk to the population in the area near a nuclear power plant of cancer fatalities resulting from nuclear power plant operation should not exceed 0.1% of the sum of cancer fatality risks resulting from all other causes; or the equivalent performance goals for prompt fatality risk and caner fatality risk should be satisfied.

The sum of frequencies of the accident scenarios in which the amount of Cs-137 release exceeds 100 TBq should be less than 1.0E-06/ry.

The equivalent performance goals for prompt fatality risk and cancer fatality risk in the draft NSSC rules are defined in the draft KINS regulatory standards/guidelines as follows:

1. CDF (Core Damage Frequency) – performance goal equivalent to cancer fatality risk

- Less than 1.0E-04/ry for operating NPPs
- Less than 1.0E-05/ry for new NPPs (e.g. APR 1400 and follow-up designs)

2. LERF (Large Early Release Frequency) – performance goal equivalent to prompt fatality risk

- Less than 1.0E-05/ry for operating NPPs
- Less than 1.0E-06/ry for new NPPs (e.g. APR 1400 and follow-up designs)

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

PSAs of operating and new NPPS

In Korea, the PSAs for NPPs have been in the limelight due to the following incidents: 1) the TMI-2 accident (1979); 2) the Severe Accident Policy of Nuclear Power Plant (2001); and 3) the Fukushima accident (2011). The first PSA in Korea was performed for Kori unit 3&4 and Hanbit unit 3&4 in 1989 as a follow-up action after the TMI accident. Since then Level 1 and Level 2 PSAs during full-power operation for all operating plants were performed until 2007 based on the Severe Accident Policy. The PSA in Korea has been focused on CDF and LERF during full-power operation under the jurisdiction of the NRC (Nuclear Regulatory Commission), and thus considerations in the PSAs are limited to internal/external events mainly during full-power operation; internal events during LPSD (Low Power and ShutDown) operation were performed just for some plants on a trial basis until the Fukushima accident. The treated cases for external events during full-power operation were earthquake, internal flooding and fire. For some plants, SMA (Seismic Margin Assessment) was performed instead of earthquake PSA.

Recently, as one of the post-Fukushima follow-up activities, KHNP (the Korea Hydro and Nuclear Power Co.) revised the existing full-power and LPSD Level 1 and Level 2 PSA models to include internal and external events for all operating reactors; through this, discrepancies among PSA models for each plant were remedied. An additional outcome of this revision was the LPSD Level 2 PSA models for Shin-Kori units 1&2, which was the first quantitative model in Korea to develop LPSD SAMG (severe accident management guidance). In addition, based on the NUREG/CR-685, new full-power Level 1 & LERF fire PSAs for Shin-Kori units 1&2 were conducted as a pilot study. In the Table below, PSAs of operating NPPs in Korea are arranged.

Table 1. Currrent status of PSA for operating NPPs

Plant	Plant Type	Level-1 PSA				Level-2 PSA				Level-3 PSA				note
		Full Pow.		LPSD		Full Pow.		LPSD		Full Pow.		LPSD		
		In.	Ex.*	In.	Ex.	In.	Ex.	In.	Ex.	In.	Ex.	In.	Ex.	
Kori 1	WH PWR	O	O	O	X	O	O	X	X	X	X	X	X	SMA
Kori 2	WH PWR	O	O	O	X	O	O	X	X	X	X	X	X	SMA
Kori 3,4	WH PWR	O	O	O	X	O	O	X	X	X	X	X	X	
Shin-Kori 1,2	OPR1000	O	O	O	X	O	O	X	X	X	X	X	X	PSA before OL
Hanbit 1,2	WH PWR	O	O	O	X	O	O	X	X	X	X	X	X	
Hanbit 3,4	OPR1000 (Sys 80+)	O	O	O	X	O	O	X	X	X	X	X	X	
Hanbit 5,6	OPR1000	O	O	O	X	O	O	X	X	X	X	X	X	
Hanul 1,2	Framatome	O	O	O	X	O	O	X	X	X	X	X	X	SMA
Hanul 3,4	OPR1000	O	O	O	X	O	O	X	X	X	X	X	X	
Hanul 5,6	OPR1000	O	O	O	X	O	O	X	X	X	X	X	X	
Wolsong 1	CANDU	O	O	O	X	O	O	X	X	X	X	X	X	SMA
Wolsong 2,3,4	CANDU	O	O	O	X	O	O	X	X	X	X	X	X	
Shin-Wolsong 1,2	OPR1000	O	O	O	X	O	O	X	X	X	X	X	X	PSA before OL

(* External: internal fire and flooding, earthquake)

Regulatory reviews of the PSA results have been completed for the Shin-Kori units 3&4 (APR1400 reactor) OL (Operating Licence) application and the Shin-Kori units 5&6 CP (Construction Permit) and are ongoing for and Shin-Hanul units 1&2 OL applications. The scope of the OL application covers Level 1, 2, and 3 PSAs for full-power operation including internal and external events, and Level 1 and 2 PSAs for shutdown conditions. In addition, as a part of regulatory reviews of a PSR for operating NPPs, the adequacy and usage of the up-to-date PSA results are under review for several operating reactors.

Besides this, PSA for the BNPP (Barakah Nuclear Power Plant) which is under construction was performed also.

PSAs of future NPPs and other nuclear facilities

PSAs for future plants, such as the APR+ (the next-generation plant type) and the premium NPP (the next-next generation plant concept), were performed with the purpose of design improvement. For the JRTR (Jordan Research and Training Reactor) exported to Jordan, PSA was executed during the licensing process. Regarding the SMART (System-integrated Modular Advanced ReacTor), PSA was performed on the process of SDA (Standard Design Approval), and PSA for SMART-PPE (Pre-Project Engineering) is proceeding under co-operation with Saudi Aribia. For the SFR (Sodium-cooled Fast Reactor), PSA is being performed for SAR (Safety Analysis Report) chapter 19 and RI-D (Risk-informed Design). Recently, in addition to the above works, the necessity of PSAs on facilities for radioactive waste and pyro-processing, and for decommissioning is discussed.

Scope of ongoing PSA studies

Since the Fukushima Daiichi nuclear accident, Korea has been trying to reflect on lessons learnt from the accident and to apply those lessons to research projects. Relating to this, KAERI has been carrying out the government-sponsored R&D projects that aim at developing the following technologies.

1) Risk evaluation methodologies for extreme external events, whose scope covers (a) the development of a re-evaluation methodology of the floor response spectra and in-cabinet response spectra using a revised input ground motion response spectrum, (b) the development of multi-hazard risk assessment technology including earthquake and tsunami events as well as typhoons and heavy rain events, (c) an aircraft impact risk assessment considering the structural vibrations from an aircraft impact and external fire from an aircraft fuel explosion, (d) a risk assessment for other extreme site-specific natural hazards (such as strong winds and floods), and (e) a seismic risk assessment for seismic isolated nuclear power plants considering the ultimate capacity of the seismic isolators and interface piping system.
2) Integrated risk assessment technology for a multi-unit site, the scope of which covers (a) the development of a site risk assessment methodology and model, (b) the development of a KSRP (Korean Site Risk Profile), based on all-mode, all-hazard Level 1/2/3 PSAs including extreme risk factors, (c) the establishment of a domestic-specific Level 3 PSA infrastructure, and (d) the upgrade and development of computational programmes for a multi-unit risk assessment in the field of logic tree generation and the quantification of logic trees. The basic concept for the development of a site risk assessment methodology is to treat the site as a single nuclear power generation system with multiple units. Each unit may have unit-specific initiating events that are independent of other units and dependent on initiating events, which mean that multiple units can experience simultaneous initiating events owing to an external hazard or other causes. The dependencies among the units at the site are then considered by means of common SSC (System, Structure and Component) modelling and CCF (Common Cause Failure) in the initiating event and SSC failures. Within this basic concept, a logic tree is constructed in the form of an ET (Event Tree) and FT (Fault Tree). Since the logic tree is quite huge, and a simplification method for the quantification, such as a rare event approximation, is not applicable, a quantification of the occurrence frequency is obtained through Monte Carlo sampling. As one of the case studies, we performed multi-unit risk (frequency) quantification for multiple LOOPs (Losses Of Offsite Power). All mode and scope PSA models are required to quantify the site risk (site risk profile). In this sense, all internal/external event PSA models

are under development. In addition, a Korean specific Level 3 PSA data base is being constructed to quantify the consequence/risk for each accident scenario. Finally, several computational programmes to help construct the site risk models have been upgraded. More specifically, the AIMS-PSA code, which was developed at KAERI, is being upgraded to enhance the computational speed and handle large sized logical models (ET/FT). In addition, the first version of the FTeMC (Fault Tree top event probability evaluation using Monte Carlo simulation) code was developed to apply Monte Carlo sampling to the accident sequence logic models; this version is currently being improved.

3) Advanced technologies for site-level AM (Accident Management) and EP (Emergency Preparedness) whose scope covers the development of (a) integrated AM technology and relevant technical base to cope with site-specific extreme external hazards/events, (b) risk-informed EP technology to secure effective EP countermeasures and assess the risk-relevance of typical EALs (emergency action levels) and EPAs (emergency protective actions) such as evacuation and sheltering, and (c) plant-level SFP (Spent Fuel Pool) risk and accident management technologies.
4) Advanced risk assessment technologies for risk-informed applications and a digital system environment whose objective is to secure key technologies that are able to contribute to an enhancement of risk-informed applications as well as to a reduction of risk uncertainty under a digital I&C environment by resolving several urgent issues; these technologies include (a) a high-precision FT calculation S/W (e.g. FTREX upgrade version), (b) a digital system PSA (e.g. one that can take into account software reliability that is one of the significant issues in the DI&C system), and (c) an HRA (human reliability analysis) handbook covering data collection guidelines and an associated qualitative/quantitative database.

In addition to the aforementioned R&D projects, KAERI has a plan to develop a Korea-specific Level 3 PSA code through a government-sponsored mid- and long-term project. As a preliminary step, main framework, specifications and key factors for the Level 3 PSA code have been drawn up through an assessment of the current state of the art of Level 3 PSA technology, a basic structure of the computer programs to integrate relevant models such as source terms, atmospheric dispersion and deposition, exposure pathways, dose estimation, and health effects, etc.). Based on these results, a technical roadmap and development strategy are under development. Development of Level 3 PSA code will be launched in 2017 as a part of the national research projects.

Besides this, for the purpose of supporting KINS, KAERI is also developing a regulatory Level 1 APR1400 risk model for risk-informed regulation (RIR). Its sub-goals are 1) to develop a highly effective regulatory risk model that reflects the design and operating experiences of domestic nuclear power plants and through this model to establish a base framework for risk-informed regulation of the nuclear power plants in operation; and 2) to develop regulatory software that enables the regulatory body to perform the overall safety assessment and significance determination process for the purpose of risk-informed regulation suitable for domestic circumstances.

5. PSA METHODOLOGY AND DATA

PSA standards and guidance

Regulatory standards and guidelines for regulatory review of PSA level-1, level-2 and level-3, and risk-informed applications were issued by KINS in 2010. Since then, the standards and guidelines have been revised to reflect the changes in the domestic and international environment. As of June 2016, the KINS regulatory standards and guidelines on PSA are in an update to reflect the amendment of the Nuclear Safety Act and the subsequent amendment of the NSSC rules. Major updates are as follows;

1. Scope of PSA
2. PSA quality validation process (e.g. peer review) with appropriate standards
3. Risk target values
4. Utilisation of PSA results

PSA validation

Generally, in Korea, the quality of PSA is validated through regulatory review. Recently, however, peer review is required for regulatory review. The first peer review for PSA results was requested through the regulatory review process for the operating licence application of Shin-Kori units 3 and 4. The peer review results and how the utility addressed the F&Os (Facts and Observations) were also reviewed by the regulatory body. The quality validation processes through the peer review has been requested by the regulatory body for subsequent operating licence applications after Shin-Kori units 3 and 4.

PSA data

Within a PSA framework, data analysis is an essential component in evaluating CDF and LERF. In Korea, earlier, generic data came from the EPRI (Electric Power Research Institute) URD (Utility Requirements Document); recently data have come from NUREG/CR-6928 and are developed by collecting operational experience data of numerous reference nuclear power plants. Plant-specific data are developed by collecting operational and maintenance experience data of pertinent nuclear power plants. The reliability data utilised in the PSA include equipment failure data, test and maintenance unavailability data, common-cause failure data, human error probability data, initiating event frequency data, and special event data.

Korea has only a single operating company, and plant-specific data can be as coming from periods before and after the ERP DREAMS (Enterprise Resource Planning Digital Real-time Enterprise Asset Management System) establishment. First, before implementation the ERP DREAMS, Korea made use of work requests, senior reactor operator logs, shift logs, regular surveillance tests, equipment maintenance reports, work orders, unexpected plant trip reports, and PUMAS (Power Unit Maintenance System) data. Among these many sorts of data, the source of major data recorded the full particulars of equipment failure, tests and maintenance for a work request; the significance of these data was that they made it possible to check the information about the relevant control equipment for work duration, failure mode categorisation, and failure/maintenance impact assessment. After completing the ERP DREAMS setup, KHNP developed the PRinS (Plant Reliability Data Information System), which is a systematic data managing system for convenience and reliability improvements of plant-specific information management at nuclear power plants. Since July 2003, this system has been managing and storing plant-specific failure and maintenance data. Therefore, information like the aforementioned work requests can be seen by means of the Notification and Work Order of the ERP DREAMS, whose purposes are to notify operators of failures and malfunctions in terms of time, equipment, and so on, and to describe man hours, work duration, necessary materials, procurement, etc. Senior reactor operator logs and shift logs are accessible through the ERP DREAMS as well. Therefore, with the establishment of ERP DREAMS, the system can sort, analyse, and produce all plant-specific data in accordance with the procedures (KHNP PSA procedure) through the plant reliability DB system.

Reflecting recent equipment reliability data for the PSA models, KHNP has Bayesian-synthesised and applied plant-specific and generic databases to the PSA models. The equipment database usually has a tendency to have very low values. In cases of collecting only plant-specific data, the equipment failure frequency becomes even lower. Accordingly, the equipment failure data calculated using low failure frequency has, statistically, a high level of uncertainty. Therefore, in order to analyse the equipment failure data, information on equipment failure is integrated and analysed for all units of the 16 domestic PWR plants; then the plant-specific and generic data of domestic PWR plants are statistically combined through a Bayesian method, after which they are developed and utilised. In the evaluation of up-to-date PSA reliability data, NUREG/CR-6928 has been used as a representative source of generic data. This data makes use of Beta and Gamma distributions for demand failure and running failure probabilities respectively.

Unavailability due to test and maintenance might lead to different values depending on the characteristics of each nuclear plant, that is to say, data can depend on the ways of testing and maintaining the plant and who the engineers are. The latest local unavailability assessment has gathered, analysed, and applied only the generic operational experience of corresponding plants.

On the other hand, domestic CCF data have recently used the ALWR (Advanced Light Water Reactor) URD and NUREG/CR-5497 data as generic data; however, these data are quite conservative compared to the operational experience of the current local and overseas plants because they reflect the long-term operational experience of US plants. The US has been achieving about 90% availability since 2000. Data from Korea and the US, CCF data of relatively recent plants, from the NUREG/CR-5497 (revised in 2007), are being used as generic data. Thus, KHNP applied the CCF population parameter by discerning between the Alpha Factor Model provided in the NUREG/CR-5497 and results from sequential and non-sequential tests under implementation for each domestic plant.

It is common that both HRA method developers and HRA practitioners need various kinds of HRA data that are helpful for not only understanding the contexts of erroneous behaviours but also for quantifying their likelihood or for quantifying the HEP (Human Error Probability). In this regard, a full-scope simulator has been regarded an important source for collecting HRA data because such a simulator can be used to recognise the effects of task contexts on associated HEPs for diverse off-normal conditions. Accordingly, several frameworks that specify how to extract HRA data from full-scope simulators have been developed. For these reasons, in Korea, KAERI tries to cope with the above-mentioned issues through the development of a framework with the associated promising solutions; and the validity of the proposed framework has been investigated. As a result, a total of 37 preliminary HEPs have been successfully quantified for 21 task types. It is expected that the proposed framework will be a good starting point to enhance the quality of HRA results by providing a firm basis for collecting HRA data from simulation records.

In case of initial events, the plant-specific frequency of initial events in the Transient has been developed and applied by investigating the trip records collected over the last 20 years for the 20 local plants in operation. In case of a LOCA (Loss-of-Coolant Accident), the source NUREG/CR-6928, which is the newest generic data has been utilised.

Lastly, the special event data are regarded as data on basic events in the process of developing event trees; these data cannot be derived from the equipment failure database. Domestically, an adequate source of data is utilised and reflected in the PSA models for eight basic events including the probability of a reactor RCP seal failure.

Korea is endeavouring to improve the integrity of its reliability testing and the objectiveness of the latest reliability database that has been applied for the purpose of updating and developing PSA models for nuclear power plants, both those under construction and those in operation. The development of a plant-specific data has been completed, and its availability is under discussion with the regulatory body.

6. NOTABLE RESULTS OF PSA

As mentioned in Ch.4, KHNP carried out the LPSD PSA project from January 2013 to December 2015. Through the project, for the NPPs operating in Korea, the Level 1 internal PSA models were upgraded based on the ASME PRA Standard, and also seismic/flooding PSA models and Level 2 PSA models for full-power operations were updated. For fire PSA, the new methodology of NUREG/CR-6850 was first applied to a pilot plant. KHNP has also developed LPSD Level 1 PSA models based on NUREG-6144. To support the development of plant-specific LPSD SAMGs, which was drawn up as one of the post-Fukushima accident near-term action items, LPSD Level 2 PSA models were also developed to a pilot plant. To obtain a technical adequacy for internal Level 1 PSA, KHNP included the major results of the peer review, which was carried out in the previous projects, and standardised CCF/HRA methodologies, which have been being considered as the most influential factors to measure the plant risk. For the scope of LPSD PSA, KHNP has developed Level 1 PSA models for Westinghouse, Framatome and CANDU-type reactors, and upgraded the models for OPR1000-type reactors, based on standard outage maintenance practices and Plant Operational Status (POS). LPSD Level 2 PSA models have also been developed for two types of pilot plants, one for PWR and another for PHWR (Pressurised Heavy Water Reactor).

Westinghouse-type reactors

KHNP has been operating six units of Westinghouse-type reactors and two units of Framatome-type reactors. For the first two Westinghouse-type reactors, the CDFs were estimated as being relative high, and showed slightly different trend from those of the other four Westinghouse-type reactors. However, the two Framatome-type reactors with capacity of about 950MWt have CDFs similar to those of the four Westinghouse-type reactors. Fig. 1 shows the CDF distributions of each PSA scope, except for fire PSA, for the six units (three plants). The results of seismic PSA on full-power operation were found to be up to two times higher than those of the internal PSA; CDFs of the flooding PSA were estimated to be lower than any of the others. According to Fig.1, while the CDF results of LPSD PSA are lower than those of the PSA on full-power operations, however, the CDFs of the LPSD internal PSA were estimated as being quite high. The difference in terms of 'level of details' between the PSA models of full-power operation and the LPSD PSA models is regarded as the main reason, which led the relatively high CDFs for LPSD operations.

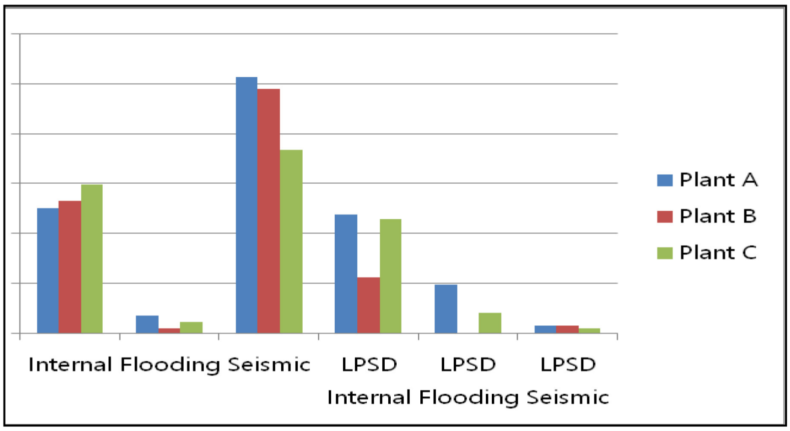


Fig. 1. Risk (CDF) profiles of Westinghouse- and Framatome-type reactors

OPR1000-type reactors

KHNP has been operating 12 units of OPR1000-type reactors, which have a capacity of 1 000 MWt. The first two units of OPR1000-type reactors were designed based on the System 80+ reactor of Combustion Engineering and the other ten units have been continuously modified and improved separately, especially for the auxiliary feed water system, the component cooling water system, and the digital instrument and control (DI&C) systems. Fig. 2 shows the CDF distributions of each PSA scope except for fire PSA for the 12 units. According to Fig.2, while the overall risks (CDFs) were estimated as being much lower than those of the Westinghouse-type reactors, they were similar to those of the Westinghouse-type reactors.

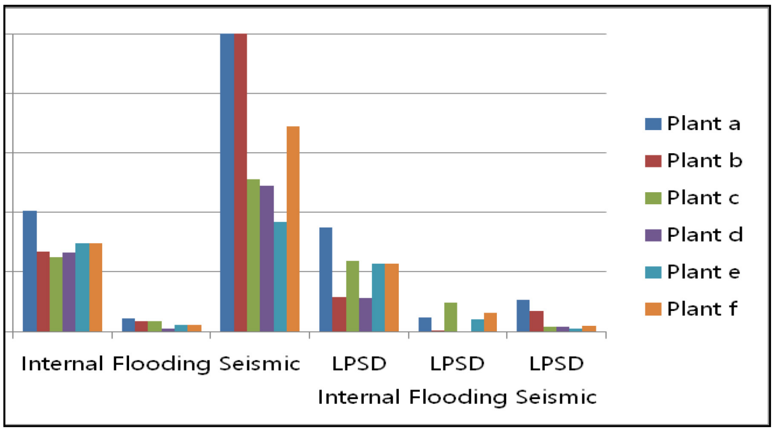


Fig. 2. Risk (CDF) profiles of OPR1000-type reactors

CANDU-type reactors

KHNP has been operating four units of CANDU-type reactors, which have a capacity of 700 MWt. CANDU PSA was performed based on Generic CANDU PSA – Reference Analysis in the mid-2000s. However, we performed CANDU specific FMEAs (Failure Mode and Effect Analysis) for initiating event analysis and accident sequence analysis based on T/H analysis, and so forth. The first unit of CANDU-type reactors obtained permission for a 10-year life extension in 2015. While the first unit was reactor of older design, it showed lower measures of risk because it had many design changes for life extension, including post-Fukushima actions such as the addition of PAR (Passive Autocatalytic Re-combiner), and a CFVS (containment filter ventilation system) were reflected in them. Fig. 3 shows the CDF distributions of each PSA scope, except for fire PSA, for the four units. As for the first unit, the results of seismic PSA are not shown in Fig. 3 because the first unit performed SMA.

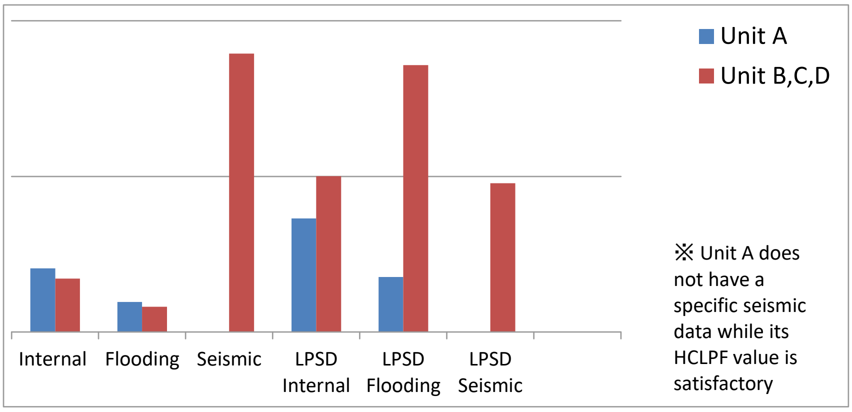


Fig. 3. Risk (CDF) profiles of CANDU-type reactors

According to Fig.2, CDFs during LPSD operations were estimated as being higher than those estimated during full-power operations.

Sensitivity studies reflecting post-Fukushima actions

After the Fukushima Daiichi accident, KHNP conducted various sensitivity analyses by reflecting the three following action items: 1) external cooling water injection to the primary flow line; 2) CFVS; and 3) power supply restoration by a movable generator truck. Table 2 shows the sensitivity study results.

Table 2. Currrent status of PSA for operating NPPs

Post-Fukushima Action Items		1. Considering Power Source Restoration Using Movable DG		2. Considering Primary External Injection Flow line	3. Considering CFVS	
Scope of Evaluation		Level 1 Internal Event CDF	LPSD Level 1 Internal Event CDF	LPSD Level 1 Internal Event CDF	Level 2 Internal Event LERF	Level 2 Internal Event CFF
Change Rate of Risk Each Unit (%)	Plant 01	-1.5		-4.5	0	-1.3
	Plant 02	-2.3		-2.7	0	-0.5
	Plant 03	-8.2		-5.4	0	-28.7
	Plant 04	-7.6		-9.7	0	-31.5
	Plant 05	-14.7		-5.7	0	-76.3
	Plant 06	-27.2		-15.8	0	-60.7
	Plant 07	-26.6		-2.0	0	-10.9
	Plant 08	-20.9		-10.0	0	-34.5
	Plant 09	-21.1		-11.1	-13.0	-38.3
	Plant 10	-33.2		-15.8	0	-58.7
	Plant 11	-33.2		-15.8	0	-58.7
	Plant 12	0.0	-54.4	-16.0	Already reflected in the base model	
	Plant 13	0.0	-37.7	-17.3	0.0	-52.5

According to Table 2, CDFs from seismic PSA were estimated as being relatively higher than those of other scopes. RCP seal integrity was identified as the weakest points of the Westinghouse-type reactors. As for OPR1000-type reactors, an improvement of containment integrity was made by installing severe accident mitigation systems, and for the CANDU-type reactors safety improvements during LPSD operations are required. Recently, KHNP has been using the PSA models when performing PSR projects and subsequently plans to update these models according to the schedules of PSR. In addition, the Level 2 PSA models, the external event PSA, and the LPSD PSA models will be continuously updated by considering regulatory requirements.

7. PSA APPLICATIONS AND DECISION MAKING

Extension of inspection periods for RPS/ESFAS

KHNP submitted a Topical Report (TR) that was approved by the regulatory body in June, 2011. The TR includes example applications and optimal methodologies to support risk-informed regulatory decision making such as RI-STI (Risk-Informed Surveillance Test Interval).

During the implementing of risk-informed decision-making process, changes in LB (Licensing Basis) are expected to meet a set of key principles as follows;

1. Principle 1: The proposed change meets the current regulations unless it is explicitly related to the request;

2. Principle 2: The proposed change is consistent with a defence-in-depth philosophy;
3. Principle 3: The proposed change maintains sufficient safety margins;
4. Principle 4: When proposed changes result in an increase in CDF or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement;
5. Principle 5: The impact of the proposed change should be monitored using performance measurement strategies.

The principles mentioned above have been applied to the OPR1000 safety-related I&C system for the STI changes below.

1. CPC (Core Protection System) channel function test (change from 1 month to 3 months)
2. RPS (Reactor Protection System) channel function test (change from 1 month to 3 months)
3. RPS logic and trip operation system (change from 1 month to 3 months, but no change in manual operation test at 1 month)
4. ESFAS (Engineered Safety Feature Actuation System) channel function test (change from 1 month to 3 months)
5. ESFAS logic and trip operation system (change from 1 month to 3 months)
6. ESF slave relay test (change from 1 month to 3 months on the basis of staggered tests)

KHNP has applied interval extension of RPS/ESFAS inspection to the types of OPR1000 (Hanbit units 3, 4, 5 and 6; Hanul units 3 and 4).

Development and pilot application of loss of voltage monitoring system

The importance of off-site power sources and on-site electric power systems is growing since an actual occurrence of station blackout at one NPP in Korea in 2011. While there has been little concern to date about the possibility of power failure due to duplicated off-site power grids and the diversity of on-site electric power systems, however, the event in question led to the building of in-depth countermeasures to prevent any failure that may cause an LOV (Loss of Voltage).

After the foregoing event, KHNP figured out causes of LOOP (Loss Of Off-site Power) through fragility analysis of off-site supply systems. Moreover, a prevention monitoring system on off-site power source has been created to check the status of maintenance progress in accordance with the status of main circuit breakers, switchyards of plants, and electric systems. By using this monitoring system, more up to work management and human error prevention could be achieved during outages.

Currently, Korean regulatory body is also reinforcing electric systems-relevant regulations because the number of case of LOV is increasing during outages. Furthermore, many efforts are being made to protect plants against LOOP by establishing and carrying out maintenance methods for checking and preventing its related situations. However, there has been no programme to prevent LOOP through some sort of systematic and well-programmed work management. Particularly, it was difficult to manage and control the work conditions for the equipment that causes LOV since there is no systematical means, which can provide warnings and cautions when the work order is allowed during outages.

There have been risks that equipment could malfunction due to equipment failure; this would result in missing line-up objects or incorrect operation in the form of human errors by maintenance workers who are not knowledgeable about the relevant facilities such that they do not have sufficient data on changes for each system operation mode. Furthermore, it is not easy to recognise the risks, in advance, that can occur due to changes of work times of work orders for main equipment pertaining to off-site power supply when it comes to designing work orders. As was mentioned earlier, cases of LOOP are divided into two groups, one that is influenced from the outside and the other that comes from inside the plant site. The problem is that KHNP may not be able to prevent failures that stem from outside the plants. Therefore, KHNP came to the conclusion that the occurrence of LOOP can be markedly reduced once failures and human errors can be prevented.

By reviewing plant design data such as LOOP experiencing systems and floor plans, as explained above, through failure mode effect and fault tree analyses were accomplished regarding the total of eight system units that can lead to LOV. As a part of the fault tree models discussed during the analysis, Fig. 4 represents combinations of possible failure in which bus circuit breakers not opened.

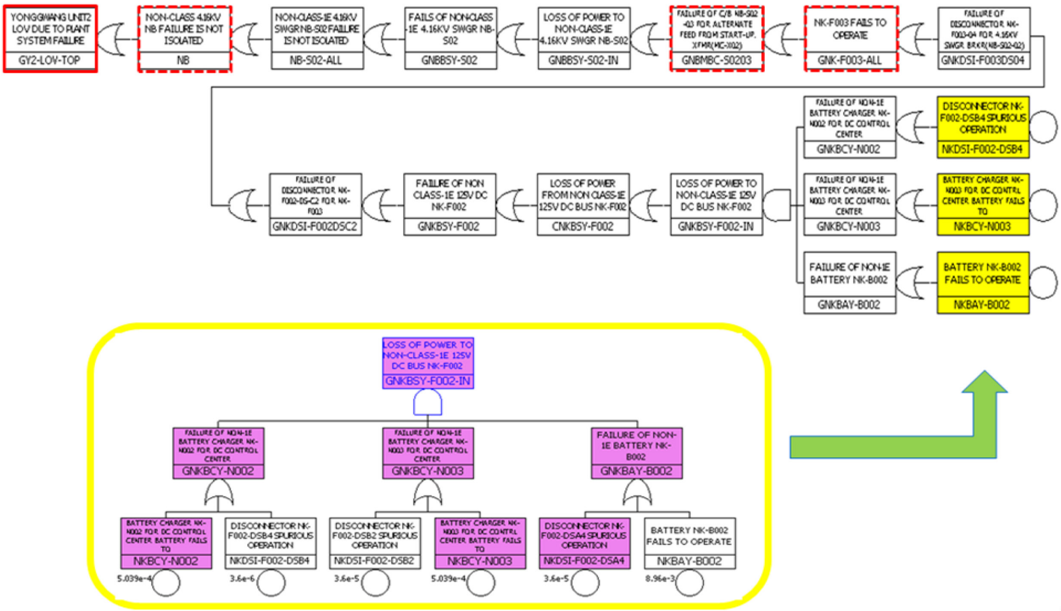

YONGGWANG UNIT2 LOV DUE TO PLANT SYSTEM FAILURE
GY2-LOV-TOP
NON-CLASS 4.16KV NB FAILURE IS NOT ISOLATED
NB
NON-CLASS-1E 4.16KV SWGR NB-S02 FAILURE IS NOT ISOLATED
NB-S02-ALL
FAILS OF NON-CLASS-1E 4.16KV SWGR NB-S02
GNBBSY-S02
LOSS OF POWER TO NON-CLASS-1E 4.16KV SWGR NB-S02
GNBBSY-S02-IN
FAILURE OF C/B NB-S02-03 FOR ALTERNATE FEED FROM START-UP. XFMR(MC-X02)
GNBMBC-S0203
NK-F003 FAILS TO OPERATE
GNK-F003-ALL
FAILURE OF DISCONNECTOR NK-F003-04 FOR 4.16KV SWGR BRKR(NB-S02-02)
GNKDSI-F003DS04
FAILURE OF DISCONNECTOR NK-F002-DS-C2 FOR NK-F003
GNKDSI-F002DSC2
FAILURE OF NON CLASS-1E 125V DC NK-F002
GNKBSY-F002
LOSS OF POWER FROM NON CLASS-1E 125V DC BUS NK-F002
CNKBSY-F002
LOSS OF POWER TO NON-CLASS-1E 125V DC BUS NK-F002
GNKBSY-F002-IN
FAILURE OF NON-1E BATTERY CHARGER NK-N002 FOR DC CONTROL CENTER
GNKBCY-N002
DISCONNECTOR NK-F002-DSB4 SPURIOUS OPERATION
NKDSI-F002-DSB4
FAILURE OF NON-1E BATTERY CHARGER NK-N003 FOR DC CONTROL CENTER
GNKBCY-N003
BATTERY CHARGER NK-N003 FOR DC CONTRL CENTER BATTERY FAILS TO
NKBCY-N003
FAILURE OF NON-1E BATTERY NK-B002
GNKBAY-B002
BATTERY NK-B002 FAILS TO OPERATE
NKBAY-B002
LOSS OF POWER TO NON-CLASS-1E 125V DC BUS NK-F002
GNKBSY-F002-IN
FAILURE OF NON-1E BATTERY CHARGER NK-N002 FOR DC CONTROL CENTER
GNKBCY-N002
FAILURE OF NON-1E BATTERY CHARGER NK-N003 FOR DC CONTROL CENTER
GNKBCY-N003
FAILURE OF NON-1E BATTERY NK-B002
GNKBAY-B002
BATTERY CHARGER NK-N002 FOR DC CONTROL CENTER BATTERY FAILS TO
NKBCY-N002
5.039e-4
DISCONNECTOR NK-F002-DSB4 SPURIOUS OPERATION
NKDSI-F002-DSB4
3.6e-6
DISCONNECTOR NK-F002-DSB2 SPURIOUS OPERATION
NKDSI-F002-DSB2
3.6e-5
BATTERY CHARGER NK-N003 FOR DC CONTRL CENTER BATTERY FAILS TO
NKBCY-N003
5.039e-4
DISCONNECTOR NK-F002-DSA4 SPURIOUS OPERATION
NKDSI-F002-DSA4
3.6e-5
BATTERY NK-B002 FAILS TO OPERATE
NKBAY-B002
8.96e-3

Fig. 4. Failure combinations when bus circuit breakers not opened

LOV inducing and associated equipment, which identified through the analysis, shall be registered in the preventive maintenance database as target equipment needed for preventive maintenance improvement and concentrated management during outages. In addition, a surveillance programme has been developed to prevent LOOP by confirming the combinations of work and facility failures and the risk that operators might trigger LOOP when implementing multiple maintenance duties or maintenance and tests simultaneously for target facilities. This programme is regarded as an integrated piece of online monitoring software, associated with the maintenance orders database including the plant information system and outage order.

Risk-informed integrated leak rate test

The ILRT (Integrated Leak Rate Test) interval extension of two plant sites in Korea, Hanbit 5 and 6 along with Hanul 5 and 6, was approved in the respective orders of October 2011 and August 2012. On completion of over two ILRT performance outcomes in operation and a PSA for ILRT interval extension, the safety assessment was performed for the ILRT interval extension of Hanul units 5 and 6, to satisfy the notification requirements of the Ministry of Education, Science, and Technology; the feasibility of the interval extension was verified based on these results.

For this, after analysing the two methodologies of NUREG-1493 “capacity-based containment building leak test program” conducted by NRC and of NEI Interim Report “Interim Guidance for Performing Risk Impact Assessments In Support of One-Time Extensions for Containment ILRT Surveillance Intervals”, the relevant methodologies were applied to Hanul units 5 and 6 to evaluate the risk impact caused by the extension of the implementation interval of the ILRT. Off-site consequence analysis was carried out by making use of the computation code MACCS (MELCOR Accident Consequence Code System), which is generally used to calculate radiation exposure dose. KHNP has identified and evaluated the radiation source terms of the Hanul 5 and 6 PSAs; these data were released in June 2006 as input material for the MACCS 2 code; data on the population spread in 2009 within a 80 km radius of the plants, and the meteorological data measured at the weather stations near the Hanul plant sites from 2006 to 2010 were included. The population dose was selected and considered as a factor to measure the risk impact due to the ILRT interval extension. The results were compared after applying the risk impact measuring factors derived as a result of the off-site consequence analysis with the risk assessment evaluation methods of NUREG-1493 and the NEI Interim Guidance and evaluating the risk impacts. Because of the uncertainty reduction of the analysis results and the ILRT interval extension, and to provide diverse risk information, different sensitivity analyses were implemented in the fields of off-site consequence analysis and risk assessment.

In conclusion, it is seen that the safety of nuclear power plants is still assured after the interval extension of the ILRT; this shall be utilised as a useful finding for sustaining risk management and surveillance in the future.

Maintenance Rule

Many utilities apply PSA results to the field of the MR (Maintenance Rule). The MR programme was launched at the US NRC in 1991. The MR has been applied domestically to all operating plants since the NSSC held in December 2002 recommended the fulfilments of the MR.

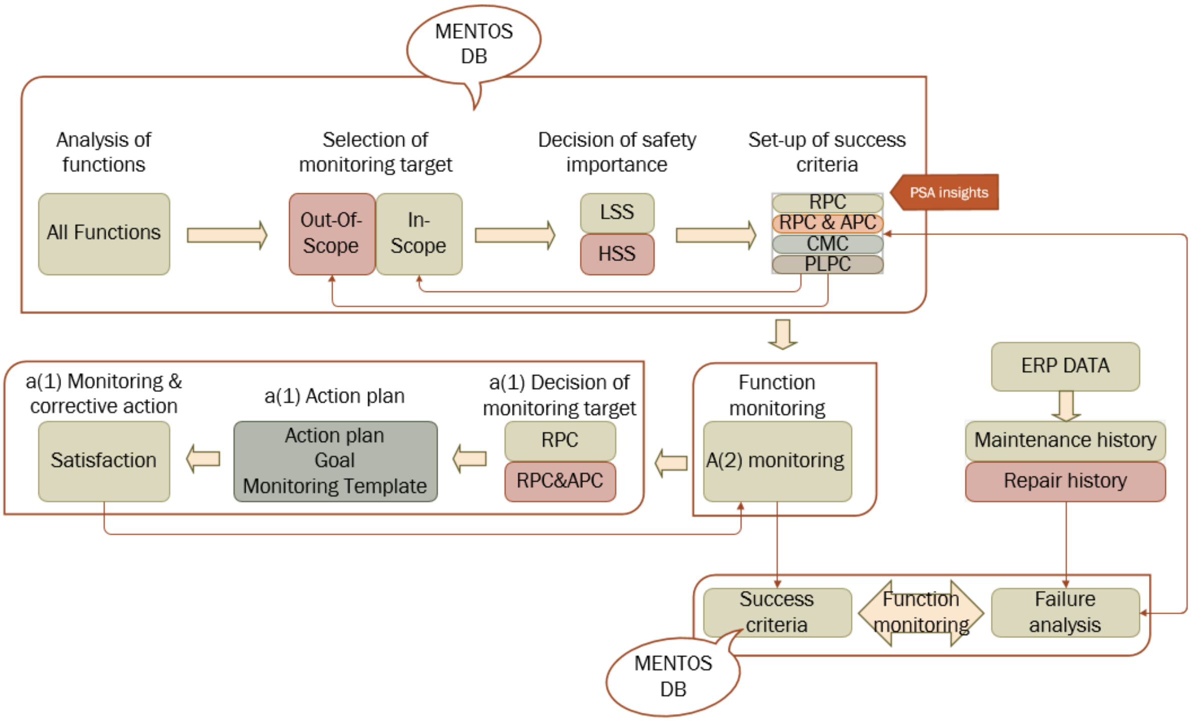


Fig. 5 Process of MR programme for development and implementation

The MR is a programme for monitoring the maintenance effectiveness and to ensure that SSCs are capable of fulfilling their intended functions, which are related to safety-related SSCs and those BOP SSCs whose failures could most directly threaten public health and safety.

The development of the MR programme is composed of three steps. The first step is to determine which SSCs are within the scope of the MR programme by applying the screening criteria. The second is to determine the safety significance of each in-scope function; the last step is to set performance criteria according to the results of safety significance determination. After developing the MR programme, the plants perform SSC monitoring regularly according to the performance criteria of the MR.

In November 2008 and July 2009, Hanul units 2 and Kori unit 2 were inspected by the regulatory body for pilot-implementation of the MR programme. Afterwards, maintenance effectiveness monitoring programmes in all nuclear power plants have been continuously developed and applied. The power plants have been performing periodic evaluation; however, if necessary, they have reestablished the RPC (Reliability Performance Criteria) and APC (Availability Performance Criteria).

Development and implementation of single point vulnerability monitor

PSA results have been applied to SPV (Single Point Vulnerability). The SPV is a single component whose failure will lead to an immediate automatic or manual reactor or turbine trip.

KHNP has been carrying out SPV analysis performed by FMEA with replaceable and repairable components. The analysis is done to determine component failure effects for systems and plant normal operation. Fault tree analysis makes it possible to consider particular component failure effects with the logical model. Since the design characteristic is that this system can be quantified with system reliability data associated with the fault tree, the analysis can show methods for design improvement.

KHNP has been applying system reliability improvement processes for SPV management. Those processes are PM (Preventive Maintenance), System Improvement (Redundancy) and PdM (Predictive Maintenance).

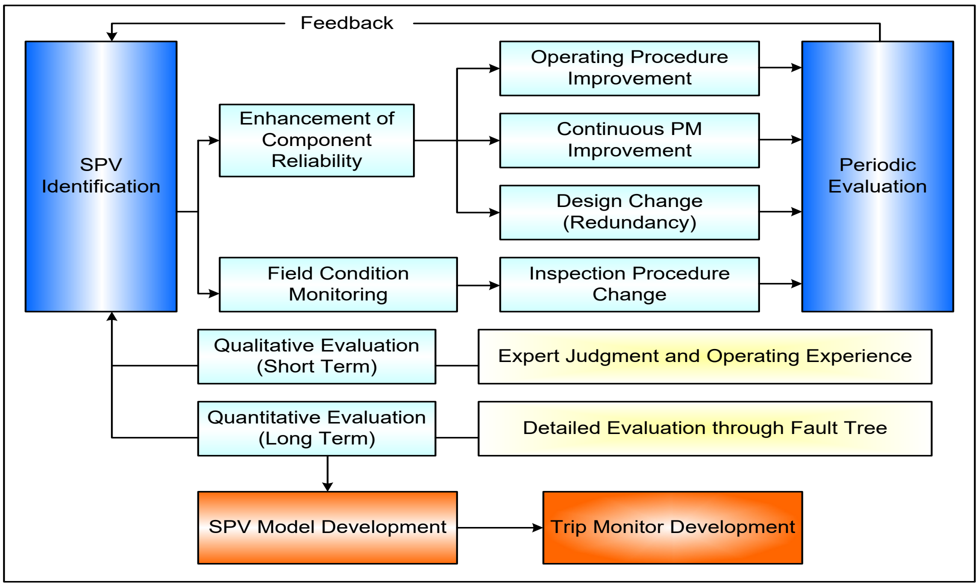

Feedback
SPV Identification
Enhancement of Component Reliability
Field Condition Monitoring
Operating Procedure Improvement
Continuous PM Improvement
Design Change (Redundancy)
Inspection Procedure Change
Periodic Evaluation
Qualitative Evaluation (Short Term)
Expert Judgment and Operating Experience
Quantitative Evaluation (Long Term)
Detailed Evaluation through Fault Tree
SPV Model Development
Trip Monitor Development

Fig. 6. Reliability improvement processes for SPV management

In addition, KHNP is working intensively not to incur incorrect operation and potential SPV failures caused by maintenance during normal operation. Therefore, KHNP has been operating a SPV monitor, which is able to evaluate power setback and unexpected trip risks induced by maintenance in normal operation. The SPV monitor produces different colours for risk change warnings and generates potential SPV lists associated with work orders.

In-circuit test (Development and Implementation)

In Korea, there was a reactor trip accident because the power source breaker of the RCPs came open after incorrect operation of the components of the electronic circuit boards in normal operation. The importance of a systematic management frame for the ICT (In-Circuit Test) of the electronic circuit boards during plant shutdown, and of safety-related facilities, was brought up through this accident. Especially, the establishment of objective analysis systems has come to be required for intervals of replacement management of components considered to have been degraded and for intervals of ICT implementation.

The ICT implementation data obtained from 1994 to 2014 have been extracted by utilising the PCB Maintenance Management System (PMMS), run by KHNP, in order to analyse the implementation intervals of the ICT. The intervals data, which reflect normal operation, have been used after maintenance work conducted for components that were regarded as having been degraded. For this, maintenance records based on ICT implementation findings have been identified for about 56 kinds of electric circuit boards of the 20 plant units that have local ICT implementation records. As a result of using these data to analyse the thorough CPC test intervals for the optimisation of the ICT targeting electronic circuit boards for each plant, it has been shown to be possible to discern and set up ICT intervals based on specific types of electronic circuit boards; this has been found to be possible because it was determined that the ICT implementation intervals were from 3.14 to 9.64 months for the year in the systems of process control, control rod drive mechanism, associated logics, plant protection.

In addition, according to reactor and board types, KHNP has analysed degraded components by using detailed trial result data. Most boards have detected to have approximately 1% degradation; a high level of degradation was sensed in certain operating computers and boards installed for the CPC. These research results will be used to adjust the circuit board ICT period associated with plant shutdown. Furthermore, this research has provided information on components that were degraded according to board locations and types; these components that should be fixed during the maintenance period.

8. FUTURE DEVELOPMENTS AND RESEARCH

Since the Fukushima Daiichi nuclear disaster, many pending problems such as safe improvement fulfilment resulting from stress tests, optimisation for both severe accident and off-site consequence analyses, multi-unit site risk assessment, and external events like earthquakes, have become main issues; more and more research and development are necessary. In addition to the things mentioned above, quality improvements for PSA for operating plants and to reflect the ASME Standard in the PSA for plants under construction, need to be achieved through continuous research.

As a follow-up activity to the new regulatory framework, KHNP has started to set up a structure for an accident management plan, including safety evaluation reports, a radiation environmental report, and a beyond DBA (design basis accident) AMP (accident management programme). In this framework, the scope of the safety analysis should be extended to reach newly classified accidents, the so-called DECs (design extension conditions). As a follow-up action, KHNP launched a government-sponsored R&D project to establish a foundation for the DECs; this project aims to develop a methodology for selecting DEC initiating events and, using deterministic and probabilistic approaches, evaluating the effects of design improvements.

The quality assurance of PSA is essential because various methods are applied in the process of PSA and the results can be utilised in diverse applications. Generally, for quality assurance, peer reviews based on standards, through which strong and weak information can be confirmed, are carried out. In the United States, the ASME PSA standard and NEI PSA Peer Review Process Guidance have been developed. Using these standards, some peer reviews have been conducted in Korea. The PSAs of Kori units 3&4 and Shin-Kori units 1&2 were checked based on NEI guidance in 2006 and 2008 respectively; for plants after Shin-Kori units 3&4, the ASME PSA standard is utilised in the licensing process. Although Korea has had several experience of using peer review for the operating and construction of plants, there are some discrepancies between each case. The reason for this is the absence of Korea-specific standard for peer review, thus sometimes, the range or method of the review process have been different according to the specific situation. Therefore, in the near future, Korea-specific standards for peer review will have to be established. For this, the followings should be supported: securing a pool of experts for the independent peer review, identifying the features of domestic plants, and achieving consensus on the level of peer review. In addition, a standard for F&O also needs to be developed.

The PSA in Korea has been focused on CDF and LERF, so the evaluation of the source terms, in Level 2 PSA, was quite conservative. Therefore, there are considerable differences in results of source term evaluation between Korea and the NRC SOARCA (State of Art Reactor Consequence Analysis). In this context, the NSSC has required results of adequacy evaluation as to the handling ability of severe accidents and a submission of research results of the SOARCA level; these items are necessary for issues that need to be improved to enhance safety, and rose to the surface during stress tests for the plants in Korea. Accordingly, KHNP is preparing a new R&D project with KAERI, entitled "Development of State-of-the-art Technology Level 2&3 PSA". The CANDU and APR1400 reactors are designated as representative model; the project has started to develop advanced techniques for the Level 2&3 PSA. This project is similar to the SOARCA report. Through this project, it is expected that technology elements of the Level 2&3 PSA and both an optimum analysis of a severe accident progress with the newest codes and an off-site consequence analysis reflecting domestic-specific qualities can be developed. Going forward, KHNP will gradually apply the improvements mentioned above to all plants.

KHNP has been carrying out research for a severe accident emergency situation response system and off-site consequence analysis improvement with advanced technology as a post-Fukushima action item. Furthermore, the nuclear industrial circle has to prepare for to meet obligations that became law in June 2015, such as that PSA must be included in accident management plan development and application, and a severe accident management plan. In the near future, comprehensive accident management, explained below, will be performed within the regulation framework.

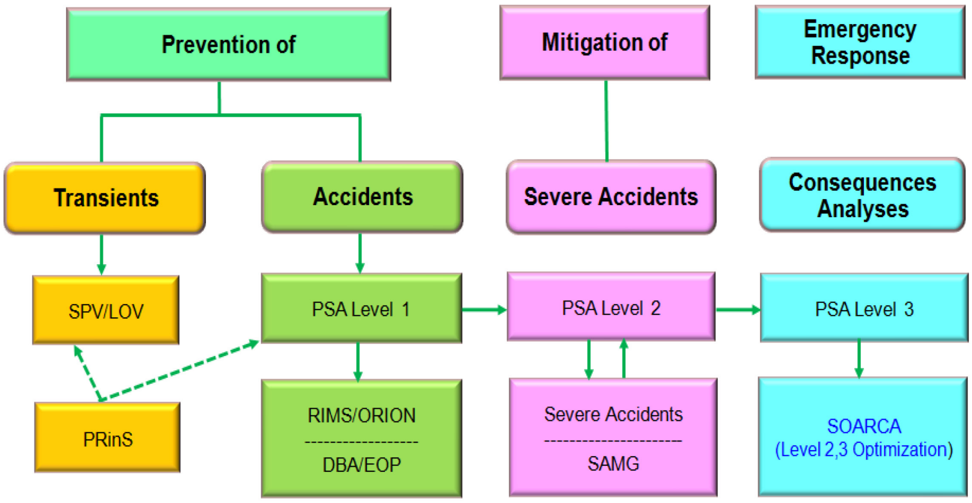


Fig. 7. Risk Evaluation and Management Programme Related to PSA

Domestic plants have the characteristic of multi-units concentrated on one site; moreover, there is a high population density around these plants. Therefore, the national interest in multi-unit risk has been very high since the Fukushima accident. However, there is not only no established method but also no basic direction for regulation and mitigation plans on this multi-unit risk issue. Therefore, at the present step, in addition to research on multi-unit risk analysis in consideration of domestic-specific characteristics, international co-operation with the IAEA and the NEA (Nuclear Energy Agency) needs to be conducted. Through this, fundamental technologies to meet the new safety goals, a methodology of risk evaluation for domestic multi-unit sites, and for operating licences are expected to be developed together.

According to the adoption of the DI&C (Digital Instrument and Control) system at Hanul units 5&6, research on DI&C PSA in Korea started quite a bit earlier than it did in other countries. Korea has conducted research on the DI&C system, such as execution of a fault injection test, development of methods for software and network reliability quantification, and analysis of operators' behaviours in a computer-based control room. Recently, the reliability of DI&C has been discussed as an issue to be treated during the NRC DC project for APR 1400; so, it has become a more urgent topic in Korea. Therefore, KAERI and KHNP plan to work together on safety issues related to DI&C systems. Based on research done by KAERI so far, KHNP wants to analyse the safety of the DI&C system in real plants. That research plan is under discussion now.

Recently, research on the physical protection is being carried out in Korea. KAERI has developed the VAI (Vital Area Identification) methodology and VAI software called VIPEX (Vital area Identification Package Expert) for identifying vital areas. Utilities have also conducted projects on development of physical protection design technique for APR 1400 exportation. In addition to this, since the Fukushima Daiichi nuclear accident, the issue of how safety should be co-ordinated with physical protection is being discussed. This issue needs to be addressed in the near future.

9. INTERNATIONAL ACTIVITIES

Relating to PSA and Risk Assessment, Korea has collaborated in various international activities such as the OECD/NEA working groups, IAEA, and other bilateral/multilateral co-operations; this has been done as part of Korea's attempt to find a way to solve several pending problems. Korea has played important roles in these organisations.

OECD/NEA Programmes

Relating to PSA and Risk Assessment, Korea is currently participating in various working groups of OECD/NEA such as WGRisk (Working Group on Risk assessment), WGHOF (Working Group on Human and Organisational Factors), WGEV (Working Group on External eVents), WGIAGE (Working Group on Integrity and Ageing of Components and Structures), and WGAMA (Working Group on Analysis and Management of Accidents).

The representative tasks of the OECD/NEA WGRisk, which Korea participated and which is currently participating in, are as follows : 1) PSA for advanced reactors (completed in 2012, KAERI took the lead in this task); 2) Use and development of Probabilistic Safety Assessment in member and non-member countries (ongoing, core group); 3) Status of the site level PSA (including multi-unit PSA) development (ongoing, core group); 4) Status of practice for Level 3 PSA (ongoing, core group); and 5) Human reliability analysis in external Event PSA - survey of methods and practice (ongoing, core group).

Korea is trying to procure some data for PSA/risk assessment, which data cannot be obtained from domestic experience, through the OECD/NEA collaborative projects. The representative projects are 1) OPDE (Operation Pipe Data Exchange) for an exchange of pipe failure frequency data; and 2) ICDE (International CCF Data Exchange) for an exchange of CCF data.

There are also two projects that Korea is participating in, being led by GRS (Gesellschaft für Anlagen- und Reaktorsicherheit). The first one is the OECD FIRE programme (Fire Incidents Records Exchange, 2014.01-2015.12), to establish a DB of fire accidents in NPPs. The aims of this project are the identification of important causes of fire and the funding of proper preventive measures. The second one is HEAF (High Energy Arcing Fault Events, 2012.07-2015.12), which will take into account the evaporation of cables at 430 Volts when a short circuit occurs between them.

Korea is participating in two collaborative research projects under an initiative of the OECD WGIAGE with various institutes: 1) MECOS (Metallic Component Margins under High Seismic Loads, 2015.03-2016.09); and 2) IRIS (Improving Robustness Assessment Methodologies for Structures Impacted by Missiles, 2015.05-2017.03) benchmark phase 3. The main objective of the MECOS benchmark study is to quantify margins in the seismic analysis of safety class piping components for high seismic loads, associated with existing design practices. The participation in the MECOS benchmark is open to experts from research organisations, technical support organisations, regulatory authorities, NPP owners, consulting firms, and in general to all those willing to perform computational prediction of experimentally tested piping systems. The purpose of the IRIS benchmark phase 3 is to continue the activity started by the OECD/NEA/CSNI CAPS (CSNI Activity Proposal Sheet) task "Improving Robustness assessment of structures Impacted by missiles" the so-called IRIS_2010 and IRIS_2012. This third part of the IRIS programme is dedicated to study of the propagation of induced vibrations of a civil structure impacted by a missile and of the transmission of these vibrations from the impacted wall to the connected walls and floors.

There are also two projects under the OECD WGEV. One is the SSAEH (Science-based Screening Approach for External Hazards), which is a project about the technical basis behind an approach for science-based screening of external hazards. Although this project is still in the planning stage under the lead of the INL (Idaho National Laboratory) and EPRI, KAERI plans to participate in this project. Another project is called Riverine Flooding - Hazard Assessment and Protection of NPPs. The objectives of this CAP are the collection of information from CSNI member countries with respect to current regulatory practices and technical approaches used to confirm the adequacy of protection of NPPs against riverine floods ; another objective is the identification of key issues regarding riverine flood hazard assessment (both deterministic and probabilistic) and flood protection.

The IAEA Programmes

Korea is participating in three topics with the IAEA ISSC (International Seismic Safety Centre) EBP (ExtraBudgetary Programme). One looks at soil-structure interaction methodologies; the objective is to review state-of-the-art practices regarding soil-structure interaction methods, assess each of the methods currently available to the practitioner (engineering toolbox), and provide guidance about the applicability of each of the methods to the nuclear industry. The final product of the task will be an IAEA TECDOC. Another topic is integrated PSA and countermeasure procedure against fault displacement hazard. This task covers enhancement of probabilistic fault displacement hazard from the viewpoint of PSA. Another task is a safety assessment for multi-hazard and multi-unit sites. The aim of this research is to develop methods and detailed guidance for safety assessment of multi-unit sites under the impact of multiple hazards. The expected outputs of this project are as follows: framework and process for multi-unit site probabilistic safety assessment, identification and screening of external hazards for nuclear installations, external hazard considerations for single and multi-unit probabilistic safety assessment, and technical approaches for multi-unit site probabilistic safety assessment.

Regulatory Standard S-294 was amended and re-issued in 2014 by Canadian Nuclear Safety Commission (CNSC) as REGDOC-2.4.2, "Probabilistic Safety Assessment (PSA) for Nuclear Power Plants" to include multi-unit impacts. Since the multi-unit PSA became an issue during the Darlington License renewal process, the CANDU Owner's Group (COG) has been conducting a project called "Development of a Whole Site PSA Methodology" to manage nuclear safety within a hierarchal safety goal framework. There is increasingly more needs for people inside and outside of the nuclear industry in Korea to look into this issue. Therefore, KHNP has decided to participate in the COG's international joint project for buy-in result documents.

On the other hand, during the CSRM (CANDU Senior Regulator Meeting) held in India in November 2005, a decision was made to compare PSA practices of countries operating CANDU-type reactors with the purpose of information exchange and future harmonisation. The first technical meeting of the CPWG (CANDU PSA Working Group) was held in Vienna in May 2010. Since 2010, the CPWG has held four meetings (2011, 2013, 2014, and 2015) to discuss the PSA practices and progress towards specific tasks included in the work programme. The IAEA recommended that the document produced by CPWG should be in the format of a TECDOC. The document preparation proposal for TECDOC on CANDU PSA Level 1 was approved by the IAEA at the end of March 2016.

Other Collaborative Programmes

Since 2010, KAERI, NRC, and BNL have agreed with the necessity of reliability quantification of DI&C systems and have co-operated in the development of methodology to combine the DI&C model with existing PSA. Currently, research on a software reliability quantification method is ongoing; as a result of this co-operation, a NUREC/CR about software reliability assessment methods based on the Bayesian networks will be published at the end of 2016.

Not only Korea but also the NRC believes that a collection of nuclear power plant crew simulator exercise information can improve data for human error probability estimation. As such, the NRC has developed the (SACADA) Scenario Authoring, Characterization, and Debriefing Application database. In an effort to increase the amount of data available for HRA method improvement, in 2013, KAERI and the NRC signed a bilateral agreement on the use of the SACADA database for the collection and exchange of operator simulator performance information. The information exchange will greatly benefit HRA quality for both the United States and Korea, and it will support the improvement of current plant operational safety. Because of data sensitivity, KAERI and the NRC plan to solely exchange analysed data instead of raw data.

The KAERI-BNL collaboration programme for joint development of seismic capability evaluation technology for degraded structures and components, involves significant contributions of both parties, with BNL focused on computer code development for simplified soil/structural models, and KAERI focused on ABAQUS analysis of detailed SSI models and development of equipment fragilities. The final results of this programme will be utilised for an update of seismic PRA technology in Korea for beyond-design-basis earthquakes. The advanced seismic PRA tools that will be developed can be used to evaluate the seismic safety of existing operating NPPs and new NPPs. This Year 1 Progress Report summarises only the research work performed by BNL. The current collaboration programme (2012-2017) was developed in light of the successful conclusion of the previous BNL-KAERI collaboration programme (2007-2012). The previous programme focused on methodology development for fragility analysis of passive structures and components with degradations.

MEXICO

1. INTRODUCTION

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 utilisation 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 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 PSA programme in Mexico formally started in the early 80s 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 organisations, 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 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 defence-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, 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 Inform Inspection Guides (RIIG) has been developed to incorporate risk information into the inspections activities. The RIIG have been used to prioritise inspections and to optimise 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.

Use of portable equipment are considered as part of the extended SBO mitigation strategies post-Fukushima, however, they are not modelled in PSA jet because still under analysis and implementation process in the LVNPP, requiring the development of explicit procedures. As soon as the above-mentioned strategies are approved and implemented, they will have to be reflected in the PSA models, doing emphasis in the human actions needed for its application.

3. 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 colours, 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.

Stage	Mining	Colour (Risk indicator)	Actions
Preliminary (stage 1), In order to screen events without risk significance from those related with safety aspects we decide to develop and to use a flow chart (which is such as a "yes" or "not" answers questionnaire), that guide us in performing our analysis. Every question here asked is a very specific question related to the situations that were involved when the event or finding took place. The principal idea is to determine if the events or findings affected the safety-related systems (or safety function).	In case of an administrative fault. If a safety-related systems or safety function was affected	Green: Very low safety significance	It must be settled by the proper administrative channels. This event or finding go to the stage 2 for continue with its analysis.
Stage 2, automated Excel worksheets were developed, to compute and determine the corresponding risk level. It is important to mention that this calculation use a simplify PSA model derived and validated with the LVNPP specific model, for that reason the result will be conservative.	Determine the corresponding risk level in accordance with the increase of the Core Damage Frequency and the result of the compute is boxed in one of four colours above mentioned.	• Green: •White: •Yellow: •Red:	It must be settled by the proper administrative channels. Refinement of the risk significance of Phase 2 findings/events, by using the PSA complete models.
Phase 3 - refinement of the risk significance of Phase 2 findings/events.	Risk increase confirmation or change of characterisation.	• Green: •White: •Yellow: •Red:	It must be settled by the proper administrative channels. A multidisciplinary team of analyst will evaluate in detail using deterministic and probabilistic models for more accurate characterisation of the event/finding to support the making decision process and the safety impact evaluation process.

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 colour will be defined risk management actions:

Colour (Risk indicator)	Mining	Actions
Green 1.0≤CDF or LERF□2.0	Minimal risk, the work is performed normally (not actions are required)	The work is performed normally.
Yellow 2.0≤CDF or 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≤CDF or LERF□20.0	High risk, you need the authorisation and approval to perform the work in this condition.	It is required the authorisation 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 LERF≥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.

It is important to mention that the criteria established by CNSNS are indicative, and we don´t have criteria for SFP, nor research reactors.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

CNSNS has initiated a programme to expand the use of risk information into the regulatory framework. The efforts are addressed to emphasise 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.

In this way, 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, until now four operational stages has been developed.

As part of the IPE updating process, which is performed each 5 years or when an important change in the plant is developed, CFE has submitted the last version of IPE Level 1 and Level 2 for its evaluation by CNSNS, so the review process is ongoing.

On the other hand, into CNSNS the updating of its PSA level 1 and PSA level 2 are ongoing.

After Fukushima in the LVNPP was re-evaluated the seismic deterministic analysis developed in 1971.

The re-evaluation was developed with base in the historical earthquakes and geological characteristics of the zone. The historical analysis took into a count the biggest earthquakes that they have presented in the region in a radius of 320 km, with base in the geological formations and the distance of the site to geological identified faults and in the local and mechanical geology of rocks. The maximum possible earthquake is the design base earthquake for safe shutdown of the plant, expressed in terms of land acceleration. The maximum land acceleration of the area for the design base earthquake is 0.26 g.

Also the potential of flood in the site of the LVNPP was analysed

Two oceanographic conditions were considered into the analyses: tsunami and hurricane, the analysts did not identify a tectonic mechanism of fault in the zone that could generate a tsunami. They postulated a tsunami of volcanic origin of magnitude 1, considering an earthquake of 6.5 richter degrees in the gulf of Mexico. Analysts determined that the maximum probable tsunami in the site would be of 0.75 m height.

On the other hand, the analysts determined that the maximum probable hurricane would be sustained wind of 276.74 km/hr, and blasts wind of 304 km/hr, which induced the formation of waves of 6.068 m above sea level outside the protection breakwaters. This surge would represent an elevation of 2.00 m inside the dock over the maximum registered level.

5. 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, internals relays, initiation logic components, etc. The component fault was defined on the failure mode concept identifying the component fault statement (example, open failure valve). All models are handled with the CAFTA code. The CCF-modelling is based on the Multiple Greek Letter model. For human reliability, pre- and post-initiating-event human errors were modelled, taking into account only errors of omission, THERP and ASEP methodologies were used to model such human actions. Failure data obtained from the maintenance rule programme have been incorporated. The human actions were modelled 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 1 000 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 oxidised 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 cesium 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 the severe accidents (MELCOR).

The PSA model uses plant-specific data for failure rates and for initiating event frequencies. 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. Failure data incorporated to the models were obtained from the maintenance rule programme.

It is important to emphasise that, for the PSA models developed in the regulatory body, a general review (peer review) was developed with the co-operation of Sandia National Laboratories, and for the low power and shutdown models the peer review was developed by Information Systems Laboratories (ISL).

The PSA consider each unit as independent, i.e. the multi-units aspects are not modelled in the PSA.

6. NOTABLE RESULTS OF PSAs

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. This connection provides an alternative way to inject water into the reactor vessel or to spray the containment during this kind of accident.

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 developed 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 programme.

The original design of the LVNPP includes a connection for the emergence venting of the primary containment, this function is performed through by opening valves, which discharge to the secondary containment (reactor building).

After Fukushima accident, Mexican Nuclear Regulatory Body (CNSNS) based on NRC orders EA-12-050 "Issuance of order to modify licences with regard to reliable hardened containment vents" evaluated the applicability of those requirements to LVNPP.

Utility decided to implement a Hardened Containment Venting System (currently in process – not installed yet) that is contained in a modification plan to install the new vent system (HCVS).

CNSNS has decided to perform the risk evaluation to quantify the safety impact because of this sensitive hardware change (Impact to Level-1 and 2 under venting configuration proposed).

Since risk point of view (PSA Level 1) the hardened venting configuration proposed has benefits, it represents a considerable risk reduction (CDF). It was a good exercise, however, it is missing incorporate the venting procedure, procedures and human factors/reliability are a very important factors for the safe use of system; this is because procedure describes times and roles for decision making of venting process.

The installation of a hard vent allows venting of the primary containment in order to prevent the failure by overpressurisation and control of temperature within containment, in this way in the case of an accident that exceeds a design base accident, system can relief in a controlled manner the overpressure always by trying to minimise releasing of radioactive material and avoid failure of the primary containment (containment integrity).

Additionally, CFD codes (Computational Fluid Dynamic) were employed together with MELCOR's results to evaluate the possibility of hydrogen detonation by effects of primary containment hard emergency venting. An important conclusion is the prediction of a high possibility to produce a H2 explosion in the hard vent pipe

Also it is important to mention that as part of the review process of the IPE Level 2 updating, we are analysing the difference trends in the results, which in this updating version, the dominant Categories of fission products releases is high early, in comparison with the previous version, which the dominant release category was high intermediate.

7. PSA APPLICATIONS AND DECISION MAKING

A PSA application was submitted by the utility following the USNRC regulatory guide 1.174 to complement the deterministic analysis presented to support a plant modification request that involved the increase of the thermal power in 5%. The calculated increase in core damage frequency was 2.87x10-6 per reactor-year. This increase is in the range of 10-6 per reactor-year to 10-5 per reactor-year. The regulatory guide establishes, in this case, that the application can be accepted if it can be reasonable shown that the total core damage frequency, considering internal events, external events, full power, low power and shutdown, is less than 10-4. The IPE for Laguna Verde currently covers only internal events for full-power operation. The contribution of the out-of-scope portions of the model was allowed to be addressed by bounding analysis, since significant margin exist between the calculated change in risk metrics and the acceptance guidelines. The application also covers the large early release frequency. The increase in this frequency was very small and therefore acceptable. The regulatory authority concluded that the application complies with the regulatory guide as well as with the key principles associated. These principles establish that the proposed change meets the current regulation, that is consistent with the defence-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.

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 prioritise inspection tasks. The use of risk information for inspection purposes started in the early 1995, with the development of plant-specific risk inform inspection guides (RIIGs). These RIIGs provide the risk inform ranking of systems, components and operator actions. The RIIGs 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 RIIGs 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 programme.

Actually the PSA has also been used to develop emergency scenarios to be used to evaluate the External Radiological Emergency Procedures (PERE).

8. FUTURE DEVELOPMENTS AND RESEARCH

As a result of the CNSNS partake on the Safety Margin Action Plan (SMAP) managed by the OECD/NEA, efforts will be addressed to analyse the Dynamic PSA approach in order to assess the impact in the plant safety margins of plant modifications.

CFD codes (Computational Fluid Dynamic) will be employed together with MELCOR's results to evaluate advantage to using filtered venting of Containment vs Sprays (increasing its reliability since probabilistic point of view) during accident scenarios.

9. INTERNATIONAL ACTIVITIES

Currently there is not participation in international projects.

NETHERLANDS

1. INTRODUCTION

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 510 MWe in operation since 1973. In 1997 the Dodewaard NPP, a vintage small GE-BWR ceased operation. There are currently two research reactors in operation: High Flux Reactor (HFR) in Petten (45MWth) and Research Reactor Delft Technical University (2 MWth). Increasingly, more emphasis has been placed on the safety of the High Flux Reactor, a 45 MWth 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 in the beginning of this century. This has been further developed into a real full-scope PSA L1 in the last years. The next years completion of L2 and L3 is expected.

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. Insights from generic PSAs and PSA from others 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 tried to close the Borssele NPP by the end of 2003 by imposing a special licence condition in that respect. The staff of the plant lodged an appeal against this restriction. In 2000 the Council of State (highest administrative court in the Netherlands) revoked it on formal grounds. A newly elected government accepted this ruling and adopted the policy that the NPP could operate as long as it is safe. Then the next government around 2003/2004 adopted a goal to close the NPP by the end of 2013, the original design life. Finally this Government in 2006 made another deal: an agreement between the utility, its owners and the government that the plant may operate till end of 2033, provided that the plant will remain within the group of the safest NPPs in the world (top 25%). A so-called independent Benchmark Commission shall produce a report every five years starting in 2013 to conclude is this is the case.

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 (1x E-6/y). In 2009/2010 three initiatives for new nuclear installations came forward (two NPP’s and one Research Reactor-PALLAS- to replace the HFR). After the Fukushima Daiichi accident the NPP plans were stopped. The PALLAS project is currently in the pre-licensing phase, with a planning to start operation around 2025. It is uncertain it will be realised, since the funding should be done by private parties.

Legal and Regulatory 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 framework 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 focusing 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 radiological protection, designates the various competent authorities and outlines their responsibilities.

A number of decrees have also been issued containing additional regulations. 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 (Bkse) regulates all activities that involve fissionable materials and nuclear installations.

The Bkse sets out additional regulations in relation to a number of areas, including the procedure for applying for a licence. These contain also the requirements for the application of a licence. Among 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).

Environmental Protection Act

The Environmental Protection Act, in conjunction with the Environmental Impact Assessment Decree, stipulates (in compliance with EU legislation) that an Environmental Impact Assessment must be presented if an application is submitted for a licence for a nuclear installation.

In cases concerning nuclear installations the Nuclear Energy Act takes precedence and regulates also the aspects of conventional environmental issues.

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.

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 (Dutch acronym; NVR) and has been developed in the nineties of the 20th century. The NVRs are based on the IAEA Safety Standards. Using an agreed working method, the relevant IAEA safety principles, requirements and guidelines were studied to see how they could be applied in the Netherlands. This resulted in a series of amendments to the IAEA standards, 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 licence 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. In the period 2007-2010 the system of NVR's was updated with the then latest versions of the IAEA safety standards and an updated list of NVR's were attached in 2011 to the licence of the NPP, modified for the introduction of MOX-fuel.

Dutch Safety Requirements (DSR)

In 2009-2010 there were two initiatives for new nuclear power plants and one initiative for a new research reactor, which made the regulatory authority decide to develop the so-called Dutch Safety Rules (DSR) for new reactors. The DSR was developed with large support by GRS (TSO for the Dutch authorities) using several important sources such as the newly developed German safety requirements, modern IAEA standards (including Fukushima lessons), WENRA Safety Objectives of New Reactors and WENRA Reference Levels. At the end of 2015 the DSR has been published as a guidance document. Although new build of NPP's has been stopped, the DSR can be applied to the research reactors with a graded approach. The DSR should be seen as "requirements". In parallel, and still going on, are activities to support the DSR with adopted/amended IAEA safety guides.

Regulatory Body

Before 2015 the Nuclear Regulatory Body in the Netherlands was formed by two entities. One directorate was responsible for policy development, development of the legal framework and licensing, the other directorate was responsible for inspection, assessment and enforcement.

In 2014 the Government decided to combine all regulatory activities in one single entity the Authority for Nuclear Safety and Radiation Protection (Dutch acronym: ANVS), which started from beginning 2015. The ANVS will become an independent administrative authority in 2017 and resides under the Ministry of Infrastructure and Environment. The goal was to create a much more robust organisation and put all regulatory expertise under one roof. Currently is has a staff size of 122 fte and in the near future this will grow to about 140 fte. The ANVS carries out preparation of policy, law, regulation, licensing, supervision and enforcement tasks in the area's of nuclear safety, radiological protection, security, safeguards, waste, transport, emergency preparedness.

More information on the regulatory framework can be found on the ANVS-website www.anvs.nl and in the latest report on the Convention on Nuclear Safety.

Historic development of regulatory requirements for PSA

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 and Dodewaard (58 MWe GE-BWR). Because plant-specific PSAs were not available at that time, generic PSA insights and lessons learnt 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.

Development of PSAs for the two NPPs Borssele and Dodewaard

Both the licensees and the licensing authorities agreed with the GRS-proposal to conduct a level 1+ PSA. This resulted in two bid specifications for a level-2 minus PSA. For Borssele this PSA project was awarded to the combination KWU and NUS (currently Scientech Inc.), and for Dodewaard the project was awarded to Science Applications International Corp. (SAIC) from the United States and to KEMA (the supporting organisation of electric utilities in areas of testing, certification, assessment, research and development). Work on the Borssele PSA started in 1989 and was completed in 1992.

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 [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). To provide a computerised 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.

The development of the Dutch PSAs was more or less parallel to the large modification/backfitting programmes, which emerged, mainly as a result of Chernobyl. A backfitting requirement was formulated for the existing NPPs and supported by a backfitting policy paper in 1991. 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 involved the requirement of a periodic 10-yearly safety review. The first large safety reviews were carried out on a voluntary basis. This requirement was included in the operating licence of both plants some years later.

Since it turned out that the first large modification programmes, based on the first large safety reviews involved a licensing procedure, that also required submitting an Environmental Impact Statement according to the Dutch Environment Act it was needed to further develop the Level 1+ PSA to a full-scope Level 3 PSA, 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) . This meant also 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. The PSA work at the Dodewaard plant stopped after the decision to close it in 1997.

The first level 3 full-scope PSA for Borssele was finished in 1995.

3. PSA OF THE HIGH FLUX REACTOR (HFR)

The existing licence of the HFR at the end of the last century 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 lay with the two Nuclear Power Plants at that time. This approach was supported by the low potential risk compared with the risk from the NPPs.

After the closure of Dodewaard (1997) and the implementation of the large modification programme at the NPP Borssele (1998) it was felt appropriate to extend the policy of introducing PSR to other nuclear installations, e.g. the HFR.

In discussions between the regulatory body and both the owner/licensee (JRC-Petten) and operating organisation (NRG) the scope of work for the first (voluntary) safety re-evaluation of the HFR 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 have been 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 programme to achieve this safety concept.

Because a full scale Probabilistic Safety Assessment (PSA), as conducted for an 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.

The modification plan after the PSR led to a need for a change of the licence and at the same time this was used to transfer the licence to the operating organisation NRG. In this licence the requirement for a 10-yearly safety review was introduced.

In the framework of the second (this time obligatory) PSR it was agreed that NRG would develop the risk scoping study into a genuine full-scope PSA L1 –L3. This project was finished in 2016. This PSA is now under review by the regulator.

Transition towards a more risk-informed regulation

Because the regulatory body increasingly was 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 regulatory body, the IAEA was asked in the beginning of this century to advice 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 regulator 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 online maintenance activities.
- It 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, it was 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, as a minimum, to 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 regulator to Borssele NPP, these should be discussed with the plant to maximise mutual benefit. Also, the discussions raised the idea that perhaps the regulator and Borssele NPP could develop a consensus document to conduct and assess PSA applications.
- Finally, it was suggested to use PSA to focus the regulatory inspection programme on the more significant systems, components, and plant practices.

As a follow-up of this advice, the regulator cautiously defined a follow-up programme/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 other countries, while the next steps were centred on a particular application, such as Technical Specification optimisation.

Follow-up programme

The objective of this programme was 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 were 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.

As the available manpower within the regulatory body was limited, the development of Risk-informed Regulation would be based on existing approaches elsewhere; no separate 'Dutch' RIR development was foreseen. Main vehicle was the USNRC development, plus useful parts of the approaches in Spain, Switzerland, Sweden, Finland, Belgium and the UK.

The main objectives of the RIR were:

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

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

Overall, the RIR products would be application-oriented. In some areas, fundamental aspects may be touched, where no written guidance could 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 responsible minister 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 showed 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 and are acceptable because further continuation of safety takes place.

As a more formal start of this project the adaptation of USNRC Regulatory Guide 1.174 with regard to the Dutch Safety Criteria was prepared to formalise it as a Dutch Nuclear Safety Guide on the Risk Informed /Regulation Decision Making. This safety guide has been drafted by the regulatory body until 2009. After that an external consultant was hired to further develop it as a RIDM safety guide, also because in the meantime the EU Directive on nuclear safety was published in 2009, where the principle of continuous improvement was introduced as a legally binding requirement, to be implemented in 2011 in Dutch legislation. However the development of the RIDM safety guide was finally stopped in 2012, because it was felt that it would be too complicated in practice.

Guidance on the continuous improvement of safety was developed and published in 2015.

4. 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 form the basis for government policy on risk management.

The Nuclear Installations, Fissionable Materials and Ores Decree (Part of the Nuclear Energy Act) has been amended to incorporate this risk policy in the licensing process for nuclear installations. Risk criteria are explicitly included as assessment principles for licences 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. This set, which is part of the amended Nuclear Installations, Fissionable Materials and Ores Decree, are as follows:

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

An additional limit of 500 mSv thyroid dose (Hth) 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 n2. 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 first version of the level-1 PSA guide was an amended version of the IAEA Safety Practice: ‘Procedures for conducting level-1 PSAs’ (Safety Series No. 50-P-4) and the first version of the level-2 guide is based on the IAEA Safety Practice: ‘Procedures for conducting level-2 PSAs (Safety Series No. 50-P-8).Today in the licence of the NPP Borssele there are included NVR’s for PSA Level1 and 2 based on the recent IAEA safety standards.

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.

Recently this level-3 PSA guide has been modernised.

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

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 online maintenance,

The licensee of the Borssele plant has defined several numerical safety criteria as performance indices (PIs). Evaluation of historic output of the Risk Monitor was used as a basis for these PIs. 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%.

The PI for all operating states:

- Instantaneous TCDF shall never exceed the value of 10^{-4} /year.
- For optimisation of AOTs the licensee has adopted a value of $5x10^{-8}$ for ΔTCDF x AOT and ΔTCDF always $<10^{-4}$ /year.

5. 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 IAEA. 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 US 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 led 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 (covering the period 1993-2002) 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.

In the third periodic safety review (covering the period 2003-2012) it was agreed between the licensee and the regulatory body that the major part of the evaluation would consist of a full-scope IPSART mission, that took place in 2010, followed by a follow-up in 2013. The recommendations of that mission guided the licensee to make substantial improvements in the PSA. The regulator has asked to use this modified PSA to do the weakness analysis in the frame of the PSR. Also the effect of modifications on the CDF was calculated.

6. STATUS AND SCOPE OF PSA PROGRAMMES

Borssele

After finishing the full-scope level 3 PSA, the focus shifted towards "Living PSA" (LPSA) applications. The first model was finished in 1997 (LPSA97). New licences of the modified plants require the licensees to have an operational 'Living' PSA, without prescribing the concept and applicability of LPSA any further. The operator of the Borssele plant has also installed a risk monitor in 1999 for configuration control during outages, uses the PSA for optimisation of Technical Specifications, etc. and widely available for use in 2000. As part of the next PSR the internal fire and human error sections of the PSA were updated in 2006, reflecting also the as-built situation after the modifications. In 2010 an IPSART mission was held. The conclusions from this mission were one of the reasons to start a major update of the PSA and Safety Monitor in 2011-2013: LPSA13. The update consists a.o. of renewed screening of the initiating events, a new CCF analysis, an update of the human error analysis, a new external flooding model, a complete revision of the Level 2 and 3 analyses and a restructuring and update of the documentation. The Safety Monitor is brought in line with the renewed PSA. In 2016 the model was again updated and adapted to the major modifications that had to be licensed. The next step will be to include the rest of the modifications.

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.

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 licensee of the HFR (NRG) developed first a level-3 risk scoping study covering only the full-power state and covers both internal events and area events (fire and flooding). Recently this was transferred to a real full-scope PSA, covering all operating states, internal events, internal and external hazards and the reactor, the spent fuel pool, and experiments. The PSA L1 is ready, L2 and L3 are under development and planned to be ready by end of 2017. The use of PSA will be optimised decision making for e.g. maintenance, PSR etc.

7. 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 currently managed with codes like winNUPRA and Psimex. The current PSA contains 160 initiating events. Initiating events with a frequency smaller than 1x E-9/y or leading to core damage with a frequency less than 1xE-10/y are screened out.

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. Periodically the data set is updated via Baysian updating.

The CCF-modelling is based on the Alpha Factor Model and uses both generic CCF-parameter data and data from the International Common Cause Failure Data Exchange Project (ICDE) via the German power plant owners organisation VGB. Special attention was given to the common-cause factors for the two testing strategies (sequential testing and staggered testing)

For human reliability pre-initiating and initiating errors are modelled according to international norms/guidances SHARP (EPRI)and ASEP (USNRC). Originally, the post-initiator errors were modelled via HCR/ORE. This was later 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 plant damage states were identified, with each PDS characterised with 8 attributes. Containment event trees were developed for all 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 a plant-specific MELCOR model is used. Currently 19 source term categories (STC's), each determined by a representative accident scenario, are defined. The STC's are grouped according to three release time periods following reactor trip or shutdown; the level-3 assessment was carried out via the COSYMA code.

- Early: 0- 12 h
- Late: 12- 72 h
- Very late: > 72 h

From the 19 STC's, 15 are related to the reactor and 4 to the spent fuel pool. One additional category was defined: core damage without releases. The actual PSA-model that was used for the licence application in 2014 for several modifications has the following main results:

Reactor CDF	2.3 x E-6
SFP CDF	0.4 x E-6
No release CDF	0.2 x E-6
TCDF	2.9 x E-6

HFR (Risc Scoping Study): For the assessment of the level-1 risks the same method was used as for power reactors; small event trees and large fault trees. The models were managed with the CAFTA code.

Generic data were used (e.g. T-book for instrumentation)

For dependent failures the Beta Factor method was used. The factors were taken from NUREG/CR-4780.

For the pre-initiator human actions ASEP and THERP was selected. For the post-initiator actions were modelled with TRC.

As a basis for the fire assessment IAEA Report Series No. 10, Treatment of internal fires in probabilistic safety assessment for nuclear power plants was selected.

For the level-2 part MELCOR was modified to handle Aluminium cladding and U.Alx fuel (High Enriched Uranium) respectively U3Si2 fuel (Low Enriched Uranium).

HFR (PSA): For the assessment of the level-1 risks the methodology used is current state-of-the art and the same method was used as for power reactors: small event trees and large fault trees. The models are managed with the RiskSpectrum code. Also the level-2 is modelled in RiskSpectrum. The choice of the level-3 software is not yet made.

Plant-specific and generic data were used (e.g. ZEDB, T-book for instrumentation).

For dependent failures the Alpha Factor method was used. The factors were taken from the NRC CCF database.

For the pre-initiator human actions (type A human errors) conservative screening values are applied. If this leads to a significant contribution to the risk ASEP is used. Type B errors (initiators) are quantified with THERP and post-initiator actions (type C) with a combination of THERP and the HRC correlation method. generic values are used to quantify the probability of misdiagnosis.

As a basis for the fire assessment NUREG/CR 6850 and its updates were used.

For the level-2 part MELCOR was modified to handle Aluminium cladding and U3Si2-Al fuel.

8. PSA APPLICATIONS

This chapter exclusively deals with applications of the Borssele PSA.

In order to use the PSA in the decision-making process it is necessary to define which results are needed, and define criteria the results may be compared with. The IAEA developed a guideline that defines which quantitative results (referred to as PSA metrics) are required to use the PSA for specific applications, IAEA TECDOC 1511. The table below lists the required PSA metrics for the selected KCB PSA applications.

Six metrics involve core damage. It is therefore important to define what is included in the definition of core damage. In the PSA of KCB, only widespread core damage is modelled as the single biggest contributor to individual and societal risk. Core melt arrest is modelled as a success sequence. The failure/damage of single fuel assemblies or a limited set of fuel assemblies, including transport or movement of fuel assemblies is excluded from the scope.

The Level-3 metrics for the KCB differ from those in the IAEA TECDOC 1511. The main difference is that the Level-3 metrics for the Dutch situation as defined by law are Individual Risk (IR) and Group Risk (GR) as Quantitative Health Objective (QHO) and replace the Large Early Release Frequency (LERF) proposed by the IAEA. Level-3 risk importance measures are based on IR.

The Borssele Safety Monitor does not provide Level-3 output: Applications 3.4.1, 3.4.3 and 5.1.3 (see table) are limited to Level-1 evaluations. Therefore the use of the Large Early Release Frequency as a function of time (LERF(t)) is not necessary.

Table Required PSA results (columns) for the selected PSA applications (rows)

	CDF_{AVE}	CCDP	$CDF_{\{t\}}$	ICCDP	Key	IR/ ΔIR	Group Risk	Prime contributors	QHOs	Risk importance measures	ΔCDF_{AVE}
1.1 Assessment of overall plant safety	X					X	X	X	X	X	X
1.2 Periodic safety review	X					X	X	X	X	X	
3.4.1 Configuration planning (e.g. support for plant maintenance and test activities).			X	X		X				X	X
3.4.3 Dynamic risk-informed TS				X							
4.1.1 NPP upgrades, backfitting activities and plant modifications.						X	X			X	X
4.2.1 Determination and evaluation of changes to allowed outage time and changes to required TS actions.				X		X				X	X
4.2.2 Risk-informed optimisation of TS				X		X				X	X
4.2.3 Determination and evaluation of changes to surveillance test intervals										X	X
4.2.4 Risk informed in-service testing						X				X	X
5.1.3 Short term risk based performance indicators	X		X			X		X	X	X	
5.2.2 Evaluation and rating of operational events	X	X				X					
6.1.1 Risk evaluation of corrective measures						X					X
6.1.2 Risk evaluation to identify and rank safety issues.	X				X	X		X	X	X	

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 programme. Therefore, the new safety concept was mainly derived from a deterministic safety concept of the German Convoy plants. However the PSA played a large role in the optimisation and evaluation of the deterministic safety concept, study of alternative solutions and in the licence renewal (Environmental Impact Assessment). Examples of the use of PSA to study alternative solutions were: - second grid connection, and – turbo against electrical driven aux. Feed pump. The Modifications reduced the TCDF from 5.6x10-5 /year to 2.8x10-6 /year.

In 2003 the second periodic safety review took place. The PSA played an important role. All issues were weighed (Low, Medium and High impact) on the risk significance (TCDF and Individual Risk (IR)). The licensee presented an improvement plan. For each echelon of defence-in-depth concept modifications have been suggested:

- installation of 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.

The LPSA06 model finally resulted in a TCDF of 1,7xE-6/year.

The development of the Fire PSA was started in 2006 and finalised in 2008. The result was that the total CDF increased. The large upgrades in 2011-2013 led to a LPSA13 model, having a TCDF of 2,8xE-6/year.

In 2013 the third PSR was delivered with measures to be implemented during 2014-2017. The PSA model was adapted for the licence application: LPSA15, having a TCDF of 2.9xE-6/year. With a contribution of fire of around 40%. After implementation of all other modifications the LPAS16 model is expected to produce a TCDF of around 2.4xE-6/year.

More information about PSR related safety modifications at the NPP Borssele can be found in the CNS7-report.

Assessment of Errors of Commission (EOC):

In 1989 an IAEA IPERS/IPSART mission recommended to study EOCs. The Regulatory Body transformed this into a requirement. The Licensee contracted G. Parry (at that time NUS, now USNRC) and professor A. Mosleh (university of Maryland). This resulted in a study similar to the ATHEANA approach. Qualitative results; no direct quantitative results. For both Power POS and Low Power and Shutdown States several important EOCs could be identified

In the reports NEA/CSNI/R(98)1 (critical Operator Actions-Human Reliability Modelling and Data Issues) and NEA/CSNI/R (2000)17 (Errors of Commission in Probabilistic Safety Assessment) detailed information regarding this study can be found.

Change of Testing Strategy:

The analogue signals of the reactor protection system of the Borssele NPP form mainly a 2v3 voting system. Via transmitters and comparators the measurements are continuously checked on deviations. All 3 channels of this system were once a year sequentially tested. Borssele made a proposal to test each year only one channel (staggered testing). PSA demonstrated that changes in CDF ranged from risk neutral to risk beneficial. The reason was that the dependencies in the calibration tasks could largely be reduced by staggered testing.

Method HRA: THERP

Probability of miscalibration 1 transducer P_0 = 1E-2

Dependency of sequential calibration tasks =

- Low dependency: $(1 + 19\ P_0)/20$
- Medium dependency: $(1 + 6\ P_0\ )/7$
- High dependency: $(1 + P_0\ \ )/2$

Complete dependency: 1

- Sequential testing + hard to verify results --> high dependency. Thus, probability of dependent failure due to decolourisation of 3 or 4 transducers = $1x10^{-2}$ $((1 + 10^{-2})/2) = 5x10^{-3}$.

Resolution of Hydrogen Issue:

The PSA level-2 codes RELAP/MAAP and WAVCO (Siemens) calculations (PSA-level2) could not exclude that after core melt, despite the installed catalytic recombiners, in certain areas some small pockets of Hydrogen could be formed with a concentration near the detonation limit. Detailed CFD calculations (with RELAP/MAAP and WAVCO input) showed that active opening of the explosion windows inside the containment would prevent these pockets. Thereby, the Hydrogen issue can be resolved.

Exemption of Tech Spec:

In 2002 the reserve cooling water pump TE (see figure 1) was found to be non-available. The TE pump is a special canned pump that can operate submerged (flooding in ECCS pump room). According to the Tech. Spec. the AOT was 8 days. After that, the plant should go to a cold shutdown state. A spare TE pump was not on the shelf. Borssele made a plea for an exemption to extend the AOT time. The request was accompanied with a PSA assessment. The assessment showed that under these circumstances the cold shutdown state had a higher risk level than the Power POS.

CDF Power POS = $1.1x10^{-6}$ /year

CDF Power POS + TE unavailable = $1.6x10^{-6}$ /year

CDF Power POS + alternate pump with 10 times higher failure rate =$1.15x10^{-6}$ /year

CDF cold shutdown POS = $1.0x10^{-5}$

CDF cold shutdown + alternate pump with 10 times higher failure rate =$9.9x10^{-6}$ /year

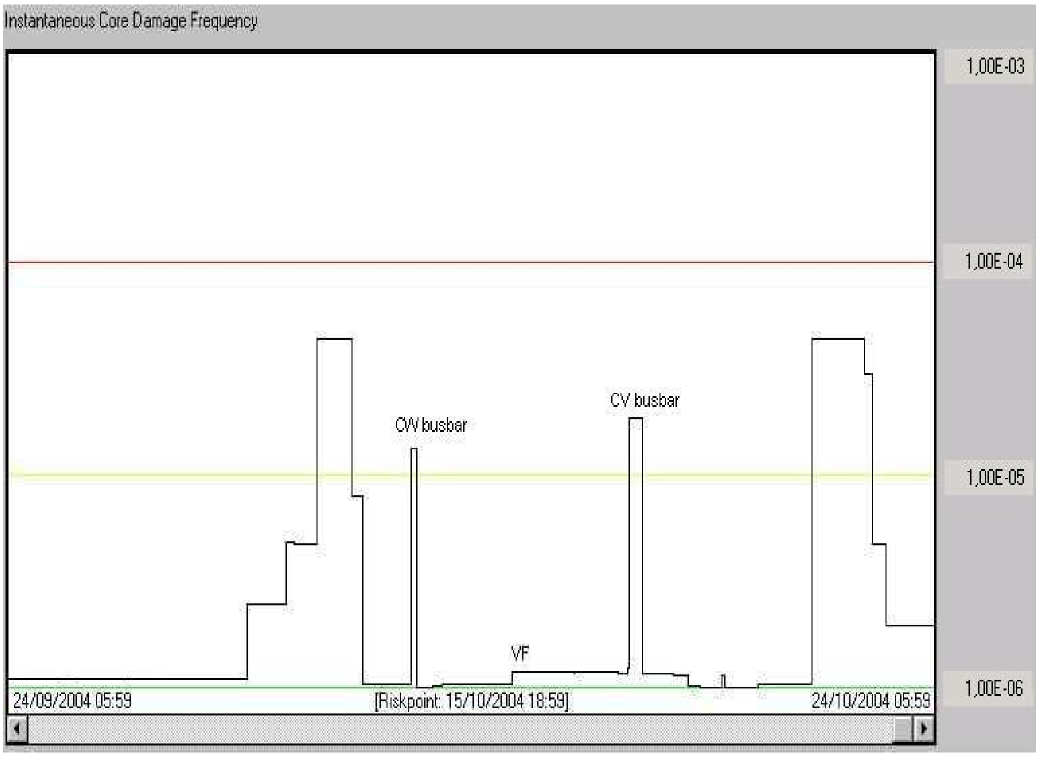
Regulatory Body agreed that Borssele didn't need to go to cold shutdown, but that an alternate spare pump should be installed in case the TE pump couldn't be repaired within the 8 days.

PSA supported SAMGs:

The level-2 PSA demonstrated that SGTR events with a dry secondary side of the SG could cause the largest source terms and thereby, a large contributor to the public health risk (Source Terms up to 50% Cs and I). The most promising strategy was the scrubbing of the source term through the water inventory in the SGs. By installing extra pathways to keep the SGs filled (including flexible hose connection with the fire-fighting system) with water a factor 14 reduction in the magnitude of the source term (CsI and CsOH) could be achieved. Although, a closer look at the MAAP4 results showed that the major effect was not the scrubbing effect, but by deposition of fission products on the primary side of the SG tubes. This deposition effect plays also a large role in other core melt scenarios such as ISLOCA.

When core damage in ATWS scenarios cannot be prevented, opening of the PORVS is suggested. Loss of primary inventory is much faster, but creation of steam bubbles will stop the fission process. Also induced SGTR is less probable because of lower primary pressure. In case induced SGTR cannot be prevented lower pressure still helps. Opening of the secondary relief valves is less probable in that case.

Risk Monitors (Outage Planning and Configuration Control): In the figure below an example is given of the result of the outage planning for the refuelling outage in 2004.



One of the main objectives for the use of the risk monitor for configuration control is to minimise the TCDF increase as a result from planned component outages by:

- mastering simultaneous component outages

- rescheduling component outages with high TCDF impact in a certain plant operating state to an operating state where the component outage has a lower impact,
- reduction of duration of the refuelling outage.
- As a decision yardstick several numerical criteria have been developed by the licensee:
- the total cumulative TCDF increase caused by planned as well as unplanned component outages < 5%
- cumulative TCDF increase caused by planned component outages < 2 %.
- instantaneous TCDF shall never exceed the value of 1x10^{-4} /year.

Optimisation of Tech Specs:

NPP Borssele has realised a project where the AOTs have been optimised. USNRC Regulatory Guide 1.177 was partly taken as a basis. Borssele has modified the numerical criteria from this guide by lowering them with a factor of 10.

For optimisation of AOTs the licensee has adopted a value of 5x10^{-8} for ΔTCDF x AOT and ΔTCDF shall always < 1x10^{-4}/year.

Apart from the PSA an expert team participated in the project to determine the maintenance times, repair times, whether or not spare parts were on the shelf, availability and duration of supply of components on the market, etc.

PSA Source Terms for off-site Emergency Planning and Preparedness:

In case a severe event occurs at the plant with a serious threat for an off-site emergency, the defined source terms in the PSA of Borssele are used as a standard source term for the prognosis.

For the definition of the planning zones for evacuation, iodine prophylaxis and sheltering the PWR-5 source term from WASH-1400 (Rasmussen Study) is still taken as the reference source term. However, the dose criteria for evacuation, iodine prophylaxis and sheltering will be lowered in the near future. As a result the planning zones would be significant larger. Therefore, a more realistic and Borssele Specific source term has been developed.

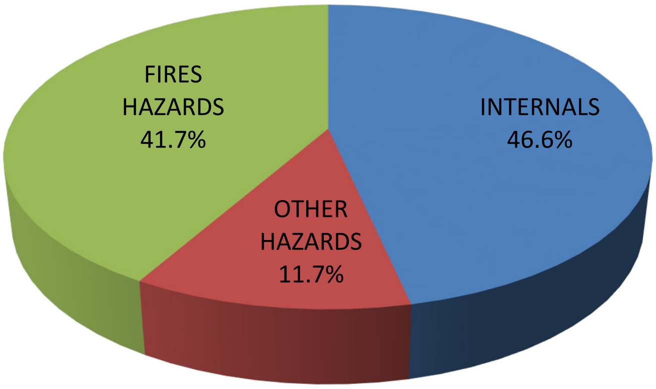
9. RESULTS AND INSIGHTS FROM THE PSAs

Borssele

The LPSA13, created after large changes recommended by the IPSART mission but without the modifications carried out in 2014-2017 based on the 3rd PSR, gives the following results for level 1:

The TCDF is 2.8 10^{-6} per year or once per 357 000 years. The internal events are responsible for 47% of the core damage and the hazards (fire and other hazards) for 53% as can be seen in the figure below. The major part of the hazards is caused by fires (42%).

TCDF: 2,8·10^{-6}



In the next figure the risk profile for all POSs is given. The risk profiles for all initiators, internal fires, and internal events are comparable and rather flat. Only the hazards have a steep risk profile, caused by 1 cut set (a drop of the TN17 spent fuel container in the spent fuel pool), which contributes nearly 75% to the CDF$_{\text{hazards}}$. As the absolute value of the hazards contribution is small (~12%) the impact on the overall risk profile is not very large.

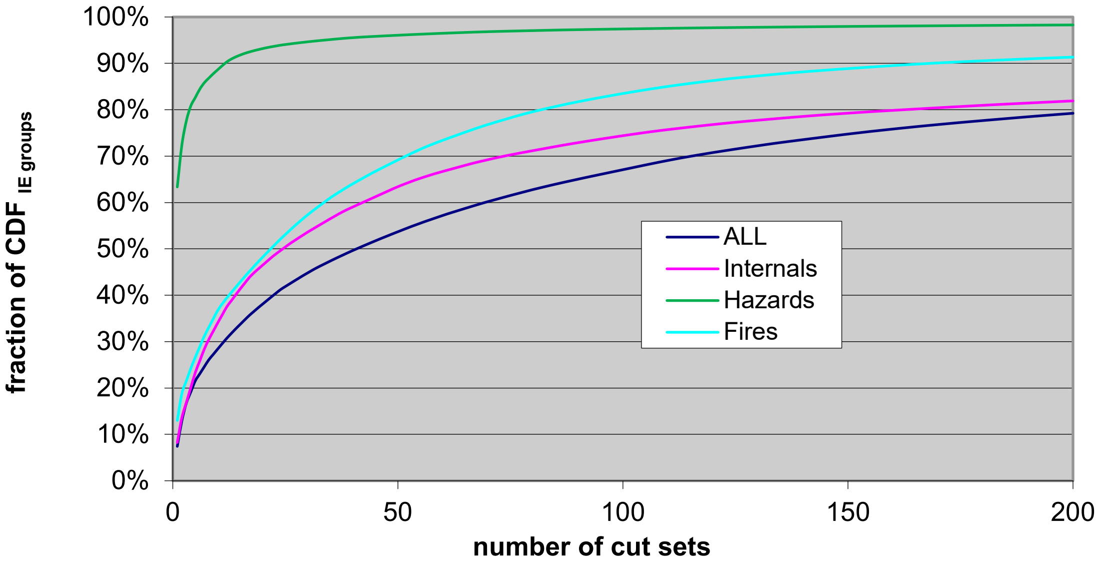


Figure: Risk profile for all initiators, internal events, hazards and internal fire

The first 100 cut sets contain 45 internal event cut sets (CDF contribution is 8.05 · 10^{-7}), 49 internal fire related cut sets (CDF contribution is 8.16 10^{-07}), and 6 hazard related cut sets (CDF contribution is 2.8 10^{-7}). The first 100 cut sets make up 67% of the TCDF.

The distribution of Plant Operational States (POSs) over the cut sets is given in the table below. The largest contribution comes from operating the reactor: POS-P. This is not a surprise as the plant is over 90% of the time in this POS. The second largest contributor is originating from the cold shutdown state (POS RE/RL). In this state the reactor is subcritical, the reactor coolant temperature is smaller than 80 °C, the reactor vessel head is closed and the loops are filled. The third largest contribution is from the plant operational state fuel pool early (POS FE). During this plant operational state the core is completely unloaded and located in the spent fuel pool.

POS	**# of cut sets**	**CDF**
Power	45	$1.3\cdot10^{-6}$
Hot Steaming	-	0
Cold shutdown	24	$3\cdot10^{-7}$
Mid-loop closed vessel	3	$2.34\cdot10^{-8}$
Mid-loop open vessel	21	$2.3\cdot10^{-7}$
Core Load/Unload	-	0
Fuel Pool Early	5	$2.9\cdot10^{-7}$
Fuel Pool Late	2	$4.5\cdot10^{-8}$

As already stated above the distribution over the initiators is rather flat. The top 10 cutsets contribute 29% of the total core damage frequency.

The biggest contribution to core damage is from Fires. Fires are typically modelled to fail all components within a fire compartment and cause additional burden to the operators in mitigation of the event. Two different fires events are found in the top 5 cutsets, one fire event in building 2 in the area connecting the bunkered system cabling to the divers systems and the other fire event in building 5 affecting electrical components.

The second biggest contributor is from loss-of-coolant accidents. 3 of the top 10 cutsets are small coolant accidents without the possibility to use the high-pressure injection system.

Other events that complete the top 10 cutsets are a heavy load drop (container) in the spent fuel pool causing leak of the spent fuel pool and coolant losses outside the reactor building. These events have in common that they are hard to mitigate as there are no systems designed to bring the lost water back to the fuel for long-term cooling.

Level 2. A breakdown of the final containment status is presented in the next figure. The following categories are chosen for this presentation:

1. Containment intact and not bypassed
2. Containment vented
3. Containment not isolated
4. Containment leak
5. Containment rupture
6. Containment bypassed

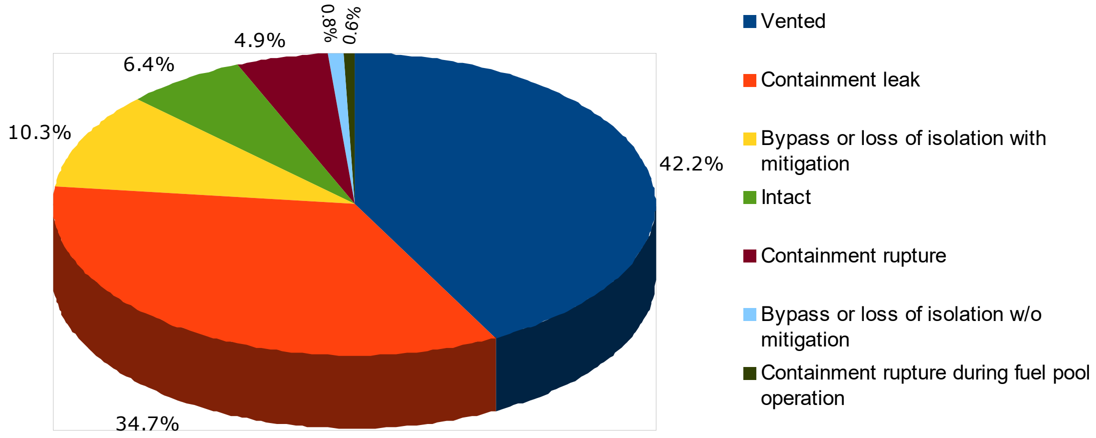


Figure: Level 2 Results: Final Containment Status as Percentage of CDF

Release via the filtered vent contribute 42.2% of the core damage frequency. Releases via the filtered vent lead to low offsite consequences. The demand for venting arises due to a high probability of the debris being non-coolable ex-vessel. This is due both to the Borssele cavity configuration which leads to a deep debris pool ex-vessel as well as the assessed probability that the operators will fail to flood the debris ex-vessel.

The next largest contribution in terms of frequency is the probability of the containment failing in leak mode, which contributes 34.7% of the core damage frequency. Leaks generally arise late in the accident sequence due to long-term combustible gas phenomena or long-term overpressurisation. Bypass releases comprise the third highest group of STCs, contributing 10.3% of the core damage frequency. Intact containment states contribute 6.4% of the core damage frequency. Containment failure in rupture mode during reactor accidents contributes 4.9% of the core damage frequency. Ruptures generally arise late in the accident sequence due to long-term combustible gas phenomena.

Unmitigated bypass or loss of containment isolation accidents represent 0.8% of the core damage frequency. These accidents may lead to offsite consequences of more than 100 fatalities. The highest contributing STCs to this category are containment not isolated, sprays failed (0.26% of core damage frequency) and induced SGTR with secondary atmospheric dump valves or safety valves stuck open (0.2% of core damage frequency).

From the actual safety report 2015 the following general PSA results can be derived, including only the modifications in the licence application.

TCDF all Plant Operating States Reactor = 2.3 E-6/year

The contribution from:

Power POS: 95.5%

Mid-loop: 4.5%

TCDF Spent Fuel Pool = 0.4 E-6/year

No emissions = 0.2 E-6/year

Total TDCF: 2.9 E-6/year

The contribution from:

Internal Events (excl. Fire): 47%

Fire internal Events: 41%

Hazards: 12 % (mainly external flooding and external gas cloud explosions/fires due to shipping accidents on adjacent river)

LPSA13 was used to identify weak points. This led to the following improvements:

Increased battery capacity

Valve control from a bunkered building

Several fire protection measures

It is expected that after inclusion of the rest of the modifications the TCDF will be around 2,4xE-6/year.

Overall the main contribution to the TCDF during the implementation of PSR is from the introduction of several mobile equipment.

HFR-results Risk Scoping Study

Prior the modifications the CDF 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/pressure side of pumps: 1.8 E-5/year (26%)

Drop of heavy load above spent fuel pool, thereby damaging primary piping below pool: 0.8E-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%)

HFR preliminary results PSA

Since L2 and L3 studies are not finished, the L1 results are preliminary and have not yet been sent to the regulator.

TCDF is now 4.6E-5/y for all POS, distributed over the following initiator groups:

Internal hazards: 97%

External hazards: 0.04%

Internal events: 1%

Irradiation facilities :2%

The contribution from Internal Hazards is dominated for almost 100% by Heavy Load Drop (HLD). The non-power Plant Operational States dominate the POS because then the heavy loads are lifted.

Protection measures against HLD are being worked out and after realisation the following picture emerges:

TCDF: 1.6E-6/y for all POS, distributed over the following initiator groups:

External hazards: 14%

Internal hazards: 1%

Internal events: 22%, subdivided in:

Transients: 14%

Support systems: 6%

LOCA: 2%

Irradiation facilities: 63%

POS At-Power dominates now with a contribution of 95%.

10. FUTURE DEVELOPMENTS AND RESEARCH

There are no research programmes or other developments foreseen for the near future.

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, 2006-2007session, 30000 No. 40, 28 September 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. US 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:

- US Nuclear Regulatory Commission, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities; NUREG/CR-6850, 2005.
- IAEA TECDOC 1151
- NVR-SSG-3 and -4.

APPENDIX: Overview of the status of PSA programmes in 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, fuel storage states	Yes + Risk Monitor	Original 1990-1994 model updates 2004, 2009, 2013, 2016	Identification of weak points; support of periodic safety reviews and associated modifications. Support of daily Operation and Risk-informed decision-making	Risk Informed Tech specs Risk Monitor Change of testing Strategy Optimisation of maintenance Prioritisation of event analyses. Development of SAMGs Outage planning Emergency planning and preparedness (source terms)
High Flux Reactor (HFR)	Research Reactor 45 MWt	Full-scope Level 1, 2, 3	Internal events Area events/ Hazards External events	All operating states for reactor (At Power and 6 LPSD), spent fuel storage (2 POSs). Sources considered: core, spent fuel, experiments, irradiation facilities	Yes	Original: Risk Scoping Study 2002-2004 Now: PSA L1 (2016) PSA L2/L3 (2017)	Periodic Safety Review, Risk Informed Decision Making, Licence requirement	Design review/ Support of back fitting and modifications, optimisation of maintenance/tech specs.

POLAND

1. INTRODUCTION

2. PSA FRAMEWORK AND ENVIRONMENT

The Polish government decided in 2009 to consider nuclear power as a possible option in the national energy strategy. Since then a considerable legal and organisational effort has been made to open the way for the possibility of building a safe nuclear power plant. New regulations have been incorporated into the Atomic Law, new Governmental acts have been accepted and Państwowa Agencja Atomistyki (PAA – Polish National Atomic Energy Agency) has been reorganised into a regulatory body.

PSA as an element of safety assessment has been included in the new regulations and PSA professionals have been trained and nw are part of the safety assessment division at PAA. A competent team in PSA is working also at NCBJ (National Center for Nuclear Research) and PAA uses the opportunities to increase its abilities in the probabilistic area.

The research reactor "Maria" at NCBJ has no PSA – the obligation to perform a PSA for every nuclear facility which has been included in the new regulations does include existing facilities.

3. SAFETY CRITERIA

Includes national/international criteria (IAEA, WENRA…)
Includes quantitative and qualitative criteria (single, multi-unit aspects)
To be structured by type of criteria
Status of criteria (mandatory, indicative..)
Includes evolutions after Fukushima (power/research reactors, SFP, site...)

Polish regulations set up safety criteria connected with probabilistic safety assessment, according to safety principles established by IAEA. There are two legal acts that include requirements on application of PSA.

The first is **"Regulation of the Council of Ministers on Nuclear Safety and Radiological Protection Requirements which must be Fulfilled by a Nuclear Facility Design"**. In the act two issues directly related to PSA can be found:

- General qualitative criteria of core damage frequency and large releases frequency for nuclear power plants and research reactors:

*"**§10**. The design of the nuclear power plant and the research reactor shall ensure the attainment of:*
1) the probability of the reactor core degradation to occur less frequently than once every 100 000 years of the reactor operation (in practice CDF<10-5);
2) the probability of releases to the surroundings of radioactive substances to occur less frequently than once every 1 000 000 years of the reactor operation, in such volumes that, beyond the limits of the restricted-use area, any of the intervention levels could be exceeded, thus requiring consideration as to whether early or long-term intervention measures should be

taken, whilst beyond the limits of the emergency planning zone the intervention level could be exceeded requiring the consideration as to whether medium-term intervention measures should be taken (in practice LRF<10-6);
3) probability of accident sequences to occur considerably less frequently than once every 1 000 000 years of reactor operation, potentially leading to the premature failure of the reactor containment or to very large releases of radioactive substances to the surroundings."

- Requirement of usage PSA in support of the safety classification of systems, structures and components of nuclear installations:

  *"**§11. 3.** The classification of nuclear facility systems and components of construction and equipment shall be performed on the basis of deterministic analyses, which are supplemented where necessary with probabilistic analyses."*

The second act, which addresses more aspects related to PSA is "**Regulation of the Council of Ministers on the Scope and Method for the Performance of Safety Analyses Prior to the Submission of an Application Requesting the Issue of a License for the Construction of a Nuclear Facility and the Scope of the Preliminary Safety Report for a Nuclear Facility**". It contains the following requirements:

- *"**§ 3.** Safety analyses shall comprise deterministic analyses and probabilistic analyses."*
- *"**§ 27. 3.** The PIEs which may lead to accidents which are more severe than design basis accidents shall be identified by combining probabilistic and deterministic methods and engineering judgment based on reasonable grounds.*

***4.** The nuclear facility accident sequences, which are more severe than design accidents, shall be defined on the basis of results of probabilistic safety assessment, as referred to in § 37–41."*

- *"**§ 32.** The criteria for acceptance of the results of deterministic safety analyses on nuclear facility accidents which are more severe than design basis accidents shall be as follows:*

2) for the extended design conditions:

b) probabilistic safety criteria for a nuclear facility, defined under §10 of the Design Regulation."

- *"**§ 37. 1.** Probabilistic safety analysis of a nuclear facility shall include the definition of all sequences of events which contribute significantly to the risk caused by a nuclear facility, the assessment of the balanced overall facility configuration design, the assessment of isolated areas of risk and the assessment of the facility design's compliance with the probabilistic safety criteria specified in § 10 of the Design Regulation.*
  ***2.** The probabilistic safety analysis shall be performed for a nuclear power plant, research reactor, isotopic enrichment plant, nuclear fuel production plant and plant for reprocessing nuclear fuel."*
- *"**§ 38.** When performing a probabilistic safety analysis of a nuclear facility:*
  1) consideration shall be given to the impact of all nuclear facility systems and components of structure and equipment in terms of their reliability in the performance of specified safety functions;
  2) the accepted levels of reliability for nuclear facility systems and components of structure and equipment shall be justified by assessments based on reliability data obtained from the operation of nuclear facilities or other data sources, analysed in a manner permitting them to be verified;
  3) consideration shall be given to possible workers errors, not only diagnostic, but also when performing control functions."
- *"**§ 39.** The probabilistic safety analysis shall be used primarily to verify the appropriate application of the principle of redundancy with regard to equipment and systems, assumed in*

the nuclear facility design, and to specify the requirement for the implementation of protective measures against the common cause failure to redundancy systems.

- *"**§ 40. 1.** The starting point of a probabilistic safety analysis of a nuclear facility shall be a complete PIE set, including both internal and external events, which may occur under all normal operational modes and lead to the release of radioactive substances from any source on the premises of the nuclear facility.*
  __2.__ An analysis shall be performed in order to identify all failure and error sequences which contribute to the risk.
  __3.__ The sequences, referred to in Section 2, shall contain:
  1) failure of nuclear facility components of structure and equipment;
  2) unavailability of nuclear facility components of structure and equipment whilst performing maintenance, repairs or tests;
  3) workers errors;
  4) failure of nuclear facility systems and components of equipment due to common cause failure;
  5) ageing of nuclear facility systems and components of structure and equipment.
  __4.__ Secondary failures, which are included in the deterministic analyses, shall be taken into account in the probabilistic safety analysis i.e. in the analysis on the sequence of events and in the analysis on nuclear facility systems."
- *"**§ 41. 1.** The probabilistic safety analysis of a nuclear facility shall be performed at the following levels:*
  1) the first level at which:
  a) the sequence of events which could lead to a failure of the following shall be defined:
  – failure of the reactor core – in the case of a nuclear power plant and research reactor,
  – failure of nuclear facility systems and components of structure and equipment containing radioactive substances of the kind and quantity such that their release to the environment could lead to a radiation hazard exceeding the criterion defined under Article 36f, Section 2, Item 1 of the Act – in the case of an isotopic enrichment plant, nuclear fuel production plant and plant for reprocessing nuclear fuel,
  b) the failure frequency shall be estimated, as referred to in Letter (a), the strengths and weaknesses of safety systems shall be assessed, as well as procedures whose purpose is the prevention of such failure,
  c) the following in particular shall be specified:
  – sequences of failures of the nuclear facility components of structure and equipment as well as workers errors, constituting the largest contribution to the failure frequency, as referred to in Letter (a),
  – safety systems which are the most important in preventing failure, as referred to in Letter (a),
  – the possibility of introducing changes in the design or operation of the nuclear facility in order to lower the risk level.
  2) the second level at which the routes of possible releases of radioactive substances to the environment from the nuclear facility shall be specified and the level of these releases and their frequency shall be estimated.
  __2.__ On the level of probabilistic safety analysis, referred to in Section 1, Item 2:
  1) the development of accident shall be examined, starting from the initiation of failure, as referred to in Item 1, Letter (a), considering the releases of radioactive substances to the environment and phenomena which could occur and lead to the failure of:
  a) the reactor containment – in the case of a nuclear power plant and research reactor,

b) the ultimate protective barrier – in the case of an isotopic enrichment plant, nuclear fuel production plant and plant for reprocessing nuclear fuel;

2) the effectiveness of solutions of the nuclear facility design shall be examined, implemented in order to limit the consequences of failures, as referred to in Item 1, Letter (a);

3) the frequency of large releases of radioactive substances to the environment shall be estimated."

The scope of the preliminary safety report for nuclear facility is also included in the regulation. A presentation of probabilistic safety assessment is addressed in a subchapter of one main chapter 7 titled "Nuclear facility safety analyses". Proposed structure of the subchapter on PSA is presented below:

*"**7.5.** Probabilistic safety analyses.*

__7.5.1.__ Brief description of the scope of probabilistic safety analyses, applied methods and obtained results.

__7.5.2.__ Quoting probabilistic safety criteria used for the purpose of nuclear facility design, in particular global criteria determined under § 10 of the Design Regulation.

__7.5.3.__ Description of the methods of probabilistic safety analyses.

__7.5.3.1.__ Modelling of accident sequences.

__7.5.3.2.__ Assessment of data and estimation of parameters.

__7.5.3.3.__ Quantification of accident scenarios.

__7.5.3.4.__ Analyses of radioactive substances releases from the containment.

__7.5.4.__ Description of the results of the probabilistic safety analysis and conclusions.

__7.5.4.1.__ Description summing up the results of the probabilistic safety analysis (with reference to the complete probabilistic safety analysis study concerning the facility, documented in the form of a separate report), containing quantity risk measures for those aspects of design solutions and facility operation which contribute the most in terms of risk.

__7.5.4.2.__ Comparison of results obtained from the probabilistic safety analysis with the probabilistic safety criteria, defined under § 10 of the Design Regulation and the formulation of unequivocal conclusions concerning the fulfilment of these criteria."

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

As no nuclear power plant exists in Poland, no PSA studies have been performed related to nuclear facilities. A PSA of the Polish research reactor "MARIA" has not been performed yet (the above-mentioned regulations do not apply to nuclear facilities under operation on the day of their entry into force).

However, in preparation for the safety assessment of the future Polish NPP, PAA decided to perform some work in order to obtain competence and experience in the field of probabilistic safety assessment. In the last 3, 4 years a number of projects related to PSA have been done in co-operation with the National Centre of Nuclear Research as follows:

- "Application of Probabilistic Safety Assessment in Establishing Safety Requirements for a Nuclear Power Plant."
- "Evaluation of computer programs for fault tree analysis for PSA studies"
- "Tutorial for using SAPHIRE"
- "Assessment of computer tools dedicated for performing PSA for NPPs."

- “Preliminary data input for the SAPHIRE v.8 programme together with example analysis.”
- “Methodology of including human reliability analysis into PSA.”
- “Reliability Analysis of Selected Safety Systems in PWR.”
- “Methodology of the Fire PSA for NPPs.”
- Methodology of including HRA in PSA studies

Two following studies are under elaboration:

- “Methodology of Probabilistic Safety Assessment on level 2.”
- “Methodology of Probabilistic Safety Assessment for spent fuel pool in NPP.”

5. PSA METHODOLOGY AND DATA

PSA methodology is under development. Data for example calculations is limited to data publicly available.

National Centre for Nuclear Research (NCBJ) is involved in the development of PSA methods with particular emphasis on:

- external events and their combination and correlation,
- application of extreme value theory for asssessing extreme rare events important for the safety of NPP,
- time-dependent PSA, in particular for power supply subsystems of NPP,
- fire PSA,
- level 2 PSA for spent fuel pool.

6. NOTABLE RESULTS OF PSAs

PSAs are partial and limited mainly to training applications. However, as the National Centre for Nuclear Research is one of the consortium partners of the ASAMPSA project, some notable results will be available.

A short description is given in section 9.

7. PSA APPLICATIONS AND DECISION MAKING

NCBJ has proposed an implementation of the IRIDM approach by using the technique known as Value Tree Analysis : M. Borysiewicz, K. Kowal, S. Potempski, “An application of the value tree analysis methodology within the integrated risk-informed decision making for the nuclear facilities”

Reliability Engineering & System Safety Vol. 139 No 7 (2015) 113-119.

8. FUTURE DEVELOPMENTS AND RESEARCH

NCBJ plans to participate in the new EU project aiming at the development of methodology for multi-natural hazard and combined hazard scenarios, using the approach based on vector-values fragility functions and Bayesian Belief network.

9. INTERNATIONAL ACTIVITIES

NCBJ takes part in the EU project: ASAMPSA_E Advanced Safety Assessment : Extended PSA

The main topic is: Consequences of Combination of Extreme External Events on the Safety of Nuclear Power Plants (NPPs).

The project ASAMPSA_E aims at identifying good practices for the identification of such situations with the help of Level 1-Level 2 PSA and for the definition of appropriate criteria for decision making in the European context. It offers a new framework to discuss, at a technical level, how extended PSA can be developed efficiently and be used to verify if the robustness of NPPs in their environment is sufficient. It will allow exchanges on the feasibility of "extended PSAs" able to quantify risks induced by NPPs site (multi-units reactors and spent fuel pools, modelling impact of internal initiating events, internal and external hazards on equipment and human recovery actions).

A series of reports is under preparation and will be finalised by the end of 2016.

SLOVAK REPUBLIC

1. INTRODUCTION

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 2017 and 2018.

2. PSA FRAMEWORK AND ENVIRONMENT

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 the Slovak Republic. 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 PSAs for the Slovak plant are performed by RELKO Ltd. and VUJE, Inc. UJD SR performs review of the PSA studies. In addition, independent review is performed by the experts of IAEA or foreign PSA organisations.

3. NUMERICAL SAFETY CRITERIA

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 ≤ 1.0E-4/y resp. LERF ≤ 1.0E-5/y. The safety goal for new plants is CDF ≤ 1.0E-5/y resp. LERF ≤ 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 AND SCOPE OF ONGOING PSA STUDIES

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 (including the spent fuel pool). In addition, extreme external events (as seismic event, non-seismic natural and man-made events) 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 status of PSA for the Slovak operating plants is as follows:

- The J. Bohunice V2 NPP (Unit 3 and 4): Level 1 and level 2 full power, low power and shutdown PSA is performed for the plant, including internal and external events (seismic and non-seismic natural and man-made events).
- The Mochovce NPP (Unit 1 and 2): Level 1 and level 2 full power, low power and shutdown PSA is performed for the plant, including internal and external events (seismic and non-seismic natural and man-made events). At the present time the PSA of external events is being upgraded. The non-seismic external event PSA will be finished in 2018, the seismic PSA in 2019.

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 MW x 1.07 = 1 471.3 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%.

The PSA studies were updated for the plants for the use of the new fuel Gd2 with increased average enrichment of 4.87%. The efficiency of utilisation of the fuel is decreased after power uprate of the plants to 107% of the nominal power and without change of the average enrichment (4.25%) at the maintaining the length of the campaign with about 330 effective days. For changing this situation it is required to use the fuel with increased initial average enrichment (4.87%). Such solution increases the burn-up of U-235 in the fuel and extends the fuel cycle from 4.5 years nearly to 6 years. Direct consequence of the increased enrichment is that fewer fuel assemblies are changed annually; therefore, the number of the spent fuel assemblies for storage is decreased.

The fuel with average enrichment of 4.87% is used in the reactors of both units of the V2 NPP and both units of the Mochovce NPP. This fuel increases the amount of decay heat and has changed the structure of the source term. The maximum burn-up of fuel assemblies at the end of the cycle is increased from about 52 MWd/kgU (fuel 4.25%) to about 64 MWd/kgU (fuel 4.87%). Therefore, it was necessary to evaluate its impact on the results of the level 1 and level 2 PSA. The level 1 and 2 PSA for the new fuel was already updated for the V2 NPP and also for the Mochovce plant. The increased enrichment of the fuel has not significant impact on the CDF and the LERF. There is also no significant impact on the dominant initiating events, dominant accidents sequences with greatest contribution to the CDF and LERF.

The PSA studies for both plants have involved the severe accident management systems and guidelines. The following systems were implemented during the last years for the purpose of severe accident management in both plants:

- Reactor coolant system (RCS) depressurisation,
- emergency water source for water injection into RCS, spent fuel storage pool and spraying of confinement,
- emergency power supply,
- flooding of reactor cavity for external cooling of reactor pressure vessel (RPV),
- vacuum breaker of containment,
- hydrogen management in containment,
- long-term heat removal from containment.

The PSA studies have involved also safety measures implemented after the Fukushima accident and the stress tests performed in the EU member countries.

In addition, PSA is used to support the decommissioning of the A1 and V1 plants on J. Bohunice site and the construction of the unit 3 and 4 on the Mochovce site.

5. METHODOLOGY AND DATA

The regulatory authority issued a guidance for requirements for PSA studies (BNS I.4.2). The guidance is not intended to be a procedural guide for performing a PSA. Such procedures have been developed by IAEA and other organisations. 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.

The IAEA safety guides and US PSA standards and NUREGs are used to develop the plant-specific PSA models.

The responses of the plant to the initiating events of the accident are modelled in the PSA. The initiating events under consideration are those internal and external events that could lead in combination with the safety system failures to the core damage and release of radioactive materials to the environment. The PSA studies include loss-of-coolant accidents (LOCAs), transients, internal fires and floods as the internal initiators. In addition, the following external initiators are analysed: seismic event, aircraft crash, extreme meteorological conditions and influence of surrounding industry to the plant operation. Also the heavy load drop is considered for the shutdown operating modes.

The accident sequences have been modelled using event trees, where the consequences have been identified in dependence on the success or failure of safety systems after occurrence of the initiating event. The consequences are concerning the core damage for the level 1 PSA and the source term categories for the level 2 PSA.

The reliability of the front-line and support systems is calculated using the fault tree methodology. The dependent and independent component failures, pre- and post-accident human errors, unavailability for maintenance and testing are considered in the analysis. The 24 h mission time is used in the evaluation of the post-accident reliability of the systems in the level 1 PSA and 48 h in the level 2 PSA.

Due to extensive changes in plant configuration during a shutdown period, plant operational states (POS) are defined which properly reflect the plant configuration during an outage evolution. The POS is used to define boundary conditions within which there would be no changes in major characteristics which are important for PSA modelling. A typical number of POSs considered in the PSA for the Slovak NPPs is about 12 to 15. It should be noted that the scope and objectives of a PSA have a dominant effect on the selection of the POSs.

The RISK SPECTRUM PSA code is used to develop the level 1 and 2 PSA models. The small event tree and large fault tree approach is applied.

Plant-specific data are used in the Slovak PSA models. Data collection is performed using the DATAFARM database which was developed by RELKO in 2005. Initiating event frequencies and component failure rates are calculated based on the data from:

- the J. Bohunice V1 NPP (for time period 1978 - 2008),
- the J. Bohunice V2 NPP (for time period 1985 - 2015) and
- the Mochovce NPP (for the time period 1998 - 2015).

The database was developed using the approach adopted from NUREG/CR-6823: Parameter Estimation for PSA, Sandia National Laboratories, September 2003.

6. NOTABLE RESULTS OF PSAs

The Level 1 PSA has shown us that implementation of automatic start of low pressure safety injection pumps during shutdown operation modes significantly decreases the shutdown risk. At the present time, after implementation of this change, the shutdown risk is lower than the full power risk. Before implementation of the change the shutdown risk was higher.

Given implementation of severe accident management (SAM) systems the total core damage frequency is decreased by a factor of 4.4.

Implementation of SAM systems significantly decreased the LERF and the probability that the containment remains intact during a severe accident.

7. PSA APPLICATIONS AND DECISION MAKING

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 used.

The risk monitors

The status of risk monitors for the Slovak plants is as follows:

The J. Bohunice V2 NPP (Unit 3 and 4): Level 1 and level 2 full power, low power and shutdown EOOS (Equipment Out Of Service – product of EPRI, United States) risk monitor was developed to monitor the CDF and LERF. The monitor was used to evaluate the risk profile for the plant in operation and for preventive maintenance planning. At the present time the RiskWatcher software is used for risk monitoring.

The Mochovce NPP (Unit 1 and 2): Level 1 and level 2 full power, low power and shutdown safety monitor (Safety Monitor – product of Scientech, United States) was developed to monitor the CDF and LERF. The monitor was used to evaluate the risk profile of the plant in operation and for preventive maintenance planning. At the present time the RiskWatcher software is used for risk monitoring.

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 prioritise areas for safety improvement and to support the regulatory work.

Other applications:

- improving safety of the plants
- optimisation of the technical specification,
- implementation of the reliability-centred maintenance,
- in-service inspection, etc.

8. FUTURE DEVELOPMENT AND RESEARCH

High cost of long outages caused that preventive maintenance activities during refuelling were changed in the plants of EU and US to online 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, online 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 online preventive maintenance. For this purpose the methodology will be developed in the future and it will be applied for the plants.

At the present time the research activities are also focused on the level 3 PSA.

9. INTERNATIONAL ACTIVITIES

RELKO Ltd has a closed co-operation with IAEA in PSA training courses. During the last years the RELKO team had lectured PSA training courses organised by IAEA in Argonne National Laboratory (Chicago, IL, United States), Abdus Salaam International centre for Theoretical Physics (Trieste Italy), Malaysia, Viet Nam and Jordan to support experts from developing countries.

SLOVENIA

1. INTRODUCTION

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 programme, modernisation in the year 2000 when the steam generators were replaced, and reactor power uprated, fire protection action plan implementation, seismic hazard re-evaluation) since then. The PSA model update is preformed once every fuel cycle to reflect plant configuration and SSC 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. The last review of the Krško NPP PSA was done as a part of the second PSR between 2010 and 2012.

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 online 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 an 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 is 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 online 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 PROGRAMMES

Historical development

The development of the PSA started in Slovenia in 1991 with the issuance of a SNSA decree, which required from the Krško NPP to develop the PSA for all plant states of operation. The KRŠKO NPP PSA model was originally developed along the KRŠKO NPP IPE/IPEEE project (1994 – 1995). Since then the PSA model has undergone various revisions to reflect plant configuration changes. The model has also undergone various peer reviews by IAEA IPERS and IAEA IPSART missions. The last review was preformed within the scope of the second 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. Since 2010 the Krško PSA 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 implemented in 1999, which helped reduce risk by more than 85%. In 2004 the seismic hazard re-evaluation was conducted, based on which the risk was reduced by more than 50%. Another major risk reduction was done by the installation of the 3rd EDG in 2012, which contributed to around 30% additional total risk reduction.

The Krško NPP also uses PSA for evaluating and scheduling the online maintenance of equipment, technical specification optimisation, plant modernisation 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.

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 categorise all "internal" initiating events on the basis of similar transient progression or consequences. Next, the initiating event categories were grouped into three categories, LOCAs, transients and special initiating events. LOCAs include all accidents that result in a reduction of primary coolant system water inventory.

The category was divided into three subcategories: leak to the secondary system (SGTR), leak that bypasses the containment (interfacing system LOCA), and leaks within the containment (which was further subdivided based on the size of the break). In order to determine the specific events modelled for the transients and special initiating events, the Krško's systems were reviewed to determine if the failure of the system could result in a reactor trip, the Krško's operational data were reviewed and compared to similar plants, and the initiators provided in NUREG/CR-3862 were reviewed for applicability. The transient initiators were than grouped into categories based on plant response, signal actuation, systems required for mitigation, and subsequent plant related effects.

Common Cause Failure (CCF)

In the Krško NPP IPE PSA the failures of equipment due to common causes were represented in the fault trees explicitly by means of basic events. Two types of modelling of CCFs were distinguished:

- The modelling of CCF of two components in IPE PSA was done in a way to define separate basic events for each group of two components susceptible to CCF. For quantification of CCF of two components beta-method was used and a representative basic event was quantified accordingly.
- The 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-modelling of the existing CCF representation in the Krško NPP baseline PSA was performed by employing (RiskSpectrum) built-in CCF modelling capabilities. The focus of the work done was on re-modelling CCFs involving two components. For each two-component CCFs the components to which CCF basic event relates were determined. Respective individual failure basic events were determined. Individual failure basic events identified were sorted into RS CCF groups. Re-modelling was performed. Existing CCF basic events were removed from a FT structure, together with associated parameters and notes describing them. New RS parameters representing beta factors were defined and appropriate notes were added in a RS model. New CCF groups were defined instead using beta factors from the Krško NPP IPE CCF Notebook.

Human Reliability Analysis (HRA)

The HRA was based on the THERP (Technique for Human Error Rate Prediction) methodology described in the NUREG/CR 1278 and Westinghouse RMOI HRA Guidelines. The HRA consists of delineating the procedural steps which are absolutely necessary for successfully completing the task for a given event, modelling the task in failure configuration, and deducing the probability that the operating crew will fail to complete the task.

Data analysis and Master Data Bank

Plant data are collected, organised, 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 organised effort is performed 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 overpressurisation 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 and Small Leaks),
- Loss of offsite power (LOOP) events

The event tree structures in the PSSA are developed based on the Krško shutdown operational procedures. At least one event tree (represented by a Group Variable) exists for each initiating event modelled in the Krško PSSA. Although each initiating event is treated separately, the mitigative responses are similar among many of the initiators, which in turn, create similar event tree structures.

6. 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 online 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 summarised 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 behaviour, 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 authorisation 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.

7. RESULTS AND INSIGHTS FROM THE PSAs

Results and insights are based on the valid NEK PSA model “NEKC28DU” 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	1.24E-5	3.86E-7
Seismic events	1.11E-5	1.28E-6
Internal fires	1.26E-5	1.72E-8
Internal floods	4.87E-6	5.41E-9
HELB	1,39E-6	1,61E-9
Other external events	3.73E-6	3.03E-8
Total	**4.61E-5**	**1.72E-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 [/yr]
1	Core recovered in-vessel, no containment failure	4.30e-8
2	No containment failure	9.19E-6
3A	Late containment failure, no molten core-concrete attack	0.00E-0
3B	Late containment failure, molten core-concrete attack	0.00E-0
4	Basemat penetration (no overpressure failure)	1.86E-6
5A	Intermediate containment failure, no molten core-concrete attack	0.00E-0
5B	Intermediate containment failure, molten core-concrete attack	0.00E-0
6	Early containment failure	3.22E-7
7A	Isolation failure, no molten core-concrete attack	5.34E-7
7B	Isolation failure, molten core-concrete attack	3.71E-7
8A	Bypass, scrubbed	3.59E-7
8B	Bypass, unscrubbed	1.33E-7
3AV	Late containment venting (after 24 hours); no MCCI[11]	6.88E-7
3BV	Late containment venting (after 24 hours); with MCCI	1.14E-5
5AV	Intermediate containment venting (before 24 hours); no MCCI	1.69E-5

[11] MCCI: Molten Core Concrete Interaction

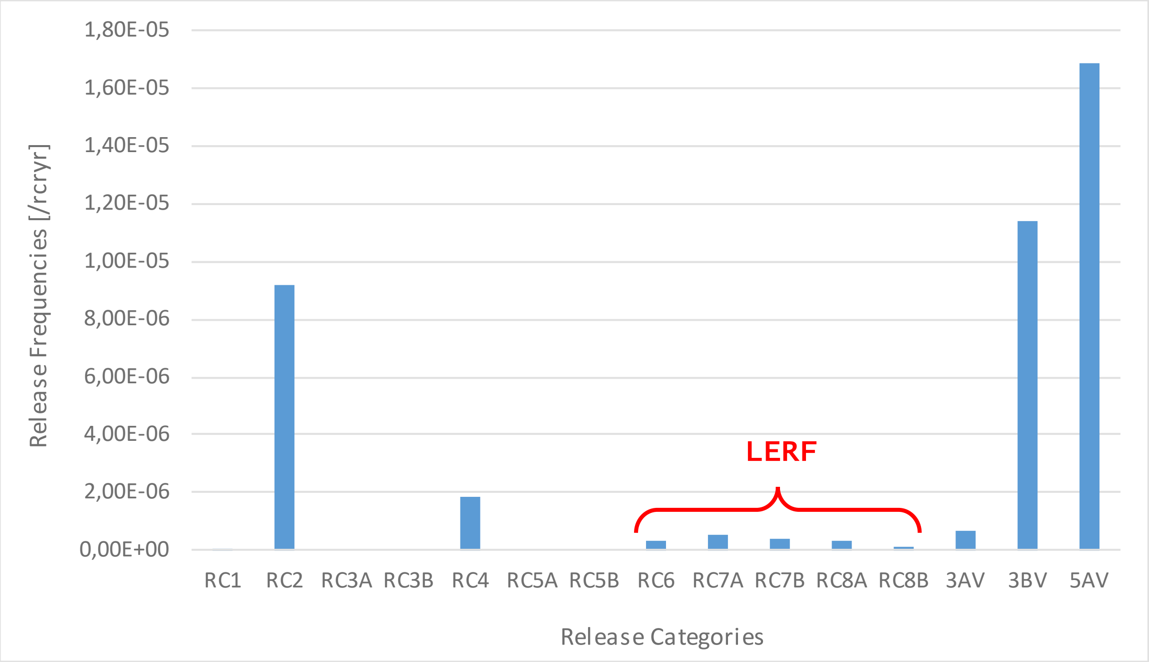


Figure 1: The distribution of releases by release categories and their frequencies

Important sequences

The event trees representing the plant response to Internal Initiating Events in the Baseline of the Krško NPP PSA Model "NEKC28DU" contain 176 event sequences that lead to core damage. The most important sequences are: Loss of Component Cooling ($1.52\cdot10^{-6}$ /rcryr), Medium Size LOCA ($1.39\cdot10^{-6}$ /rcryr) and Transient without MFW Available ($1.01\cdot10^{-6}$ /rcryr). There are 4 sequences, which have frequency above the value of 10^{-6} /rcryr. They contribute roughly 40% 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 Loss of Component Cooling (CCW), Medium Size LOCA and Small Break LOCA (SLO). These three categories contribute cumulatively somewhat around 64% 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 Component Cooling System (CCW and Essential Service Water System (ESW), DC panels, Refueling Water Storage Tank (RWST) and 6 kW AC buses.

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 component cooling pumps group. Risk Increase Factor has the largest impact on Motor Operated Valves, Air Operated Valves and Human-Errors groups.);

- Unavailability of Equipment Due to Preventive Online 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 $1{\cdot}10^{-10}$/rcryr for the quantification of IIE CDF had been set appropriately);
- Impact of change in Reactor Containment Fan Coolers success criterion (Level 2);

2004 Seismic PSA

Results

A result of the 2004 seismic PSA study was a significant reduction in the seismic CDF by more than 50%. The CDF has decreased due to new equipment added to enhance safety, addition to the model of some systems previously assumed to be unavailable after a seismic event, and removal of some conservatism in the plant model and data.

Importance Analyses

Importance analyses were preformed in the 2004 seismic PSA study to identify the dominant contributors to seismic CDF. The importance was expressed as the change in CDF when the event was removed from the analysis. The most significant seismic initiating events are seismic loss of off-site power (33.3% change in CDF), seismic station blackout (19.3% change in CDF) and seismic ATWS (14.4% change in CDF). The most important seismic failure events are due to seismic failure of the condensate storage tank (24.2% change in CDF), relay chattering of CC and SW pumps (8.1%) and seismic failure of diesel generator control panels (6.7% change in CDF). Importance of the operator’s actions (fail to switch valve alignment from the condensate storage tank to essential service water brings 14.8% change in CDF) were estimated as well.

Sensitivity Studies

Sensitivity studies indicating the value of further plant modifications were performed in the 2004 seismic PSA study. Modifications like additional third independent full size diesel generator, incorporation of existing small portable diesel generator (DG) to the power positive displacement pump and battery charger, implementation of backup to existing condensate storage tank (CST), addition of nitrogen tanks for operation of pressurizer power operated relief valves and implementation of backup to the existing essential service water (ESW) system, were evaluated. It was evaluated that especially the addition of third large 6.3kV DG (52%) or incorporation of the existing small portable diesel generator would significantly reduce the seismic risk.

Uncertainty Analysis

Uncertainty analyses in the 2004 seismic PSA study were preformed with the combination of uncertainty in the seismic hazard, the fragilities, random failure and human reliability. The predicted seismic CDF was based on the mean seismic curve and mean seismic fragility curves for systems, structures and components. The predicted seismic CDF increased by about 24% if also uncertainty in random failures and human error probability were included. Uncertainty in the seismic hazard and fragility was determined to have a bigger effect than uncertainty in random failure and human reliability.

Summary of main improvements impaired by risk analysis

Improvements based on risk analysis were:

- Internal Events:
    - Modification of air supply for Air Operated Valves 14500 and 14501;
    - Separation of Instrument Air Supply for Pressurizer Relief Valves;
- Seismic PSA study:
    - Installation of the third safety-related emergency diesel generator;
    - 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 0.3 g;
    - Improvement of support points and fixing places for different equipment;
    - Improvements in reducing possibility for equipment interactions as a consequence of a seismic event;
- Internal Fire:
    - Modification packages to install fire (smoke) detectors in following areas:
        - Radwaste Building;
        - Auxiliary Building Safety Room Pumps;
        - CC Building pump area, chiller area and HVAC area;
        - Fuel Handling Building;
        - ESW Pumphouse;
        - Main Control Room Panels;
        - IB AFW area and compressor room;
    - Installation of emergency lightning in some areas;
    - Improvement of the Krško NPP Fire Brigade efficiency to:
        - Train Fire Brigade members about the Krško NPP systems and operations;
        - Associate field operators to the Fire Brigade Team;
        - Supplement the Fire Brigade Rooms with Fire Announciator;
    - Implementation and sealing of fire barrier penetrations;
    - Improvement of fire doors between fire areas;

Level 2:

- RX Vessel Cavity; Level 2 PSA results showed important impact due to changing “dry cavity” into “wet cavity” on containment response and on core damage and fission products release out of containment. The Krško NPP performed the analysis and changed the design in accordance with its results.

- Accident management; By using PSA results, the dominant core damage sequences were identified. Response of containment and containment systems to each of these CD sequences was then evaluated. Actions for reducing the phenomenon and undesired consequences propagation were set up in Severe Accident Management Guidelines for the Krško NPP (SAMGs). This represents a direct PSA application.

8. 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:

- the plant is developing a PSA model for the spent fuel pool,
- the plant is also developing a shutdown PSA according to newest standards,
- 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.

References

[1] Evaluation of New RS PSAP NEK Baseline Model “NEKC28DU”, NEK ESD-TR-08/16, 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: Overview of the Status of PSA Programmes in Slovenia

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/ revision***	***Reason for carrying out PSA***	***PSA applications***
Krško	2 loop PWR Westinghouse	Level 1 & 2 full power Level 1 for shutdown	Full scope All internal and external events	Full power and shutdown	Yes updated every 18 months	Original: 1992 Revised: Living PSA	Regulatory requirements	Design review, Risk Monitor, PSA-based event analysis, OLM

SPAIN

1. INTRODUCTION

2. PSA FRAMEWORK AND ENVIRONMENT

PSA development started in Spain in 1986. The general driving document of PSA activities at the time was the “Integrated Program on Performance and Use of PSA in Spain” (IP), released by CSN that year. Both Regulatory Body (CSN) and Utilities used that document to carry out the PSA developments in the eighties and nineties. The IP on PSA was revised in 1998, when CSN issued its second edition.

In the years of experience with the first edition of the IP, the activities in the country went more along the line of PSA development, following the first of the objectives indicated in its title. The activities in relation with the second main objective, namely the use of PSA, were 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. This edition also included the CSN activities on PSA review and acceptance and established the need of utility activities to revise and update the previous PSA projects. The second edition also discussed the activities to reach a final and common scope for 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 thoroughly reviewed by the CSN.

Finally, as part of the Spanish Action Plan in the framework of the WENRA Reactor Harmonisation Working Group (RHWG), CSN developed a legal framework for covering PSA Program. Thus, 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”.

This Instruction is directed to Nuclear Power Plant (NPP) licensees, who must perform a PSA in order to verify that all potential risk scenarios have been properly considered for nuclear safety. The Instruction establishes the final scope for each specific NPP PSA, which must include level 1 and level 2, considering all operational states with fuel in the vessel and in the spent fuel pool and all relevant internal and external initiating events (fires and floods). Regarding external hazards, other methodologies, different to PSA, can be used in order to evaluate their impact in risk.

The Instruction also requires the PSA to be updated by the licensee after every refuelling outage so that the PSA model reflects a realistic modelling of plant response. 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, probability and availability parameters for the events included in the PSA models.

Finally, the instruction establishes bases for PSA applications and general criteria for PSA quality to be used for regulatory applications.

As a part of their safety management, the Spanish NPP licensees also have to update their PSA in order to incorporate new insights important to safety and reassess risk. The

Periodical Safety Review (PSR) required for operation permit renewal every ten years includes the PSA updating; in this context all the Spanish NPPs are required not only to update data and design modifications but also to incorporate methodological improvements.

In addition to the mandatory Instruction, two guides have been issued by CSN:

1. Guide GS 1.15: “PSA Actualization and Maintenance”, focused on the updating process for PSAs (frequency and scope);
2. GS 1.14 “Basic criteria for carrying out PSA Applications” focused on the process for PSA regulatory applications.

In the framework described above, utilities have been developing PSAs for the Spanish NPPs for their own use in different regulatory processes and activities. Some of those processes are compulsory, as is the case of maintenance rule, risk monitor, or Technical Specifications improvement. In other cases, utilities are making use of PSAs in a voluntary manner in regulatory processes such as risk-informed in-service inspection, or NFPA 805 transition. It is also important to mention other processes as training where utilities use the PSAs as a source of knowledge.

At the same time, CSN is making use of these PSA models (developed by utilities) in order to set up a risk-informed oversight system. The use of PSA in this context is aimed, for example, at prioritising system and component inspections or quantifying the risk from inspection findings.

Within the Spanish Regulatory Oversight system, SISC by its acronym in Spanish, PSAs are used to calculate a performance indicator measuring the approximate impact in core damage frequency arising from equipment failures and unavailability.

There have not been changes related PSA activities in Spain after the Fukushima event.

3. SAFETY CRITERIA

No quantitative safety guidelines or numerical goals have been officially used in Spain. PSA results within the usual range of published results all over the world are considered acceptable and, in many cases, values outside this range have led to plant modifications.

Of course, international nuclear safety objectives as those established by European Commission or IAEA in Safety Guides are goals to achieve.

Nevertheless, since several PSA applications need 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, quantitative goals are established similarly to those of the USNRC RG guide 1.174 “An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis”.

Lack of numerical goals results also in lack of criteria to account for single or multi-unit aspects. However, after Fukushima, nuclear safety objectives require taking into account all sources of risk in the site (including spent fuel storage) and the use of shared equipment for several units.

In Spain, NPPs with shared equipment have included models for quantifying risk from this equipment only at individual unit level. No quantification of risk per site has been performed.

4. STATUS AND SCOPE OF ONGOING PSA STUDIES

According to the IS 25 Instruction, the common scope to be achieved by the Spanish NPP PSAs has been Level 1 and 2 analyses, including all reactor operating modes (power operation, low power operation and shutdown), for internal events as well as fires and internal floods and including the spent fuel pool in the analysis. Currently, all NPP operators have programmes in order to develop and complete these analyses.

Regarding external hazards (earthquake, winds, external floods, etc.), PSA have not been required and utilities are allowed to use alternative methodologies. Quantitative risk analysis is not a requirement for external hazards.

Current status can be summarised as follows:

Spanish nuclear fleet currently comprises 5 sites with a total 7 operating units plus a site with a unit in shutdown with all the fuel in the spent fuel pool. For each of these NPPs there is a specific PSA.

After Fukushima, most PSA activities in Spanish NPPs oriented to get the full PSA scope have focused on developing level 2 analyses at low power and on completing the spent fuel pool analysis. Level 2 PSA at low power and shutdown was required by the CSN before the end of 2014 as part of Fukushima requirements in order to acquire knowledge for the development severe accident management guidelines in low power and shutdown states.

The following list identifies, for each NPP, the PSAs being maintained and the scope achieved at present:

- Trillo Nuclear Power Plant (KWU-3 loops):

  Level-1 PSA of internal events at power, low power, shutdown and spent fuel pool.

  Level-1 PSA of internal flooding at power.

  Level-1 PSA of internal fires at power.

  Level-2 PSA of internal events at power, low power and shutdown.

- Vandellós II Nuclear Power Plant (Westinghouse-3 loops):

Level-1 PSA of internal events at power, low power, shutdown and spent fuel pool.

Level-1 PSA of internal flooding at power.

Level-1 PSA of internal fires at power.

Level-2 PSA of internal events at power, low power and shutdown.

- Cofrentes Nuclear Power Plant (GE-BWR6).

Level-1 PSA of internal events at power, low power, shutdown and spent fuel pool.

Level-1 PSA of internal flooding at power.

Level-1 PSA of internal fires at power.

Level-2 PSA of internal events at power, low power, shutdown.

Level-2 PSA of internal flooding at power.

- Ascó Nuclear Power Plant (Westinghouse-3 loops, 2 units):

Level-1 PSA of internal events at power, low power, shutdown and spent fuel pool.

Level-1 PSA of internal flooding at power, low power and shutdown.

Level-1 PSA of internal fires at power.

Level-2 PSA of internal events at power low power and shutdown.

Level-2 PSA of internal fires at power.

- Almaraz Nuclear Power Plant (Westinghouse-3 loops, 2 units).

Level-1 PSA of internal events at power, low power, shutdown and spent fuel pool.

Level-1 PSA of internal flooding at power.

Level-1 PSA of internal fires at power.

Level-2 PSA of internal events at power low power and shutdown.

Level-2 PSA of internal fires at power.

- Santa María de Garoña Nuclear Power Plant (GE-BWR3). Currently in shutdown:

Level-1 PSA of internal events at power, low power and shutdown and spent fuel pool.

Level-1 PSA of internal flooding at power.

Level-1 PSA of internal fires at power.

Level-2 PSA of internal events at power.

As indicated before, PSA has not been required for external hazards. Instead, Individual Plant Examinations for External Events (IPEEE) were completed for all NPP. They were oriented towards the identification of plant vulnerabilities to external hazards like high winds, external floods or extreme temperatures. With regard to seismic hazards, in accordance with the seismic margin methodologies applied (EPRI and USNRC), 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

5. PSA METHODOLOGY AND DATA

Licensees developed PSAs during the nineties under very detailed procedures and thoroughly reviewed by CSN staff but there was no standard for carrying them out. Therefore, PSAs have a wide variability on their hypothesis and support calculations for success criteria, even if they have similar level of detail and use similar methodologies. Currently, CSN is working to get a comparison against ASME/ANS RA-Sa-2009. “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plants Applications”.

The risk measures chosen for PSA results are Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) in all cases, but usually there is no full aggregation of results coming from different models (i.e. CDF from fires and floods is not added to CDF from other internals events).

After Fukushima there has not been a change in models, risk measures or risk aggregations. The only change implemented in PSAs is that related to models for the recovery of external power, which have been adapted to new sources of external AC power, also taking into account the time involved in the recovery.

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.

For data analysis, PSAs use following methodologies:

- Initiating event frequencies: Some of them are generic (LOCA, SGTR, etc.); plant-specific events are based in specific fault tree models (Loss of instrument air systems, ISLOCA, etc.) and plant-specific data are used for frequent events (turbine trip, loss of outside power, etc.). In some cases, Bayesian analysis with plant-specific and generic data is used when the feedback from plant experience is not enough.
- Unavailability of components, trains or systems (planned or unplanned) is based on plant-specific data and operating experience.
- Plant-specific failure data are collected for most of the components and used for estimation of component failure rates. In those cases where plant-specific data are not enough, Bayesian analysis of plant-specific data with generic databases is used. Spanish NPP have generated a generic database that collects information mainly from NUREG/CR 6928, to be used for components with scarce plant-specific data. However, very few component failure rates are taken from this generic database.
- The CCF-modelling is based on the use of Alpha factors and generic CCF-parameter data. However, NPPs analyse collected data looking for common-cause failures.

Related to Human Reliability Analyses (HRA), Spanish NPP PSAs are mainly based on the SHARP methodology. These analyses have been conducted for internal events, covering at power and the other operational modes, and fire and flood events. Therefore, pre- and post-initiating-event human actions have been identified and modelled. 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 mainly used. Dependency analyses are included. These methodologies have been complemented with some additional specific human reliability criteria and considerations as the PSA scope departs from a standard level 1 PSA for internal events at power. Some new methods (NUREG-1921 and the HRA calculator/HCR-ORE) are currently under consideration for human reliability in fire and flood events in order to better inform PSA applications (see below).

The level 2 Spanish PSA involves the three classical aspects: Interface, Containment Event Tree and Source Term Calculation. The grouping done at the Interface model incorporates the back-end systems and expands 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, each branching point being the result of a Decomposition Event Tree (DET). The Source Term Analysis sets up the source term categories and identifies its representative scenarios. Level 2 studies use the

MAAP code, and do not include uncertainty analysis. LERF is the resulting risk measure, which includes the frequencies of all the releases greater than 3% in iodines before 12 hours from the reactor trip.

The methodology used for fire PSAs is NUREG 6850 (EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities). Regarding HRA, the methodology is NUREG 1921 (EPRI/NRC-RES Fire Human Reliability Analysis Guidelines).

The methodology used for internal flood PSAs is EPRI Report 1019194 “Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment”

PSA models are continuously updated with plants modifications (after the refuelling outage in which these modifications have influence in the results) and with the operating experience feedback. The process for this maintenance is reviewed through a CSN staff inspection every other year.

6. NOTABLE RESULTS OF PSAs

In the following tables, we provide some quantitative information on the current results.

The initiating events with highest CDF contribution are:

NPP	for power states	for non-power and shutdown states
Trillo	Groups of initiating events: – LOCAs (71%), – Break of other lines (12%), – Loss of auxiliary electricity supply or LOOP (10%) – Generic transients (5%), – ATWS (2%) Individual initiating events: – LOCA (steam LOCA at pressurizer) 40% – SGRT 13% – Very small LOCA 13% – Loss of auxiliary electricity supply or LOOP (10%)	Groups of Initiating events: – LOCA (49%), – LOOP (33%) – Loss of RHR (14%), – Boron Dilution (4%) Sequences – scenario – RHR break or leak with the cavity full (34%) – Loss of auxiliary electricity supply with the primary system at 3/4 open loop (31%) – Break or leak outside containment with the Reactor Coolant System (RCS) at 3/4 open loop (12%) – Loss of RHR at ¾ open loop (7%), and

NPP	for power states	for non-power and shutdown states
Vandellós	Groups of initiating events: – Transients (35%) – Loss of DC power (18%) – LOOP (12%) – LOCAs (10%), Individual initiating Events: – Reactor and turbine trip (27.18%) – Loss of off-site power 400 kV (9.79%) – Loss of DC 125 V (9.29%)	Groups of Initiating events: – Loss of RHR (43.6%) – LOCA (31%), – LOOP (22.8%) – Overpressure (2.3%) Sequences – scenario – Loss of RHR train in service with primary inventory on flange level (20.3%) (spent fuel) – Loss of RHR train in service with primary inventory on flange level (13.8%) (fresh fuel) – Loss of external power supply during hot shutdown (12.53%) – RHR small break during operation in mode 5 (12.8%)
Ascó I y II	Group of initiating events: – Transients (43.43%) – LOCAs (24.94%), – LOOP (8.42%) – SGTR (6.32%) Individual initiating Events: – Reactor and turbine trip (25.81%), small LOCA (18.91%), – Loss of main feedwater (10.52%) – Steam generator tube rupture (6.32%)	Groups of Initiating events: – Loss of RHR (54.8%) – Overpressure (19.43%) – LOOP (15.48%) – LOCA (8.77%), Sequences – scenario – Loss of RHR train in service during hot shutdown (20.4%) – Loss of support systems for RHR train in service during hot shutdown (13.7%) – Loss of external power supply during hot shutdown (12.53%)
Almaraz I y II	Initiating Events: – Generic transients (20.34%) – Loss of Component Cooling Water System (15.16%) – Loss of Service Water system (14.07%) – Small LOCA's (8.33%), – Interface LOCA´s (4.26%)	Sequences – scenario – Loss of Service Sater (Unit 1 outage U2 at Power) (13.31%) – Loss of coolant inventory in RCS during reduced inventory phase. (12.69%) – Loss of RHR support systems during full inventory phase. (8.91%).

NPP	for power states	for non-power and shutdown states
Cofrentes	Groups of initiating events: – ATWS (71.27%), – SBO (16.44%) – ISLOCA (9.43%), – Transients (1.1%) Individual initiating Events-sequences: – SBO failure to recover AC power before DC power failure and failure to supply water (low pressure) with fire protection pump. (11.55%) – ATWS /Turbine trip with level control failure with MFW and boron injection failure (18.3%) – ATWS /Turbine trip with level control failure with MFW and level control in low pressure failure. (8.94%)	Group of initiating events: – Loss of power supply to RHR-loop in operation (64.10%) – Drainage of RHR by SDC (14.8%) – RHR isolation (9.40%) Sequences – scenario – Drainage of RHR by SDC with vessel head removed (refuelling) – Loss of power supply to RHR-loop that is operating during cold shutdown. – Loss of power supply to RHR-loop that is operating during vessel level < 7 m vessel flange

The components with the highest importance measures (Fussell-Vesely and Risk Achievement Worth) in Level 1 PSA (at power) are as follows.

NPP L1	**Fussell- Vesely** Main components (no Common cause failures)	**Risk Achievement Worth**
Trillo	– Failure to open, valve for restoring water to demineralised water tank. – Functional group failure- trip, feed water pumps to SGTR – Human Error (HE) in execution of the primary F&B – HE in recovery water to emergency feed water.	– Common cause failure to start, low pressure injection pumps – Common cause failure to open, recirculation valves.

NPP L1	**Fussell- Vesely** Main components (no Common cause failures)	**Risk Achievement Worth**
Vandellós	– Failure to operate, backup pump for injection to reactor coolant pump seals. – Fail to start, AFW turbine-driven pump – Loss of function, pressure instrumentation for opening recirculation valve – HE SG level control with AFW – HE F&B – HE change to recirculation	– Failure to remain open, supply valve from CST. – Failure to insert control rods (SCRAM failure) – Failure to operate, DC distribution centre – Common cause failure to start, Essential Service Water
Ascó I and II	– Failure to open and control failure, AFW turbine-driven pump control valve – Failure to run, low pressure pump for recirculation – HE SG level control with AFW – HE F&B – HE change to cold leg recirculation	– Control rods fail to insert (SCRAM failure) – Common cause failure, batteries. – Common cause failure, reactor trip breakers
Almaraz I and II	– Failure to start, AFW turbine-driven pump – Failure to run, component cooling water pump – Failure to run, service water pump – HE to trip RCP – HE F&B – HE to control feed water to SG	– Common cause failure to run, service water pump – Common cause failure to close, FW system valves (return to CST)
Cofrentes	– Failure to run, boron injection pumps – Failure to run, fire protection pump – HE to control level using main Feed water. – HE to supply power to emergency bars on long term.	– Common cause failure, batteries – Common cause failure to open, essential service cooling water valves. – Common cause failure to run, essential service cooling water pump.

Level 2 PSA results (At Power):

NPP	Level 2 for power states
Trillo	The contribution is driven fundamentally by Steam Generator Tube Rupture scenarios, secondary pipe ruptures and induced generator tube rupture and, to a lesser extent, by scenarios of Interface Systems 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 rupture 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 systems LOCA (containment bypass).
Almaraz I y II	Frequency of Large 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	Yearly frequency of Large Early Releases (LERF): the most important contributors being early failure of the vessel and containment and Drywell (DW) bypass Yearly 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.

7. PSA APPLICATIONS AND DECISION MAKING

In the origin of the Spanish PSA Program, one of the main goals was to develop PSA applications, since PSA was considered a useful tool to identify important contributions to the risk (core melt and early radioactive release).

With this goal, during the developing phase, licensees used PSA insights to identify vulnerabilities and to carry out design evaluations; therefore, some design modifications were identified and implemented. The main purpose of these modifications was to reduce the risk in operation for NPPs and to enhance safety. Some examples of these are:

- Modification of logic for broken loop selection (GE-BWR/3).
- Modification for avoiding FW isolation in case of ATWS in order to control level through FW system (GE-BWR/6).

At same time, CSN has made use of these PSA insights to review safety in the framework of Periodical Safety Reviews (PSR). In those cases, CSN staff required some plant modifications focusing on reducing those risk contributors that were considered very high. Some examples of these are:

- Motorisation of recirculation valve to improve the action to change to recirculation phase.
- Modification of piping layout through the control building to avoid the high impact from flooding scenarios in CDF.

None of the above cases had a numerical objective, but CDF close to 10^{-4} was used as a criterion to consider risk too high.

In this phase, there were also changes and improvements in abnormal operation procedures, and emergency operation procedures to optimise operation action (for example inhibition of automatic depressurisation in GE-BWR/6). In addition, several operating procedures were developed to cope with failures during shutdown activities. PSAs have not been used in the case of guidelines for severe accident management, nor for strategies in beyond-design-basis accidents.

Among PSA Applications developed by licensees, we can distinguish those required by CSN from other voluntary actions taken by them.

- PSA applications required by CSN to NPPs (main examples):
  - 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, NPP use procedures developed to manage safety based, in some cases, in shutdown PSA models.
  - Evaluation of Technical Specifications: In 2011, CSN issued a new Technical Specification Instruction (IS-32). In this Instruction, new operational conditions are required for risk significant components or systems.
  - Currently, NPPs are adapting their Technical Specification to this new requirement. In 2006 Cofrentes NPP had already adopted this criterion and new operational conditions were included for equipment not previously required in the Standard Technical Specifications (venting valves, fire pumps for injecting water to vessel in case of SBO).

  - IFSM indicator for the Spanish Regulatory Oversight scheme.
- Voluntary PSA applications carried out by NPP and reviewed and approved by CSN
  - RI-ISI/RI-IST:
    - Cofrentes NPP has implemented RI-ISI for class 1 and class 2 piping and RI-IST for valves (motorised, pneumatic, solenoid and check) and motor-driven pumps.
    - Almaraz NPP has implemented RI-ISI for class 1 piping.
    - Ascó NPP has implemented RI-ISI for class 1 piping and RI-IST for check valves.
  - Transition to NFPA 805 for Fire Protection Program: So far, Almaraz NPP and Ascó NPP have applied for transition to NFPA 805 and CSN staff is currently involved in the evaluation of this change a the new licence base.
  - Since the completion of PSA level 1 models, several applications for changes in technical specifications changes have been submitted to CSN. Not all of them were approved by CSN.
- PSA applications implemented by CSN

Licensees regularly send PSA NPP reports and models (RiskSpectrum or CAFTA) to CSN for review. They are also available for CSN use in internal applications. In 2006, CSN developed and started a Systematic Oversight Program for supervising activities at NPP that makes use of licensee PSA models.

  - The CSN supervision programme has two different parts. First, it has an inspection programme focused on the most risk significant components and processes in the NPP. Inspection findings are categorised by their risk impact. The second part is an indicator programme; some of these indicators track availability and failure of components and their impact on PSA.
  - PSA-based event analysis. The analysis of operational events using PSA is integrated in the CSN operational experience feedback process. CSN staff makes the determination of the quantitative importance of a few well-selected operational events per year.

8. FUTURE DEVELOPMENTS AND CURRENT RESEARCH

Currently, licensees have not modified the activity programme about PSA and are working to complete the whole scope for PSA. They are not embarked in new research related to PSA or in new developments after Fukushima accident.

From the side of CSN, currently two new research activities have been launched.

First, CSN is working together with the Polytechnic University of Madrid in a project to assess whether capability exists and the effort required to develop PSA level 1 models independent of those of the industry. The objective is for those models to be used in regulatory oversight tasks.

Second, CSN is revisiting its approach to PSA Level 2 independent verification and validation activities of the application of NUREG 1150 to Spanish plants. The objective is to update the methodology and tools used at the time when the Individual Plant Examinations (IPE) of Spanish Plants were independently assessed.

The intent of this revisiting process is to take into account the large and deep increase in new PSA technology-related techniques, particularly through the integration of DSA and PSA. Special emphasis will be given to the impact of the time dependencies and how to ensure consistency between static and dynamic elements in event tree and source term assessments. The process includes improvement of some of these aspects in the CSN PSA Level 2 software package. Research activities with this aim are now active, with special emphasis in accident progression event tree (APET) and associated source terms uncertainty assessment and reduction. There is also a particular interest in the potential and consistent use of PSA insights and data in the field of Severe Accident Management Guidelines (SAMG).

9. INTERNATIONAL ACTIVITIES

Regarding PSA international activities, CSN is mainly involved in projects under NEA cover including FIRE and ICDE databases. CSN has also participated in the CSNI working group to write a report on “Informing Severe Accident Management Guidance and Actions through Analytical Simulations” (INFSAMG), where the potential for incorporating PSA insights into the V&V of the severe accident emergency guides was also considered.

Additionally, CSN has participated in the Open PSA initiative. The objective of this initiative is to provide a standardised format for PSA models. This standardised format can then be used as a platform for PSA applications independent of the underlying quantification programme.

SWEDEN

1. INTRODUCTION

Here, no contribution is expected from the participants.

2. PSA FRAMEWORK AND ENVIRONMENT

During the 80s and 90s the Swedish PSA work was very much linked to the programme of the domestic ASAR-programmes (ASAR80 and ASAR90 programmes) (ASAR = As Operated Safety Analysis Report). In the ASAR80 programme, the licensees had to perform PSA level-1 studies (scope in principle limited to full power mode and LOCA/Transients). In the ASAR90 programme, PSA level-2 studies were performed including scope extension with low power and shutdown modes as well as CCIs.

The PSA had to be published and reported to the regulatory body SKI, every 8th-10th year as an appendix to the respective ASAR report.

In 1998 SKI published SKIFS 1998:1 “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”. Probabilistic analyses were only mentioned in the advice section, however included advice on scope: PSAs level 1 and level 2 should be performed for all operating modes.

Since 2004, PSA requirements were updated (SKIFS 2004:01). Now they explicitly stated that probabilistic methods shall be performed in order to provide as comprehensive a view as possible of safety. Advices were similar as in the previous regulation.

SSM was formed in 2008, and then all previous regulations were republished and SKIFS 2004:1 was replaced with SSMFS 2008:1 “The consolidated version of the Swedish Radiation Safety Authority’s Regulations concerning Safety in Nuclear Facilities with amendments made up to and including SSMFS 2010:3. SSMFS 2010:3 is only available in Swedish. The latest consolidated version of the regulation with amendments made up to and including SSMFS 2014:3 is only available in Swedish. SSMFS 2008:1 has the previous advice on expected scope of the PSA (level 1 and level 2 and all operating modes) as requirements. Advices are complemented with description on expected applications of PSA. This is the regulation currently in place.

Since the previous report on use and development of PSA, there was first a rather low profile on supervision activities in the PSA area. Because of possible new build projects, SSM PSA resources were strengthened during 2012-2013 from one to about four full time persons. The strengthening was influenced by an IAEA IRRS review to Sweden in 2012, Fukushima stress tests, a Vattenfall submission on new NPP:s, increase in PSA supervision activities and steps in using more risk information in SSM supervision planning. A large project to develop a completely new set of regulations was also initiated in 2012. This include an update of PSA requirements. In general, the new set of requirements should consider updated WENRA reference levels, Fukushima and related stress test requirements and also other new information and international agreements within the Convention on Nuclear Safety (CNS) and implementation of the Euratom

Nuclear safety Directive (NSD) and Basic Safety Standard (BSS) on radiological protection. The plan is to have the new regulations in place in the beginning of 2018. Deadline is due to NSD and BSS implementation deadlines.

New Regulations in development

The new regulations are composed of four major documents:

- General safety requirements
- Design requirements
- Analysis requirements
- Operation requirements

Specific PSA requirements are mainly in the Analysis requirements document. Design and Operation requirements refer to PSA to risk inform various issues, in principle similar to the WENRA reference levels statement on the use of PSA. One new requirement being discussed regarding PSA is a potential extension of requirements towards PSA level 3.

First internal review of the proposed new regulations is completed in 2015. A second internal and external review is ongoing (in the end of 2016).

PSA Supervision

SSM PSA supervision uses the following activities:

- Review of PSA updates that are notified to SSM on a regular basis,
- Review of PSAs when they are part of a notification on plant changes
- Operation review at the licensees and
- Technical meetings for exchange of information and discussion of selected topics at SSM.

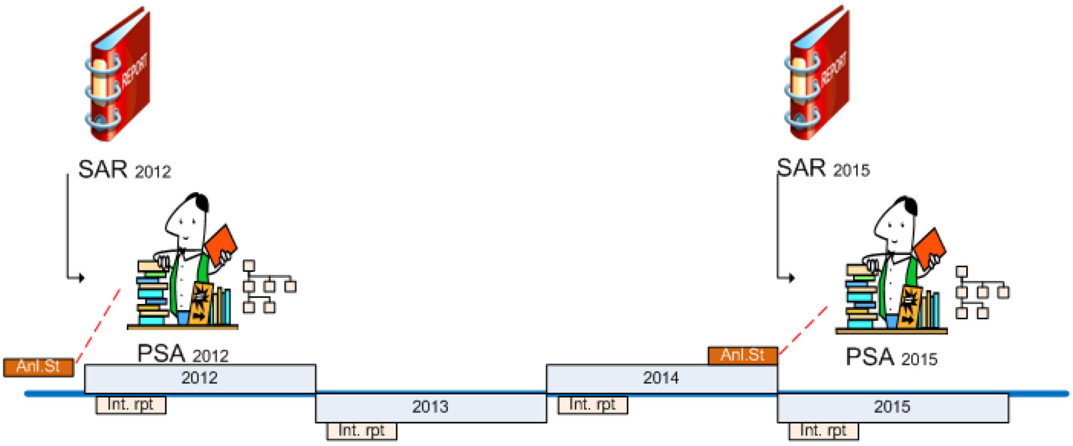
In addition, SSM is also reviewing certain PSA aspects as part of the review of licensee periodic safety review (PSR) reports.

Living PSA

SSM organised in 2013 the PSA castle meeting, a reoccurring Nordic meeting organised by one member of the Nordic PSA Group (NPSAG) every18-24 months. The 2013 meeting had as one main theme: a discussion on definition of living PSA (LPSA) and its implementation. One background to this discussion is the SSM requirement to have an updated SAR reflecting the actual plant design, plant operation, consideration of R&D development and operating experience. This requirement means that also PSAs have to be up-to-date. Updating of PSA models and documentation is a process in place for many years at the utilities, but SSM had seen much delay in notification to SSM on PSA updates. SSM also wanted to have more regular updates in support of developing and maintaining a so-called risk map, an activity initiated in 2013 [1]. The purpose by the risk map is to support SSM supervision activities in general with PSA-based risk information for a graded supervision planning approach, and for prioritisation of specific issues as prioritisation of depth of review of event reporting and notifications from licensees. The risk map activities will also be a learning tool in general concerning risk drivers for each plant.

All current PSA versions were delivered to SSM in 2013 in support of the risk map development and licences presented the status of their PSA work and PSAs at meetings held at SSM.

The Living PSA practice now in place and agreed on between SSM and the utilities is visualised in the figure below:



PSA SAR chapter including PSA reference documents is notified every third year, as indicated in the figure. The reporting is expected to include information about changes etc. as in intermediate reporting.

Intermediate reporting at the end of each year should contain the following: PSA activities since last time, new PSA results, ongoing development activities, plant changes, operating experience, new R&D results taken into account.

The first round of interim PSA reporting review was completed in spring 2015. The review identified a need for certain clarifications on SSM interim report expectations. It is expected that the interim reports have the following information:

- Model status w.r.t. plant design and operation
- Changes in methods, scope and data since previous reporting
- Important differences in results and their interpretation/evaluation
- A clear statement on the validity of the PSA
- A clear statement of the applicability in different applications

The first interim PSA reporting review also noted that there are still challenges for licensees to keep PSA and documentation up-to-date with reasonable delay and efforts.

PSA supervision activities

Currently, the following supervision activities are in place:

- Operation monitoring meeting at each utility approximately every second year.
- Review of specific notifications involving PSA, approximately one a year.
- Yearly review of new PSA information and update of risk map with new information as it becomes available.

Operation monitoring is a meeting where SSM can present what´s going on at the authority and the utility can present current activities regarding PSA, e.g. organisation changes, man power, competence, R&D work, use of PSA.

Notification review is usually targeting some specific issue, e.g. a method where PSA is used by the utility to risk inform plant changes. SSM has not performed a complete PSA review since many years, neither by own or hired competencies.

Almost all PSA are in 2016 complete level 1 and level 2 PSAs with regard to the source of activity, operating modes and set of initiating events, see appendix.

Source of activity	Fuel in the reactor pressure vessel, fuel in the spent fuel pool and fuel being transported between these.
Operating modes	Power operation, low power and shutdown modes
Initiating events	Internal process hazards (BoP including support system CCI (cooling systems, electrical systems, signalling systems etc.), internal area event hazards as fire, flooding and missiles, and external hazards)

The main purpose with the PSAs is to identify week points in the present design, operational routines and instructions and support the deterministic approach in reaching a balanced risk profile. The guidelines provided in SSMFS 2008:1 express also that PSA is expected to be used to support various plant activities, e.g. programme for operator education and training, safety classification of systems, structures and components (SSC), and technical specification justifications.

PSAs are historically mainly developed and maintained by domestic consultants and this has been the case also for the last 5-10 years. However, note that the overall responsibility is by the PSA offices at the licensees. The utilities have in most cases own personnel developing the SAR PSA chapter and own personnel being assigned as responsible for the respective plant-specific PSAs.

SSM does not perform own development of PSA. The role of SSM is to have supervision to meet the objectives as mentioned above.

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). Results are presented for total CDF/LERF and contributors from operating states and initiating event are shown.

SSM requirements do not contain any numerical criteria for PSA. However, SSM has criteria for the deterministic analysis indicating the frequency for event classes and the related dose consequence level. Current and proposed deterministic frequency classes and related dose /release level criteria are shown in the tables below:

<table>
<tr><td colspan="5">Existing criteria according to SSM decisions from 2009 [2] on requirements for radiological environmental consequences analysis.</td></tr>
<tr><td>Event class according SSMFS2008:17</td><td>Source term for long-term land contamination</td><td>Effective dose (mSv)</td><td>Equivalent thyroid dose (mSv</td><td>Frequency</td></tr>
<tr><td>H2 expected</td><td>0.001*FILTRA</td><td>1</td><td>1</td><td>During lifetime of one reactor.</td></tr>
<tr><td>H3 not expected</td><td>0.01*FILTRA</td><td>10</td><td>10</td><td>During lifetime of several reactors.</td></tr>
<tr><td>H4 unlikely</td><td>0.01*FILTRA</td><td>100</td><td>100</td><td>Not expected to occur. Design-basis events.</td></tr>
<tr><td>H5 very unlikely</td><td>FILTRA (0.1 % Cs-134 och 137 in a 1 800 MWth power (same as Barsebäck)</td><td>-</td><td>-</td><td>Not expected to occur, potential for large core damage. Design basis for mitigating systems as FILTRA and scrubbers.</td></tr>
</table>

<table>
<tr><td colspan="5">Proposed design requirements for effective dose to adults in the public (mSv/y-1 – reactor-year)</td></tr>
<tr><td>Event class</td><td>Existing NPP</td><td>New NPP</td><td>Internal hazard frequency</td><td>External hazard frequency</td></tr>
<tr><td>Expected (H2)</td><td>1</td><td>0.1</td><td colspan="2">1E-2 < = H2</td></tr>
<tr><td>Not expected (H3)</td><td>10</td><td>1.0</td><td colspan="2">E-4 < = H3 < 1E-2</td></tr>
<tr><td>Unlikely (H4A)</td><td>100</td><td>20</td><td>1E-6 < = H4A < 1E-4</td><td>1E-5 – 1E-4</td></tr>
<tr><td>Special events (H4B)</td><td>100</td><td>20</td><td>H2, H3</td><td>1E-6 – 1E-5</td></tr>
<tr><td>Events with large release of radioactive substances (H5)</td><td>1 000</td><td>100</td><td colspan="2">H5 < 1E-6</td></tr>
</table>

<table>
<tr><td colspan="2">Proposed design requirements concerning worker exposure</td></tr>
<tr><td>Event class</td><td>Design requirement (mSv)</td></tr>
<tr><td>Expected (H2)</td><td>20</td></tr>
<tr><td>Not expected (H3)</td><td>20</td></tr>
<tr><td>Unlikely (H4A)</td><td>20</td></tr>
<tr><td>Special events (H4B)</td><td>20</td></tr>
<tr><td>Events with large release of radioactive substances (H5)</td><td>50</td></tr>
</table>

Utilities have chosen to define own PSA criteria /target safety goals for interpretation of results and assessment of their acceptability. New regulations are proposing a requirement that utility shall define safety criteria for evaluation of results. These criteria are influenced by international criteria and the deterministic criteria for event classes.

In principle, the current level 1 criteria used by all utilities says that the CDF shall be lower than 1E-5/y. It has been debated if this shall include all scope contributors, and arguments lean towards the conclusion that the CDF shall be lower than 1E-5/y, all contributors included.

For level 2 there is a basis in the definition of unacceptable release dating back to the design requirement for Barsebäck plant (closed in the 90-ties) FILTRA (containment filtered venting system), that also was applied for the containment scrubber system installed for all other NPPs. The design criterion is 0.1% of release products (e.g. CsI, CS, BAO, MoO2, excluding noble gases) from the former Barsebäck 1 reactor or a core with the corresponding thermal power. A frequency limit at 1E-7/year for unplanned release of core inventory larger than this criterion is usually used to evaluate PSA level 2 results.

Some utilities also compare the PSA results with the frequency criteria for the deterministic event classes.

Events and event sequences with a frequency lower than 1E-7/y are usually screened out.

The Nordic PSA group sponsored a research project on safety goals, the so-called "Validity of Safety Goals" project. This project was initiated in 2006 and finalised in 2010 with the SSM Report 2010:36 "Guidance for the Definition and Application of Probabilistic Safety Criteria". The aim was to provide a general description of the issue of probabilistic safety goals for nuclear power plants, of important concepts related to the definition and application of safety goals, as well as of experiences in Finland and Sweden. The project has also aimed at providing guidance related to the resolution of some of the problems identified, such as the problem of consistency in judgement, comparability of safety goals used in different industries, the relationship between criteria on different levels, and relations between criteria for level 2 and level 3 PSA.

4. PSA STANDARD AND GUIDANCE

National regulations:

Current requirements for PSA are given in SSMFS 2008:1. In principle they state that the plant shall be analysed using PSA level 1 and 2 and that all potential contributors shall be considered, similar to the requirements for deterministic analysis. In addition, there are requirements that impact from uncertainties shall be considered in the analysis. So-called advices in SSMFS 2008:1 provides some more details on regulator expectation on the quality of PSA. As mentioned above, there are some statements concerning expectations on the use of PSA in various risk-informed applications.

National standards:

There are no formal domestic standards available. The requirements and advices provided in SSMFS2008:1 is the basis. Further guidance on the quality of a PSA is given in the PSA review handbook SKI report 2003:48 (in Swedish Tillsynshandbok PSA). SKI2003:48 was published in 2003. This report also included a list of more or less all the most important references that had been used in the domestic PSAs until then. The PSA review handbook can be seen as expressing SSM expectations on PSA and PSA activities. The handbook describe what is to be done rather than how it is to be done.

The PSA review handbook was and is still a support in SSM supervision (inspection and review) of licensee PSA activities and the PSAs. 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.

Three basic types of review activities are covered

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

Evaluation criteria are 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.

***"National (Nordic) guides"**:*

In addition to the review handbook, there are also several reports developed through combined efforts by SSM (SKI) and the utilities within NPSAG co-operation projects. These reports provide much of the state of the art in Sweden (and Finland) and are used as references in licensee method descriptions. Swedish PSAs are also heavily influenced by using IAEA and US developed guides and standards. The latter can also be seen in both SKI2003:48 and the various guidance documents.

SSM and the industry (NPSAG) have published several guidance, methodology and data reports.

Guidance listed in the previous use and development report			
Org.	Year	Number	Title
SKI	2002	SKI 2002:27	Guidance for External events Analysis.
SKI	2003	SKI 2003:25	Branddata projektet In 2003, SKI produced a report dealing with best estimate of fire frequencies for Swedish NPPs.
SKI	2003	SKI 2003:48	Tillsynshandbok PSA (PSA Review Handbook), in Swedish.

Not listed in the previous Use and development report			
SKI	2004	SKI 2004:04	Vol1 Dependency Defence and Dependency Analysis Guidance.
SKI	2004	SKI 2004:04	Vol2 Dependency Defence and Dependency Analysis Guidance.
SKI	2006	SKI 2006:19	Consideration of CCF in PSA and PSA applications (in Swedish: Hantering av CCF vid beräkningar i PSA och PSA tillämpningar).
SKI	2008	SKI 2008:33	Risk-informed-assessment-of-defence-in-depth-LOCA-example.
NPSAG/VTT	2009	NPSAG 20-005:01 VTT-R-11463-08	Methods for risk follow-up and handling of CCF events in PSA applications.
SSM	2010	SSM 2010-16	Guidance to Risk-Informed Evaluation of Technical Specifications using PSA.
SSM	2010	SSM 2010-36	Guidance for the Definition and Application of Probabilistic Safety Criteria.
NPSAG	2011	NPSAG 04-007:02	R-book, second version.
NPSAG	2012	NPSAG 30-002:01	Application of ASME PRA Standard on Nordic PSA studies.

NPS AG	2013	NPSAG 36-001:01	Workshop on handling of seismic events in Swedish PSAs.
NPS AG	2013	NPSAG 20-001	Modeling of loss of offsite power.
NPS AG	2014	NPSAG 34-003:01	Common methodology for analysis of initiating events: Method for identification and categorisation of initiating events.
NPS AG	2014	NPSAG 34-003:02	Common methodology for analysis of initiating events: Methods for classification and parameterisation of initiating events.
SSM	2015	2015-04	DiD-PSA: Development of a Framework for Evaluation of the Defence in Depth with PSA.
NPS AG	2015	NPSAG 11-004-03	Evaluation of Existing Applications and Guidance on Methods for HRA EXAM-HRA: HRA Application guide.
NPS AG	2015	NPSAG 11-004-02	Evaluation of Existing Applications and Guidance on Methods for HRA – EXAM-HRA: A Practical Guide to HRA.
NPS AG	2015	NPSAG 11-004-01	Evaluation of Existing Applications and Guidance on Methods for HRA – EXAM-HRA: Final Summary Report from the NPSAG/SAFIR Project EXAM-HRA.
NPS AG	2015	NPSAG 39-001:01	Result Presentation Seminar Guidance for quantification and result presentation and evaluation (results of a workshop in April 2015).
NKS/ NPSAG	2015	NKS-330	Guidelines for reliability analysis of digital systems in PSA context - Final report.
NKS/ NPSAG	2015	NKS-341	Software reliability analysis for PSA: failure mode and data analysis.
NPS AG	2015	NPSAG 41-001:01	Dependencies in HRA.
TuD/ Vattenfall	2015	Available via Vattenfall	T-book: New T-book version 8.
NPS AG	2016	NPSAG 44-002	C-book: Part 1 CCF reliability data book.
NPS AG	2016	NPSAG 44-002	C-book: Part 2 CCF reliability data book: Practical handbook.

All SSM (SKI) research reports are available at www.ssm.se and several also at www.npsag.org.

5. STATUS AND SCOPE OF PSA PROGRAMMES

Status of the Swedish PSA programme as of end of December 2016 is presented in the table in Appendix A.

6. PSA METHODOLOGY AND DATA

PSA work at the licensees is to a large degree based on US and IAEA methods descriptions including WASH 1400 in 1975 and forward:

- Reactor Safety Study, WASH1400
- PRA Procedures Guide, NUREG/CR-2300, 1983

- PSA Procedures Guide, NUREG/CR-2815, 1985
- Human Reliability Handbook, NUREG-1278, 1983
- Good Practices for Implementing Human Reliability Analysis (HRA), NUREG-1792, 2008
- Guidance provided in the US for the Individual Plant Examination program required by the NRC Generic Letter GL-88 in 1988.
    - Individual Plant Examination: Submittal Guidance , NUREG-1335, 1989
    - Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, NUREG-1407, 1991
- IAEA guides and TECDOCs:
    - Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide, Safety Standards Series No. SSG-3, IAEA 2010
    - Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants Specific Safety Guide, Safety Standards Series No. SSG-4, IAEA 2010
    - Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants , TECDOC-1511, IAEA 2006
    - Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, TECDOC 1804, IAEA 2016 (replacing 1511).
- Standards
    - Guidance on PSA quality as provided by ASME standards, in particular RA-S 2009
- Several guidance documents developed in the Nordic countries (see the table above).

All these references are the basis for licensee own method descriptions and instructions.

All licensees uses RiskSpectrum PSA software as their PSA model development, model maintenance and analysis tool.

The once so-called small event trees and large fault tree approach (SE-LF) has been used since first Swedish PSAs. However, today also event trees are rather complex, it is more of a large event tree large fault tree approach LE-LF).

All plants have completed full-scope studies covering PSA level 1 and 2, all operating modes (full power + low power and shutdown (LPSD) for level 2 studies) and internal as well as external hazards with a few exceptions as shown in appendix A.

Some of the characteristics of Swedish PSAs are given below:

Identification of risk sources

- Several PSAs consider both the fuel in the reactor pressure vessel and in the spent fuel pool. Some screening is applied to limit the analysis work needed, e.g. when very long time is available.

Initiating events:

- Identification of transient type (loss-of-coolant and non-loss of coolant) initiating events based on results from other studies, operating experience and usually complemented by checking of generic lists and master logic diagrams.
- Area events mainly restricted to internal fire and flooding. Fire and flooding scenario identification follows specific methods as the whole area event analysis. These methods usually are kind of bounding analyses starting with conservative approaches and going into more details if needed. Area events analyses focus on identification of potential scenarios that need further compensatory measures (fire/flooding prevention fire/flooding detection, and fire/flooding fighting, e.g. separation by fire doors, flooding routes to make sure that these hazards are small risk contributors. These analyses are therefore in general expected to be conservative.
- External events identification and analysis is based on Nordic guidance. This guidance was further developed after Fukushima and was also an input to OECD/NEA and IAEA guidance.
- Transient initiating events data updated by the plants themselves on a regular basis. This process includes also an analysis and grouping of all the occurred transients and other initiating events modelled in the PSA.
- R-book is introduced for LOCA frequencies. R-book is based on data from the OECD/OPDE database project (now called CODAP).
- Fire frequency data from Swedish statistics combined with data from OECD/FIRE, except for OKG that uses another approach.
- Flooding frequency data based on own statistics and R-book.

Accident Sequence analysis:

- As mentioned above, large fault trees and large event trees.
- Success block diagrams presenting the accident scenarios in a success path fashion used as a link between PSA analysts and plant personnel and are the basis for event tree development.
- The level 1 end consequence core damage (CD) in several cases divided into 3 subcategories, core damage due to failure of reactivity control (CD1), due to failure of water injection/feeding (CD2), due to failure of heat removal (CD3). In addition, sometimes categories for overpressurisation end-states are applied with the assumption that reaching these categories is equivalent to immediate core damage.
- Rather detailed system descriptions are the link between plant personnel and PSA analysts and are the basis for fault tree development.
- PSA models in RiskSpectrum has a quite extensive use of exchange events and boundary conditions, features inherent in RiskSpectrum. This allows e.g. the reuse of event trees for different situations where boundary conditions/house events used to shape event tree to the specific situation, e.g. different success criteria.

Level 2 PSA:

- Similar as above and level-1 and level-2 PSA models are integrated.

- Consideration of level 2 related phenomena is based on APRI R&D results (APRI=Accident Phenomena of Risk Importance and is an R&D effort that started in the 80ties and still continues with participation from all utilities and SSM. The project and keeps track of state of the art regarding phenomena affecting accident scenario development and the source term to be released in case of an accident).
- Most phenomena threatening containment and mitigating systems screened out for BWR PSAs while more are included in PWR PSAs.

Level 3 PSA:

- L3 PSA is not required.
- However, several aspects are available, e.g. source terms in level 2 and analysis of radiological consequences for cases representing different radioactivity sources and event classes. These are deterministic type analyses.
- R&D work has been ongoing 2013-2016 and potential requirements for level 3 PSA is discussed in new legislation project.

Dependent failures including common-cause failures (CCF):

- Explicit modelling of all functional dependencies in fault trees.
- Common Cause Initiators accounted for in the initiating events analysis and accident sequence analysis.
- Dynamic effects considered as part of LOCA analysis.
- Secondary effects in general should be considered.
- Area dependencies considered in the specific analysis for fire and flooding, mapping of all area dependencies including all systems, structures and components (also all types of cables) of importance for safety functions.
- CCF considered between redundant similar components within a system.
- Intersystem dependencies not considered in the PSAs. However, to meet SSM requirements on diversity, mapping of similar component parts is made with support of PSA model and tools. Mapping results used to prioritise any compensatory measures needed.
- Alfa-factor main method used for modelling of CCF in low redundant systems (up to four trains).
- HiDep common load model used for modelling of CCF in high redundant systems, e.g. control rods and steam relief valves. Formal method description of the common load model theoretical background developed in 2015-2016 and to be published in 2017.
- Participation in the OECD/ICDE project.
- CCF data book developed and published in 2016. It is planned to incorporate data from C-book into several PSA models in the near future.

Human reliability:

- Initiator type human actions are covered by initiating event data or in some cases specific analysis, e.g. for heavy lift operations.

- Pre-initiator human actions such as erroneous alignment and calibration errors covered by component data (T-book).
- Sequence human actions (as part of the sequence development/recovery type actions) explicitly modelled by individual basic events. (EXAM-HRA project influenced also of HE analysis needs and good practices, given in the NUREG-1792)
- Quantification methods varies but mainly based on Technique for Human Error Rate Prediction (THERP) and SLIM (Success Likely Index Method) type methods.

Component reliability 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.
- Data scope in T-book are on demand failure probabilities, on demand failure rates, mission failure rates and repair times. Standby failure modes are represented by a demand failure probability, a standby failure rate or in some cases with both a demand probability (undetected failures) and a standby failure rate.
- Plant-specific component data are available in the T-Book - Reliability Data of Components in Nordic Nuclear Power Plants. The T-book has been regularly updated about every 4-5 calendar year. The most recent edition is - T-Book version 8 published in 2015. The T-Book can be ordered from: The TUD office, Vattenfall AB, Safety Analysis, Evenemangsgatan 13, SE-16956 Arenastaden, Sweden.
- PSA models are usually updated with new T-book data within a rather short time period when a new version is available.

PSA results presentation and evaluations:

- In general results are presented in terms of core damage frequencies and release category frequencies and detailing contributions from individual as well as groups of initiating events and also contributions from different operating states.
- Most of the PSAs also presents the dominating event tree sequences, dominating cut sets, as well as dominating basic events and basic event groups and parameter values. Importance measures are commonly estimated by using the Fractional contribution (FC), the Risk Increase Factors (RIF) and the Risk Decrease Factors (RDF).
- Status of the Swedish PSAs 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.

Review:

- A PSA study that a licensee sends to SSM as a notification has to be independently reviewed and a documented statement of results of this process have also to follow with this delivery.

External Events

- Identification and analysis of external hazards based on Nordic guidance,
- Most hazards screened out because of their low frequency
- A few external events have explicit representation in event trees and fault trees

Internal hazards (Area events fire and flooding)

- Usually conservative approach to show that contribution is small, and focus on identification of need for and prioritisation of area event protection improvements.

Low Power and Shutdown

- The operation over a calendar year is divided into operating states.
- So-called phases are used to further subdivide where needed in case of success criteria and technical specification changes from one point in time to another.
- Standard event tree and fault tree approach
- Initiating event frequency based on time in each phase.
- Pipe break and events with loss of water consider statistics and to some extent human reliability analyses.
- Heavy lifts are included, mainly using human reliability analysis methods

Success Criteria formulation

- MAAP and MELCOR codes are used to support the accident sequence analyses to define success criteria in terms of flow capacities, pressure relief capacities and time available for operator actions etc.

7. PSA APPLICATIONS

Use of risk-informed approaches at SSM:

SSM (and previous SKI) supervision has always been more or less risk-informed. It is a natural ingredient in a regulators way of taking on daily questions.

However, there has been identified a need to develop and more clearly describe how SSM:s overall supervision is risk-informed and applies a graded approach, e.g. an IRRS mission to Sweden in February 2012 had one recommendation on this. SSM has therefore been working with a new project to further develop and document how SSMs oversight activities are risk-informed and follows a graded approach in all areas of operation.

The overall project objective is to improve precision in prioritisation of supervision planning with regard to risk, develop risk and performance based supervision programmes for each of SSM areas of responsibility (including non-nuclear) and development of supervision strategies adapted to the needs of each area. Choice of and blend of supervision tools (inspection, review, operations monitoring information meetings etc.).

The project include an analysis of the different risks and risk aspects that are SSM responsibility. One example is to consider the three aspects: safety (against accidents), security, and radiological protection (mainly workers safety) for a nuclear power plant. What are the hazards? What are the consequences and expected frequencies? What are the causes behind the hazards and what options are available to manage the risks? Where shall SSM use the resources in order to be an effective and efficient regulator? A paper on this was presented at the ANS2015 conference in Sun Valley [3].

A new method for supervision planning and performance evaluation of nuclear facilities is now (2016) being developed using insights from the risk analysis and also from a number of other activities. It is planned for test use in 2017.

The risk map, operating experience from the plants and SSM supervision findings are some of the input to the programme. The risk map provides a quick reference for status of PSA studies for all plants as well numerical results from the studies, such as calculated frequencies for core damage and radioactivity release and contributions from dominating initiating events and event groups. The risk map is currently under further development to incorporate estimates of uncertainty in results as well as to provide more information about importance of systems and components for modelled safety functions.

Further examples of risk-informed activities are decisions on the depth of review that shall be applied to notifications and the depth of analysis that should be applied to licensee event reports. PSA has also been used to support development of requirements and evaluation of licensee solutions regarding robust independent core cooling (following Fukushima and the stress tests).

Concerning SSM site-specific and annual safety assessments, PSA-results and PSA-activities are input to this internal process.

Use of risk-informed approaches at utilities:

The PSAs are being used in the following applications (varies between utilities and plants);

- identification and reduction of the risk from dominant contributors (e.g. functions, systems, components, human errors). This is basic use.
- support for backfitting activities with design option evaluation.
- providing an input into risk-informed Technical Specifications.
- Shutdown planning
- analysis of operational events.
- risk-informed in-service inspection, in-service testing.
- verification of deterministic requirements, e.g. separation and diversity.
- Technical Specifications evaluations (AOT, maintenance, testing, instructions).

Some specific examples are:

- OKG Fire PSA methods using a graded approach
- OKG Risk significance method (based on a combination of deterministic and probabilistic insights). This method is used in many different issues to determine the risk significance to be used in the decision-making process.
- Forsmark method for shutdown planning
- Ringhals PWR plants are using risk-informed in-service inspection of piping since many years, see previous report on use and development.
- Ringhals PWRs Standard Technical Specification according to NUREG-1413 principles.

8. RESULTS AND INSIGHTS FROM 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 PSAs 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 increasing level of confidence in PSA results. By the time a 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 PSAs have been used to show, in many cases, an optimised design solution before a modification proposal is accepted.
- The PSAs 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 PSAs, is that while the contribution from LOCA:s is decreased, the impact of electrical systems and dependencies become more important.

In general, the core damage frequency is in the order of 1E-5 and the frequency for large release (above design criteria for filtered venting/scrubbing) is between 1E-6 and 1E-7.

SSM review has identified the following:

- Analysis and presentation of uncertainties is insufficient and should be improved.
- Methods for area events analyses are mainly based on conservative assumptions. This is not always clear when results are presented on high-level. SSM:s view is that it is important with clear presentation of uncertainties, both regarding parameters, but also regarding degree of conservatism in the end results and among different contributors. Vague information about uncertainties will bias risk-informed decision making.
- Presentation of results is usually good, but it can be improved with addition of clarifications concerning interpretation and evaluation of the results, not only on high level as the total core damage frequency, but also for different contributors to the total scope.

9. FUTURE DEVELOPMENTS AND RESEARCH

This section describes not only future research and development but also provides a summary of what has been going on during the last 4-5 years.

Nordic PSA Group

The Nordic PSA Group (NPSAG www.npsag.org) is a forum for discussion of issues related to probabilistic safety assessment (PSA) of nuclear power plants, with focus on research and development needs. Work follows the roadmap [4] and issues cover all aspects of the PSA from initiating events analysis to result interpretation and presentation (level 1-3, all operating states, all kinds of hazards, systems analysis, success criteria formulation, accident sequence analysis, human reliability, data, and dependencies including CCF). NPSAG has members from the Swedish and Finnish utilities (Forsmark, Oskarshamn, Ringhals, TVO, and Fortum). Fennovoima joined in 2016. SSM and STUK (SSM from 2000 and STUK from 2017) are associated members.

NPSAG follows and discusses current issues related to PSA nationally and internationally, as well as PSA activities at the participating organisations. The group initiates and co-ordinates research and development activities and discusses how new knowledge shall be used.

NPSAG R&D Projects			
Title	Scope	Reporting	Period /completed
R-book – Reliability data for piping	• Completed second version in 2011 • Now implemented by all utilities. • Workshop on experience completed in spring 2016	See list above.	2011
PSA Level 3	Industry and Literature Survey Appropriate Risk Metrics Regulation, guides and standards Pilot applications Development of a Guidance document	Ongoing	2013-2016
Critical CCCG seminar	• Develop improved management and protection strategies against Common Cause Failures (CCF) in critical Common Cause Component Groups (CCCG) (SSMFS 2008:17 paragraph 10). • Increase awareness on critical CCCG issue in general and to develop an improved understanding of methods and strategies to avoid Critical CCCG to be introduced. • Methods presented and discussed	No report, but thesis on Feasibility study of a strength of defence method for estimation of CCF probabilities, see list above.	2012
Loss of Offsite Power	• Modelling of LOOP – establishing voltage/frequency profiles • PSA-modelling – how to model the different types of LOOP identified • Data Quality issues • Investigation of PSA-result impact	Final report available, see list above.	2013
Initiating Events	• Review of definitions • Harmonisation of methods • Development of new frequencies • Focus on integration of different event types (e.g. internal and external hazards) allowing a robust risk profile in consideration of potential differences in degree of conservative approach and uncertainties.		2013-2015
Multi-unit site PSA	• First work during 2016, co-ordinated with SAFIR PRADA activities and WGRISK activity on site risk	No reporting yet available	2016

NPSAG R&D Projects			
Title	Scope	Reporting	Period /completed
Pilot study on simplified Seismic PSA	• Workshop in 2013 requested specifically to address the following: o Review the credibility of the earthquake spectra that have been used for assessment of the Swedish reactor plant; o Clarify knowledge of the effects of earthquakes, including margins; o Compare alternative methods of seismic assessment and in particular to compare the merits of seismic margins assessment with seismic PSA. o Draft methodology in 2015 o Pilot cases for Swedish sites ongoing. Planned for completion in 2017.	See above	2013
NAFCS2	• CCF model parameter development based on mainly ICDE • Scope of components: Centrifugal Pumps, Emergency Diesel Generators, Check Valves, Motor Operated Valves, Level measurements, Breakers, Batteries • Component specific reports basis for C-book • Represented by Excel calculator and a manual • Output: Direct estimate CCF probabilities for simultaneous and staggered testing and independent and group repair policies	C-book, see above	2016
EXAM-HRA	• Final reports completed in May 2015 • Links to OECD NEA Report NEA/CSNI/R(2015)1, “Joint CSNI WGHOF/WGRISK report on Establishing Desirable Attributes of Current Human Reliability Assessment (HRA) Techniques in Nuclear Risk Assessment”	See guidance documents listed above	2016
DIGREL	• Project on Digital Systems reliability covering I&C hardware and software FMEA, Operating experience – parameter estimation hardware and software and Fault tree modelling and quantification • Important items for further activities (from seminar) • Approach to comprehensive safety justification is needed. PSA is part of the justification. • How to analyse initiating events caused by spurious actuations of software systems (common-cause initiators) • How to capture spurious signals from the I&C system; these are not fully captured in the PSAs today • How should data for a digital I&C system be compiled. How should this project and International Common-cause Failure Data Exchange (ICDE) project co-operate	See guidance documents listed above	2012-2015

NPSAG R&D Projects			
Title	Scope	Reporting	Period /completed
Guidance for quantification and result presentation and evaluation	Some conclusions: • Result evaluation can be developed, e.g. different contributors varying degree of conservatisms/uncertainty need to be clarified. • Extending the use of sensitivity analyses and with a focus on increasing credibility of results. • Provide more information on plant strengths in addition to weaknesses	Final Report (in Swedish except the survey appendix)	2014-2015
HRA Dependencies	• Phase 1 2015 included recommendations on consideration of dependencies in HRA • Further work in 2016: o Suggest efficient ways to identify important human actions need for dependency evaluations o Implement the recommendations in the selected plant models o Evaluate how the implementation would influence the PSA results. • Plans for HRA work on errors of commission in 2017.	Phase 1 report, se guidance and R&D reports above,	2015
T-book	T-book: New T-book version 8 published end 2015 • For all pumps and some valves previous q+ƛ*t model replaced by a ƛ*t model • Based on data on component failures reported until 2012 – 438 reactor operating years from Swedish NPPs + TVO, Finland. Planning for T-book 8 taking into account R&D work reported during the last two years: o Component grouping o Homogeneous grouping o + more data available		2015
Maintenance of HIDEP CLM (CCF method)	Documentation of the method in a theory manual.	Will be published as an SSM report in 2017.	2016-2017
Application of ASME PRA Standard on Nordic PSA	This project includes a pre-study with a limited evaluation of how Swedish PSA studies generally comply with ASME PRA Standard requirements. Utilities also made their own evaluations.	Pre-study report in list above.	2012-2015

10. INTERNATIONAL CO-OPERATION

Over the years, international contacts have increased, especially with partners in Europe (initiated by BWROG and EU-research contacts). This is in line with the group's aim to create a common and lasting basis for the performance of PSA and for risk-informed applications of PSA in Europe.

Sweden also participates in the OECD/ICDE and OECD/FIRE projects. Since the previous report on use and development of PSA, Sweden left the OECD/OPDE project (since some years this is the CODAP project). SSM and Sweden was one of the main stakeholders in OPDE and OPDE results are used to develop the R-book being the basis for pipe rupture frequencies in the PSAs. PSA group at SSM acts as the National Coordinator in ICDE. NBSG is national coordinator in FIRE.

NPSAG meets three times a year to discuss and prioritise project proposals. NPSAG has a report outlining the strategy, goals and purposes including Program and Roadmaps for 2014 up to 2016 on topics that are identified as needing some further R&D [4].

Note that projects also can be initiated directly by SSM and financed only by SSM. There are also many projects that get funding via both SSM, NPSAG and NKS (and also some co-operation projects with Finland that are also co-funded by Finnish state R&D budget.

SSM is also aiming at co-ordination directly with STUK, CNSC and the NRC. Several telephone meetings and exchange of information is made during 2014-2015. Exchange cover information on ongoing activities and positions, e.g. Site (multi-unit) PSA, site safety goals and integrated site risk.

SSM is a member also of NBSG (NBSG = Nordic Fire safety group) with fire specialist from SSM, FKA, RAB, OKG, SKB. This group has 3-4 meetings per year. NBSG scope of work include NPP fire safety and ordinary fire safety. NBSG plan and initiate research projects on fire-related topics and supervises the OECD/FIRE and OECD/PRISME projects. PSA group at SSM acts as the National Coordinator in these projects with NBSG being a member in PRISME management board and Lund technical high school is a member in the test programme reviewing board.

SAFIR

Through Finland and SAFIR (Finnish research programme), SSM and Sweden co-ordinate certain activities. SSM was a member in reference group 8 for the SAFIR 2014 programme. Group 8 cover PSA and related topics.

SAFIR activities with some SSM involvement during 2015-2018 (SAFIR2018 programme) are:

- PRAMEA
- EXWE
- SAUNA - MODIG

Activities in SAFIR where SSM is interested are related to SSM own needs and to NPSAG interests.

For PRAMEA it is Level 3, multi-unit PSA and HRA. A final report VTT-R-04580-15 "Multi-Unit PRA - Literature review" was completed in December 2015.

For EXWE it is severe weather including freezing precipitation and also space weather.

For SAUNA-MODIG it is assessment of defence in depth by PSA with an emphasis on I&C. Topics covered include an approach to analyse spurious actuations, follow-up in previous DIGREL recommendations and preparation of a proposal for an international collaboration on the development of a systematic approach for the diversity assessment of digital I&C systems for PSA. SAUNA-MODIG also looks at

Internally at SSM:

A project on Defence in Depth and PSA was performed from 2008-2012 with several papers presented at PSAM conference series. The final report was available in the beginning of 2013 and eventually published as an SSM report in the beginning of 2015 (see list of reports above). The project was about better understanding 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 better treat these aspects and new findings with the traditional PSA technique.

SSM has been working on development of supervisions planning strategies in many years. For a long time it is expected that SSM:s supervision is conducted according to a graded approach, similar as SSM and the community expects the licensees to work with a graded approach. Graded approach meaning that more attention and resources are spent on areas and issues where the return in radiation safety is best. Internal work was performed in 2014. This work was documented in a report in Swedish and was also presented in a paper at the ANS2015 PSA conference in Sun Valley, Idaho [3].

SSM is developing a tool for rapid source term prediction (RASTEP) [5]. This is a large project that has been ongoing for more than 5 years. The tool uses PSA model data and results as input.

Parallel to the supervision planning work and living PSA structure put in place, SSM and the PSA group are developing a risk map [1].

SSM hosted the Nordic PSA castle meeting in spring 2013 [6]. One main theme was about living PSA. This is discussed above.

Outlook

NPSAG work continues with efforts on multi-unit and site PSA, HRA dependency work. One important area is also on treatment, interpretation and evaluation of results taking uncertainties into account. Risk aggregation, is discussed also as part on how to interpret results from different scope including in multi-unit and multi-source cases.

SSM has also identified a need to look into more details in PSA level 2, both probabilistic parts and also the source terms. One main reason for this is ongoing work to develop a tool for rapid source term prediction (RASTEP) mentioned above. This tool uses PSA information and it is therefore important that the PSA model is qualified for this use.

References

Most references are listed above and are not repeated here.

[1] Olofsson, Ralph Nyman, Per Hellström, “Mapping the Risks of Swedish NPPs to Facilitate a Risk-Informed Regulation”, paper presented at PSAM12, Honolulu, 22-27 June 2014.

[2] SSM orders on analysis of radiological consequences, SSM2008/1945-6 (Oskarshamn), SSM2008/1945-7 (Ringhals) and SSM2008/1945-8 (Forsmark), SSM 2008.

[3] Per Hellström, “Graded Approach in Supervision Program and Strategies at SSM”, paper presented at ANS2015, Sun Valley, 26-30 April 2015.

[4] The Nordic PSA Group (NPSAG) strategy; Goals and purposes with NPSAG network, Appendix 1: Program and Roadmaps for 2014 up to 2016, NPSAG REPORT 00-001:1, NPSAG 2014.

[5] Michael Knochenhauer, Vidar Hedtjärn Swaling, Per Alfheim, ”Using Bayesian Belief Network (BBN) Modelling for Rapid Source Term Prediction – RASTEP Phase 1, NKS267, 2012.

[6] Ralph Nyman, Per Hellström, Frida Olofsson, PSA Castle Meeting in April 2013: LPSA Workshop Summary, NPSAG 00-004:1.

APPENDIX: STATUS OF PSA IN SWEDEN BY END DECEMBER 2016

Low electricity price is one reason behind decisions by utilities in 2016 to permanently shut down four NPPs in Sweden. O2 will not restart after the extensive modernisation and power uprate project PLEX and O1 will close in 2017. R2 and R1 will close in 2019 and 2020 respectively. This will have an impact on PSA activities. After shutdown of the four units, there will be six remaining: Westinghouse PWR: Ringhals 3 and 4; ASEA ATOM BWR: Forsmark 1-3 and Oskarshamn 3 representing three NPP generations: R34-R4, F1-F2 and F3-O3 with F3 and O3 being the newest. Operation of these six units is expected to continue at least until about 2040.

The table below presents the scope of the PSAs. Note that all PSA are updated regularly according to living PSA procedure described separately and being implemented since 2014. A full PSA reporting is delivered to SSM every third year and intermediate reporting years in between. Even a full reporting may be limited to a statement that the previous version is still applicable if plant changes, methodology changes and new operating experience not is affecting the PSA results. Utilities also in many cases have separate intermediate versions for internal use to support decision making in various internal issues.

In principle, all hazards are within the scope for all PSAs even if they may be screened out in some cases. All hazards refer to BoP events as LOCA and transients including CCI:s, Internal Fire, Internal Flooding, drop of equipment and External Events.

Status of PSAs in Sweden by end December 2016										
	Oskarsham			**Forsmark**			**Ringhals**			
	BWR	**BWR**	**BWR**	**BWR**	**BWR**	**BWR**	**BWR**	**PWR**	**PWR**	**PWR**
	Unit 1	**Unit 2**	**Unit 3**	**Unit 1**	**Unit 2**	**Unit 3**	**Unit 1**	**Unit 2**	**Unit 3**	**Unit 4**
Operating status	To be closed	Closed 2016	Operating	Operating	Operating	Operating	To be closed	To be closed 2019	Operating	Operating
Level 1										
Power operation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Shutdown, - restart	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Refuelling	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Level 2										
Power operation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Shutdown, - restart	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Refuelling	Y	Y	Y	N	N	N	Y, area events planned for 2017	Y	Y	Y

SWITZERLAND

1. INTRODUCTION

The development of the first probabilistic safety assessment (PSA) for a Swiss nuclear power plant (NPP) 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 (ENSI) required the utilities to perform full power Level 1 and Level 2 PSAs for all Swiss nuclear power plants. Four years later, the development of plant-specific low power and shutdown PSAs, including external events was required.

After the initial phase of development and review of various PSA models, 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 process to maintaining their plant-specific "living PSA". The implementation of "living PSA" at all plants was completed in 2005.

In February 2005, a new Nuclear Energy law (Nuclear Energy Act, NEA SR 732.1) and an accompanying ordinance (NEO SR 732.11) were enacted in Switzerland. Since the ordinance requires a full-scope, plant-specific Level 1 and Level 2 PSA for all relevant operational modes, Level 2 PSAs were extended to include low power and shutdown.

Another major task was the updating of the probabilistic seismic hazard analysis. To comply with an ENSI requirement, the nuclear power plant operators carried out a thorough investigation into the seismic hazard at the NPP sites from 2001 to 2004 within the scope of the PEGASOS (German acronym for «probabilistic seismic hazard analysis for Swiss nuclear power plant sites») project.

After completion of the PEGASOS project, substantial new seismic data were gathered and significant new seismic models were developed both in Switzerland and worldwide. In 2008, the NPP operators launched the «PEGASOS Refinement Project» (PRP) with the aim of reducing the spread of the hazard analysis results by incorporating the new data and models. Due to review concerns identified by ENSI, a hybrid model was assembled from PRP and the national seismic hazard study. The final hazard results were enacted under the German denomination «Erdbebengefährdungsannahmen ENSI-2015».

The Nuclear Energy Ordinance anchors the development and application of the PSA in the regulation and requires the derivation of corresponding supporting guidelines. The quality and scope of the PSA as well as the application of the PSA were further specified in two guidelines (ENSI-A05 and ENSI-A06).

All Swiss NPPs maintain plant-specific Level 1 and Level 2 studies, including internal and external events such as fire, flooding, earthquakes, aircraft impacts and high winds. Full power as well as low power and shutdown modes are considered in both the Level 1 and Level 2 PSA.

Extensive reviews of the PSAs assure similar high level of quality and some degree of harmonisation for all licensees. In general, PSAs are continuously improved and refined such that applications like a comprehensive system or component importance analysis or a probabilistic event analysis can be conducted often without additional modelling effort.

2. PSA FRAMEWORK AND ENVIRONMENT

The objective of PSA is to estimate the risk of beyond-design-basis accidents. Additional objectives are to draw conclusions about the existence of vulnerabilities in the installation and to provide insights into meaningful plant improvements to reduce the risk.

Regulatory Framework

According to Art. 4, Para. 3 of the Nuclear Energy Act (NEA, SR 732.1), licence holders of nuclear installations have to take all safety measures that are necessary based on the operating experience and the state of the art in science and technology, and have to seek to further reduce the risk to the extent appropriate. PSA is an internationally established tool to identify improvements to the safety of nuclear installations and to assess the effectiveness of the corresponding measures.

The use and the scope of PSA are addressed explicitly in the accompanying ordinances of the NEA.

- The Nuclear Energy Ordinance (NEO, SR 732.11) requires the completion of a plant-specific Level 1 and Level 2 PSA and regulates the involvement of PSA in the licensing and regulatory process for nuclear installations. The NEO requires the assessment of the safety level from the PSA point of view and that the effects on plant risk from proposed plant modifications and events using an up-to-date, plant-specific PSA be evaluated.
- The NEO requires (by a department ordinance established with the "DETEC Ordinance on hazard assumptions and assessment of protection against accidents at nuclear installations", SR 732.112.2) among others sufficient protection from natural hazards. According to the DETEC Ordinance (Art. 5, Para. 3) the corresponding safety analysis/proofs shall be based on site-specific probabilistic hazard analysis (e.g. earthquakes). Furthermore, Art. 12 of the DETEC Ordinance includes requirements for existing nuclear power plants with respect to the probabilistic assessment of the safety level and the balance of risk contributions from beyond-design-basis accidents.

Requirements regarding the development and application of PSAs are further specified in two regulatory guidelines aimed at harmonising the use and development of PSA:

- Guideline ENSI-A05, PSA: Quality and Scope[12]

[12] www.ensi.ch/en/wp-content/uploads/sites/5/2014/02/ensi-a05_e.pdf

- Guideline ENSI-A06, PSA: Applications[13]

A description of the content of both guidelines is included in Chapter 5.

In order to have a comprehensive, balanced and adequate decision-making process, ENSI has implemented an integrated regulatory safety oversight process. Plant-specific risk assessment is one element of the integrated regulatory safety oversight process.

PSA Users and Developers

Every licensee develops and maintains a plant-specific PSA. The PSAs are independently assessed by ENSI. The Paul Scherrer Institute (PSI) supports ENSI's review activities and performs research in the field of PSA with a focus on human reliability analysis (HRA). The licensees and the regulator ENSI both contract external Swiss and international experts to support their work.

Evolution after Fukushima

There was no need to revise the regulations concerning PSA due to the Fukushima accident. External events are comprehensively addressed. Processes to reassess external hazards according to the latest state of the art are implemented. Updates and refinements of the PSAs are conducted.

– SAFETY CRITERIA

The Nuclear Energy Ordinance (NEO, SR 732.11) anchors PSA applications into the law and defines fundamental directions for the decision-making process relevant to PSA as follows:

- For the construction permit of new nuclear power plant, the applicants need to demonstrate that the estimated Core Damage Frequency (CDF) is less than 1E-5 per year. To the extent that is feasible and reasonably achievable, this CDF criterion is also expected to be met by the operating plants.
- The risk impact of plant modifications, findings and events shall be assessed systematically using plant-specific PSAs.

On the basis of the NEO, the Swiss Federal Department of Environment, Transport, Energy and Communication (DETEC) released a DETEC Ordinance on the Hazard Assumptions and the Assessment of the Protection against Accidents in Nuclear Installations (SR 732.112.2). This DETEC Ordinance requires that:

- the frequency of core damage for existing nuclear power plants is less than 1E-4/a,
- at a frequency of core damage between 1E-4/a and 1E-5/a for existing nuclear power plants, all reasonable precautions have been taken,
- the risk contributions of beyond-design-basis accidents are balanced,
- the frequency of releases of radioactive substances in perilous amounts is noticeably lower than the frequency of core damage.

[13] www.ensi.ch/en/wp-content/uploads/sites/5/2009/03/ENSI-A06_Edition_2015-11_E_web.pdf.

The risk assessments and risk criteria addressed by the above-mentioned ordinances are further specified in Guideline ENSI-A06. This guideline introduces risk criteria for some mandatory PSA applications (see Chapter 7 of the Swiss contribution of this report).

Beznau NPP is the only twin-unit in Switzerland. The corresponding PSA considers potential dependencies between the units (in particular in case of an external event). However, there is not a specific multi-unit risk criterion.

The reactor accident at the Fukushima Daiichi power plant did not induce a modification of the safety criteria.

– STATUS AND SCOPE OF PSA IN SWITZERLAND

All Swiss NPPs maintain plant-specific Level 1 and Level 2 studies, including internal and external events such as fire, flooding, earthquakes, aircraft impacts and high winds. Full power as well as low power and shutdown modes are considered in both the Level 1 and Level 2 PSA. The development of a Level 3 PSA is not foreseen according to the Swiss regulations.

The major tasks in the last decade were:

- Seismic hazard: In 2008, the NPP operators launched a project ("PEGASOS Refinement Project", PRP) to refine the seismic hazard analysis by incorporating new data and models gathered since the completion of the PEGASOS project (SSHAC Level 4 seismic hazard analysis completed in 2004).
- ENSI assessed the achieved refinements to be well-founded in the project focal points which were the «ground motion characterisation» (subproject 2) and the «site response characterisation» (subproject 3). In contrast, the «seismic source characterisation» (subproject 1) was not investigated in sufficient detail, according to ENSI. Due to the reservations concerning PRP subproject 1, ENSI developed a hybrid model in which the model part of PRP subproject 1 was replaced by the corresponding model part of the Swiss Seismological Service. In May 2016, ENSI ordered the implementation of the results of the hybrid model, denoted as seismic hazard assumptions ENSI-2015 (in German «Erdbebengefährdungsannahmen ENSI-2015»).
- Fragility analyses: Many of the seismic fragilities were revised and refined. Extensive walkdowns were conducted in order to re-evaluate the specific assumptions of the fragility analyses, e.g. also regarding seismic interaction or seismically-induced fires and floods.
- Extreme weather hazards: A systematic re-investigation of the hazard of extreme meteorological events was required by ENSI, including the development of site-specific hazard curves for the major events such as high/low air and river temperatures, high winds, heavy rains, snowfalls and tornadoes.
- External flood hazard analysis: For each site the external flooding hazard was reassessed by updating the data (including historical flood events) and using 2D modelling considering sediment transport. Various scenarios involving blockages or break of water control structures or dam failure were computed.
- The Mühleberg NPP plant will be disconnected from the grid in December 2019. The relevant accident sequences of the initial "cooldown" phase of the decommissioning process were analysed using PSA.

– PSA METHODOLOGY AND DATA

– PSA STANDARDS AND GUIDANCE

Requirements regarding the development and application of PSAs are primarily specified in two guidelines that are described below:

- *Guideline ENSI-A05 (Probabilistic Safety Analysis (PSA): Quality and Scope):* This guideline specifies the quality and scope of a PSA, designates acceptable PSA methods for specific PSA areas, defines the fundamental risk parameters and prescribes the representation of the overall results in the PSA. The guideline contains requirements for a Level 1 and Level 2 PSA for nuclear power plants, as well as for other nuclear installations. Furthermore, it is structured in such a way that it first addresses requirements for a power operation PSA and then addresses the specific features that have to be considered for non-full-power operation. Thus, for example, in the Level 2 PSA investigation of severe accident phenomena that could be particularly relevant during non-full-power operation (such as a zirconium fire) is required. Besides the basic requirements, the guideline designates specific acceptable methods (e.g. methods for the determination of common-cause failure (CCF) or HRA parameters). For the analysis of two external events, tornado and (accidental) aircraft crash, the guideline institutes requirements regarding the approaches to be used. For determining the earthquake hazard, the SSHAC (Senior Seismic Hazard Analysis Committee) procedure is prescribed.
- *Guideline ENSI-A06 (Probabilistic Safety Analysis (PSA): Applications)*: This guideline defines the role of PSA in the regulatory oversight, general principles for all PSA applications, the scope of mandatory PSA applications and risk criteria for some PSA applications.

Quality Assurance (QA) and Peer Review

The quality and scope requirements of the Guideline ENSI-A05 shall ensure that in particular the mandatory PSA applications (see Chapter 7 of the Swiss contribution of this report) are possible.

Furthermore, Guideline ENSI-A05 (Chapter 6.1) requires that:

- The development, update and application of the PSA shall be performed within the overall QA programme of the licensee. The QA programme shall define specific QA requirements for PSA issues.
- The team conducting a new PSA or an update of a PSA shall consist of members having a profound knowledge of PSA techniques and of the characteristics of the installation.
- The licensee shall be strongly involved in the development, update and application of the PSA and shall review and approve (sign-off) the PSA documents.
- The PSA shall be continuously improved.
- A newly developed PSA or a comprehensive update of the PSA should be subjected to a peer review by a team of PSA practitioners who are independent of the PSA developing team. The peer reviewers’ comments shall be made an integral part of the PSA documentation.

Regulatory Review

The requirements of Guideline ENSI-A05 form the main basis of the regulatory review of the PSA studies. The regulatory review aims to develop a thorough understanding of plant attributes, its vulnerability to potential severe accidents and plant-specific operating characteristics. The review focuses on a general evaluation of PSA models, assumptions, analytical methods, data and numerical results and also focuses on understanding the range of uncertainties in core damage frequency, fuel damage frequency, containment performance and radioactive releases. At the beginning of the review process, ENSI verifies whether the PSA documentation is complete and assesses the PSA approach and analytical methods, as well as the plant design features intended to prevent and mitigate potential severe accidents. Based on the results of this evaluation, the Inspectorate submits requests for additional information to the licensee and its responses are used in the review. In addition, site audits, including plant walk downs, are conducted. A detailed regulatory review of the PSA is conducted in particular within the periodic safety review. To support this detailed review ENSI updates its own plant-specific PSA-models.

Source Data

In general, plant-specific reliability data are required. Guideline ENSI-A05 is not specific regarding the generic reliability data or initiating event frequencies to be used. There are however, a few exceptions listed below:

- Turbine Missiles: a distribution based on the international literature is given
- Airplane crash: the distribution of the crash rate in the vicinity of an airport is given
- Tornado: the mean annual frequency of tornado events is given

A Bayesian update is generally required in order to incorporate the plant-specific operating experience into the failure rates and the initiating event frequencies.

Methodology

In Switzerland, the linked event tree as well as the linked fault tree methodology are 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. Integrated models allow the propagation of Level 1 cutsets into Level 2 and allow for an appropriate consideration of dependencies in the HRA and of CCF events if components are used in the Level 1 and the Level 2.

Guideline ENSI-A05 designates requirements on methods. For a number of issues the guideline specifically lists acceptable methods. The licensees are authorised to use a methods not mentioned in the guideline provided that the methods guarantee at least an equivalent level quality.

In the following, the methods mentioned in the Guideline ENSI-A05 are sketched:

- Component reliability: Component reliability parameters shall be derived from a Bayesian update combining the plant-specific experience with generic reliability data from accepted international references.
- Common Cause Failures: 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 and generic data. CCFs shall be modelled for

components known to have significant coupling factors with regards to CCFs (i.e. design, operational and maintenance conditions)

- Human Reliability Analysis: For Category A and B Actions, THERP (Technique for Human Error Rate Prediction), ASEP (Accident Sequence Evaluation Program) and statistical methods are accepted. For Category C Actions SLIM (Success Likelihood Index Methodology), ASEP and THERP are accepted. A seismic HRA model is provided as well. Dependency within a task (e.g. calibration and subsequent testing) and between tasks is required to be examined, quantified and documented.
- Initiating Event Frequencies: Initiating event frequencies (in particular for internal events) are required to be derived from a Bayesian update combination the plant-specific experience with generic initiating event frequencies from accepted international references.
- Turbine Missiles: A generic frequency distribution is provided in the guideline and Bayesian update using plant-specific experience is required.
- Earthquakes: Compliance with the SSHAC methodology is required for the hazard analysis. A walkdown according to international standards (e.g. EPRI-NP-6041) shall be performed and fragility parameters shall be assessed.
- Extreme Winds: Site-specific and long-term measurement shall be used for the data fit and extrapolation.
- Tornadoes: The mean annual frequencies of tornadoes of different tornado sizes are given in the guideline.
- Airplane crashes: A specific method (labelled 4-factor formula) to determine the airplane crash frequency is provided in the guideline.

– NOTABLE RESULTS OF PSAs

According to the latest results of probabilistic safety analyses, the safety objectives of the IAEA for existing nuclear power plants[14] – recommending a core damage frequency of less than 1E-4 per year and recommending a large early release frequency of less than 1E-5 per year – are met by all Swiss nuclear power plants.

The Swiss licensees published a summary of the PSA results in the framework of the EU-stress test. The results concerning CDF und LERF are:

	NPP Beznau	NPP Gösgen	NPP Leibstadt	NPP Mühleberg
Total CDF/a	1.71E-05	3.42E-06	3.91E-06	2.65E-05
Total LERF/a	3.06E-06	5.93E-07	3.2E-07	<1E-05

[14] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999)

Over the years, the PSA allowed for the identification of many safety improvements. The following improvements were identified and implemented by the plants:

Each Swiss nuclear power plant has a bunkered system for heat removal. For the newest plants, the bunkered system was planned for and installed during the construction of the plant. For the older plants, it was installed afterwards.

Many seismic improvements were accomplished over the years as a result of the various seismic risk reassessments. Walls, cable trays and anchorages were reinforced, and components specifically designed to withstand high ground accelerations were installed.

PSA provided insights that lead to improvements of the technical specifications and emergency operating procedures. In addition, plant-specific sets of Severe Accident Management Guidelines (SAMG) were developed. The Level 2 PSAs served as a technical basis.

Mobile equipment (pumps, diesel generators, etc.) were installed at each the plant site. A separate warehouse with additional material such as diesel generators and pumps was established to offer all Swiss plants additional options in the case an external event would damage corresponding on-site equipment.

– PSA APPLICATIONS

Overview

With the aim of identifying potential plant improvements, Guideline ENSI-A06 specifies the scope of mandatory PSA applications:

- Probabilistic evaluation of the safety level
- Evaluation of the balance of risk contributors
- Probabilistic evaluation of the technical specifications
- Probabilistic evaluation of changes to structures and systems
- Risk significance of components
- Probabilistic evaluation of operational experience, including reportable events.

In addition, various elements of the PSA are used as an input for other regulations (e.g. the hazard results contribute to define the load level of the design-basis accident).

Description of the Applications

The above-mentioned applications are described in the following in more detail:

- *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 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.
- *Evaluation of the balance of risk contributors*: 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. Guideline ENSI-A06 provides criteria for the evaluation of the balance of the risk contribution of the initiating event categories defined in Guideline ENSI-A05.

- *Probabilistic evaluation of the 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 are considered in the technical specifications (completeness) and assigned to adequate 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 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 during a calendar year shall be planned in such a way that a) no component unavailability configuration caused by 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 (annual) Incremental Cumulative Core Damage Probability (ICumCDP) caused by maintenance is less than 5·E-7.

Compliance with the above-mentioned requirements shall be demonstrated either by a previously conducted 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.

- *Probabilistic evaluation of changes to structures and systems*: 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 Guideline ENSI- A06.

- *Risk significance of 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:

$$\mathrm{FV} \geq 1\mathrm{E}\text{-}3 \text{ or } \mathrm{RAW} \geq 2$$

  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 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).

- Probabilistic evaluation of operational experience, including reportable events. 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 aspects 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. As part of its review ENSI incorporates all the data into a database.

Evaluation of Reportable Events: 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, Guideline ENSI-A06 provides a relationship between the cumulative conditional risk of an event and the INES Scale.

In addition, the following analyses are part of or related to the PSA:

- Probabilistic hazard assessment for external events. The hazard results are used for both the PSA and the determination of the load level to be applied in the deterministic safety proofs.
- Categorisation of accidents according to their frequency. Based on their frequency, accidents are defined as design basis or beyond-design-basis. For design-basis accidents, different dose limits are set according to the frequencies.
- Fragility analyses for seismic and wind. The fragility analyses are used for both the
- PSA and the deterministic safety proofs.
- Development of Severe Accident Management Guidances (SAMGs). The Level 2 PSA is used as a technical basis for the development of SAMGs. In particular, the Level 2 PSA provides analyses of severe accident phenomena, indications of the completeness of the SAMGs and information that can lead to the prioritisation of measures. SAMGs have been developed for all Swiss nuclear power plants.

8. FUTURE DEVELOPMENTS AND RESEARCH

Switzerland supports research and development in the following fields:

- *Data Collection*: ENSI is a member of ICDE (International Common Cause Failure

Data Exchange) and OECD-FIRE (OECD Fire Incident Records Exchange).

- Human Reliability Analysis (HRA): ENSI funds a research project on HRA methodology at the Paul Scherrer Institute (PSI). The work focuses on the further development of a method for quantifying decision-related errors, in particular for errors of commission. In previous work, PSI developed the CESA method for EOC identification and performed pilot applications. CESA has been used to investigate EOCs for three Swiss NPPs in the framework of pilot studies. The Bayesian Belief Networks (BBN) is investigated as a means to expand the CESA method by allowing a graphical representation of the dependencies between stochastic variables, thus reducing the subjectivity of expert judgement. The application of the Bayesian methods is also investigated for human error predictions using simulator studies, where a HEP derived from a conventional HRA methodology is used as a prior and simulator results are used to update this prior.

- External Flood Hazard: The aim of this project is to reassess the existing hazard analysis from the Aare river and from the Rhine. The main study started in January 2016 after the completion of an extensive preparatory work. This research involves the consideration of historical flooding events recorded since the 14th century.
- *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, simulation and prognosis, ADAM is used for training and as a tool for severe accident analysis and application to PSA Level 1 and 2 studies (e.g. review of success criteria, containment loads, accident source terms). ADAM uses a highly versatile graphical user interface, and allows to efficiently analyse potential scenarios of interest.
- *Severe Accidents*: ENSI supports a number of research projects concerning severe accidents.

The project conducted at the Royal Institute of Technology in Stockholm (KTH) on severe accident phenomena focuses a) on Melt-Structure-Water Interactions (MSWI) that may occur during a late phase of in-vessel core melt progression and b) on 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 major threats to containment integrity of BWR plants which employ ex-vessel cavity flooding in severe accident management.

ENSI funds a research project at PSI on MELCOR development in the area of air ingress and the effect of nitriding: This research project addresses the active role of nitrogen and ZrN formation in the air oxidation process by means of a coupled analytical and experimental investigation. A nitriding model is developed and formulated to be implementable into the severe accident analysis codes such as MELCOR and SCDAP.

In addition, ENSI participates in the OECD projects HYMERS (OECD Hydrogen Mitigation Experiments for Reactor Safety) and BSAF-2 (Benchmark Study of the Accident at the Fukushima Daiichi Nuclear Power Station).

– INTERNATIONAL ACTIVITIES

ENSI participates in the following international projects related to PSA:

- International Common-cause Data Exchange Project (ICDE)
- Fire Incident Record Exchange (FIRE)
- Working Group on External Events (WGEV)
- Working Group on Risk Assessment (WGRISK)
- Hydrogen Mitigation Experiments for Reactor Safety (HYMERES)
- Benchmark Study of the Accident at the Fukushima Daiichi Nuclear Power Station
- (BSAF-2)
- Melt-Structure-Water Interaction (MSWI)

UNITED KINGDOM

1. INTRODUCTION

This report presents an update on PSA developments in the United Kingdom since 2012. The sections below only include new important developments in this area; the section on regulatory framework provides general background for the use and development of PSA in the United Kingdom.

2. REGULATORY FRAMEWORK

PSA in the United Kingdom - Background

The Energy Act 2013 (TEA), which came into force on 1 April 2014, established the Office for Nuclear Regulation (ONR) as a statutory body and enforcing authority, separate and distinct from the Health and Safety Executive (HSE). ONR is responsible for the regulation of the purposes described in TEA, safety of prescribed installations (including conventional, or non-nuclear, health and safety), and the transport of civil radioactive material by road, rail and inland waterway in Great Britain (GB). ONR is also responsible for the regulation of nuclear security in the United Kingdom and ensuring compliance by the UK with international safeguards obligations.

Nuclear operators must also comply with the relevant statutory provisions of the Health and Safety at Work, etc. Act 1974 (HSWA). HSWA requires the operators of nuclear plants, 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 HSWA.

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.

PSAs are performed for all nuclear installations and new build in the United Kingdom to evaluate the design of the plant and to provide one of the inputs to determine whether the risk to members of the public and site workers is both tolerable and ALARP. An overview of the key PSA programmes in the United Kingdom is provided below. Further information is presented in chapter 3.

Generic Design Assessment

Generic Design Assessments (GDA) is a review process carried out by the regulatory organisations in the United Kingdom for new reactor designs that might be introduced into the UK . The GDA process (a step-wise approach) 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.

If the design is judged to be satisfactory, a Design Acceptance Confirmation (DAC) 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. GDA and nuclear site licensing are separate processes. A DAC does not guarantee that a subsequent site licensing application will be successful, as the latter phase covers further issues specific to site deployment including those associated with the operating organisation (the potential licensee).

The GDA process includes an assessment of the PSA which is carried out by ONR. Step 3 of the GDA has usually 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. Step 4 of the GDA includes a more detailed review of the PSA.

The GDA of the UK EPR designed by AREVA was completed in 2011 and the GDA of the AP1000 designed by Westinghouse was completed in March 2017. Reports have been published – see References [1] and [2] for the main reports and [3] and [4] for the reports on the assessment of the PSA. Currently GDAs are being carried for UK ABWR designed by Hitachi-GE (step 4) and for UK HPR1000 designed by General Nuclear System (step 1). Reports summarising some areas of ONR's review of the UK ABWR PSA have also been published [5]. A final report will be published at the end of step 4 review (expected by the end of 2017).

Construction and commissioning

ONR has completed the assessment for First Nuclear Safety Concrete for the UK EPR early in 2017. A site-specific PSA for the UK EPR is currently under development. This PSA will be considered as part of the regulatory review to consent start of construction of the nuclear island.

Commercial operation

Probabilistic techniques and numerical safety criteria have been used in the United Kingdom 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. For the Pre-Operational Safety Report (POSR), a full-scope Level 3 PSA was produced which addressed internal initiating events and internal and external hazards, and covered all the modes of operation of the plant including full-power operation, and low power and shutdown modes.

Requirement for a PSA

The Safety Assessment Principles SAPs [6] constitute the regulatory principles against which duty holders' safety cases and GDA are judged. They are the basis for ONR's nuclear safety assessment. The SAPs have been benchmarked against the International Atomic Energy Agency (IAEA) standards and the Western European Nuclear Regulators Association (WENRA) reference levels. The key SAPs applied within the regulatory assessment of PSA are the following:

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

The following are key numerical safety criteria given in the SAPs related to PSA (information on the basis and derivation of the above targets can be found in Annex 2 of the SAPs):

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

Guidance to ONR assessors in carrying out an assessment of a PSA is also provided in 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. The PSA TAG [7] provides a more detailed 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 United Kingdom, this relies heavily on the judgement, knowledge and experience of the ONR inspectors who are carrying out the assessment.

The International Atomic Energy Agency (IAEA) and Western European Nuclear Regulators Association (WENRA) standards and guidance expectations for the performance and use of PSA to demonstrate the robustness of designs and the latest Probabilistic Risk Assessment (PRA) standards issued by the American Nuclear Society (ANS/ASME) are embodied in ONR PSA SAPs and TAG.

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.

3. STATUS AND SCOPE OF PSA PROGRAMMES

UK AP1000 PSA GDA

Status

The AP1000 PSA was initially submitted to ONR in 2009 to support the GDA of the AP1000 Pre-Construction Safety Report (PCSR) (version 2011). The PSA submitted to ONR was at Level 2 with a simplified Level 3 PSA. It used the small event tree/large fault tree approach using CAFTA software developed by the Electric Power Research Institute (EPRI). The methods and data used in the PSA are well known, although not always up-to-date or aligned with the latest international good practice. This was later improved by a second submission of certain parts of the PSA in 2015.

Westinghouse Electric Company LLC (Westinghouse) completed GDA step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues required resolution prior to award of a DAC in March 2017, and before any nuclear safety-related construction can begin on site.

The initial assessment of the PSA by ONR is reported in ONR-GDA-AR-11-003 (November 2011) [4]. This concluded that, although there were many positive features of the PSA, it needed substantial improvements to adequately support the PCSR. This was particularly the case for the fire PSA and the internal events at-power PSA.

The initial fire PSA was considered by ONR to be a screening analysis for which both conservatisms and optimisms were identified. The internal events at-power PSA was considered by ONR to be excessively reliant on AP600 performance analysis and success criteria. ONR raised two GDA issues for these aspects of the PSA. A modern standard fire PSA needed, and an internal events at-power PSA needed to be developed which used AP1000 specific performance analysis and success criteria. These two GDA PSA issues would need to be addressed prior to awarding Westinghouse a DAC.

In 2014 Westinghouse re-entered GDA and submitted a new fire PSA and a new internal events at-power PSA. ONR completed assessment of these two new submissions in March 2017 (ONR-NR-AR-16-017 and ONR-NR-AR-16-018) [4].

For the internal fire PSA and internal events at-power PSA ONR concluded that the PSAs had been carried out adequately with respect to the relevant ASME/ANS standards, NUREG-CR/6850 guidance for the fire PSA and the ONR TAG on PSA.

However, ONR's assessment identified a number of shortfalls for each of these two PSAs for which assessment findings have been raised. These assessment findings need to be addressed by the future licensee. The shortfalls for the fire PSA concerned addressing a greater scope of fire targets in addition to cables and improving the completeness of the supporting fire analysis. Westinghouse used the fire PSA to undertake a systematic review of the potential for fire risk reduction measures. ONR identified that further work is needed during the licensing phase to justify whether there is a need for fire detection and suppression within a limited number of areas of the plant.

The shortfalls for the internal events at-power PSA included validation of operator error data used in the PSA, a more thorough treatment of dependency between initiating events and safety systems, ensuring that the treatment of containment bypass fault sequences is comprehensive, reviewing the methodology and data used for the treatment of common-cause failure and reviewing the treatment of plant damage states at the Level 1/Level 2 interface.

ONR concluded that Westinghouse had presented suitable and sufficient work to enable both of the GDA issues on PSA to be closed.

AP1000 Risks at Close of GDA

The table below presents the overall generic plant risks for the AP1000 reactor plant which are taken from the AP1000 PCSR (UKP-GW-GL-793 Revision 1: Chapter 10) [4].

Overall AP1000 Plant Risks at the Close of GDA (March 2017)

ONR Numerical Target 8 Dose > 1 000 mSv	Core Damage Frequency	ONR Numerical Target 9 ≥ 100 fatalities	Large Release Frequency
BSL 10^{-4}/year BSO 10^{-6}/year	9.4x10^{-7}/year	BSL 10^{-5}/year BSO 10^{-7}/year	6.8x10^{-8}/year
Contributors to the Overall Risks at GDA			
Internal fire at-power	6.7x10^{-7}/year	Internal fire at-power	5.6x10^{-8}/year
Internal events at-power	1.7x10^{-7}/year	Internal events at-power	1.2x10^{-8}/year
Internal events low power and shutdown	1x10^{-7}/year	Internal events low power and shutdown	Not reported
Internal flooding	4.4x10^{-9}/year	Internal flooding	1.2x10^{-9}/year

ONR's overall judgement from the GDA assessments presented in ONR-NR-AR-16-017 and ONR-NR-AR-16-018 [4] is that the risks measures quoted in the PCSR may rise as the assessment findings from GDA are included, and additional site hazards are assessed during the licensing phase. However, ONR Basic Safety Levels for large dose/large release fault sequences are likely to be met with a significant margin.

The PCSR (UKP-GW-GL-793 Revision 1) shows that the PSA has been used by Westinghouse during the process for developing the AP1000 reactor plant design from the AP600 reactor plant design. The ONR GDA close-out assessment of the internal events at-power and fire PSAs has not found any major areas of the plant design for which ALARP analysis is needed to consider alternative features. However, ONR's assessment does support findings which have ALARP implications for the detailed design phase. ONR concluded that the risks from internal events at-power and fire PSA are being managed ALARP as the AP1000 design process continues through GDA and into the licensing phase.

Scope

The scope of the AP1000 PSA presented for GDA is at Level 2 PSA but includes a simplified Level 3 PSA as follows:

- internal events at –power (loss-of-coolant accidents and intact circuit faults);

- internal hazards (fire and flood);
- internal events low power and shutdown plant operating states;
- internal hazards low power and shutdown (fire and flood);
- spent fuel pool PSA.

The risk measures provided are currently focused on core damage frequency and large early and late release frequencies.

Future developments

ONR expects that a full-scope site-specific PSA is developed for the AP1000 reactor plant to support the construction and operation of three AP1000 units at the UK Moorside site. This would also include the development of a risk monitor.

ONR is aware of a six year PSA development plan following completion of GDA and ending with granting the first ONR consent for 'nuclear' concrete at Moorside.

The initial PSA development stage is to address the ONR assessment findings that arose during the GDA process. This is followed by developing the internal events flooding PSA, and to develop the internal events fire and flood PSAs for low power and shutdown plant operating states. External hazards PSA will also be considered, but will at least include a site-specific seismic PSA. Multi-unit PSA work is also intended.

UK ABWR PSA GDA

Status

The GDA of the UK ABWR started in April 2013. During step 1 of GDA (April 2013 to January 2014), which is the preparatory part of the design assessment process, Hitachi-GE established its project management and technical teams and made arrangements for the GDA of its ABWR design. Also, during step 1 Hitachi-GE prepared submissions to be evaluated by the UK regulators during step 2. Step 2 was completed between January 2014 and August 2014, followed by step 3 between August 2014 and October 2015. Step 4 GDA started in November 2015 and is expected to be completed in December 2017.

The UK ABWR PSA for internal events at power was initially submitted to ONR to support step 3 of the GDA of the UK ABWR at the end of December 2014. Other PSA submissions, such as PSA methodologies were submitted to ONR in step 3 and 2.

Based upon the submissions made by Hitachi-GE during steps 2 and 3, ONR judged there were serious regulatory shortfalls associated with the development of a modern standards full-scope PSA for the UK ABWR, which would be suitable and sufficient for ONR to carry out a meaningful assessment within the project timescales. These had the potential to prevent provision of a DAC. In line with the guidance to requesting parties, ONR therefore raised Regulatory Issue (RI) RI-ABWR-0002 [8], to make regulatory expectations clear and to ensure that these shortfalls were addressed during GDA. The outcomes of ONR review were also captured in a series of related regulatory observations [9] and regulatory queries.

In response to RI-ABWR-0002, Hitachi-GE provided a project plan, revised PSA arrangements and extended PSA capability. As a result Hitachi-GE delivered a comprehensive UK ABWR PSA submission including consideration of internal events and hazards, for the reactor, spent fuel pool and other facilities for different operating modes. RI-ABWR-0002 was closed by ONR in February 2017 [5].

A number of ROs remain open, and are required to be closed within the GDA. The main area of regulatory focus for the remainder of GDA is ensuring the use of the PSA to inform the demonstration that the risk is ALARP. Hitachi-GE is expected to use the PSA to identify vulnerabilities or other areas where improvements to the UK ABWR design could be made in a systematic, transparent and auditable way. ONR has raised RO-ABWR-0076 [9] which will enable the regulatory follow-up of the work required as part of the ALARP demonstration.

Scope

The scope of Hitachi-GE step 4 PSA submission in response to RI-ABWR-0002 is comprehensive. This includes the UK ABWR internal events PSA for the reactor at power and shutdown operating modes, fuel route operations, spent fuel pool and consideration of other non-reactor facilities. The PSA also covers internal fire and flooding for the reactor at power, seismic events for the reactor and the spent fuel pool; pseudo quantitative analysis have been developed to assess the risk of the reactor shutdown operating states and SFP due to internal fire, flooding and seismic events.

A prioritisation of hazards has been developed for the reactor and non-reactor facilities, including consideration of combination of hazards; when hazards are considered important in terms of risk, more detailed studies are provided. Sensitivity analysis were undertaken to investigate the risk impact of external flooding and biological fouling events.

The PSA has in general covered Level 1, Level 2 and Level 3. Consequence analyses are also developed for non-core damage sequences leading to a release.

Future developments

Within GDA further developments are expected on the use of the PSA inform the demonstration that the risk is ALARP, including use of the PSA to risk inform the design.

Following GDA, the UK ABWR PSA will be developed into a full-scope site-specific PSA to support detailed design, construction, commissioning and operation of the UK ABWR. Two UK ABWR units are planned at the UK Wylfa Newydd site, followed by two additional units at the UK Oldbury site.

As for other new build PSAs in the United Kingdom, the PSA development will include addressing assessment findings from GDA, update of the PSA to include site-specific characteristics, consideration of multi-units, operational matters and PSA applications. For example it is expected that the PSA will be used to risk inform the design throughout detailed design development. Other PSA applications are also expected, including the development of a risk monitor and the necessary procedure/s to manage the risk at all times.

HPC PSA

Status

Two EPR^{TM} units are currently being constructed at the Hinkley Point C nuclear licensed site. Prior to a nuclear site licence being granted to the licensee [10] the EPR^{TM} design completed the UK GDA process, with the Design Acceptance Confirmation being issued in December 2012 [1]. As part of GDA, ONR reviewed the EPR PSA [11] in detail, which resulted in a number of GDA assessment findings for any future licensee to resolve [2].

The GDA PSA model has been further refined to make it more specific for the Hinkley Point site. This has included areas such as site-specific data (e.g. loss of offsite power and loss of ultimate heat sink frequencies), modelling of the Hinkley Point C heat sink design and inclusion of additional events, e.g. combined snow and wind. The results from this PSA model, known as the 'Design PSA', are summarised in the final version of the Hinkley Point C pre-construction safety report.

Scope

The scope of the Design PSA is level 1, 2 and 3 and all plant states (except for internal fire and flood which are full power only); it includes both the reactor and spent fuel pool. This is an asymmetric PSA model, in that all faults are assumed to occur in a single loop. In terms of hazards, other than those hazards implicitly captured within internal events (e.g. LOOP and LUHS) or captured only in the level 3 PSA (e.g. accidental aircraft impact) only internal fire, internal flood and combined snow and wind are explicitly modelled in the PSA. In addition a detailed seismic margins assessment was carried out as part of GDA.

In addition to the Design PSA, a number of risk-informed design PSA studies have been completed, which has included for example internal fire PSA, internal flood PSA and seismic PSA. Although these are not fully consistent with international standards, mainly due to the availability of design information and some limitations in scope, they are further refined than the studies completed at GDA.

Future developments

A new Hinkley Point C PSA is being developed that for internal events (including hazards resulting in LOOP and LUHS) will be issued in advance of the licensee commencing construction of the nuclear island. This PSA model is known as the Nuclear Island Concrete (NIC) PSA. The scope of the first issue of the NIC PSA will be level 1, 2 and 3 and all plant states. This will be a symmetric PSA model, in that faults in all loops and the associated safety system trains will be explicitly modelled.

In terms of hazards PSA, internal fire, flood and seismic PSAs consistent with international standards are anticipated to be developed based on the NIC PSA. Other hazard PSAs, where screened in, are also to be developed.

The NIC PSA will form the basis for the operational PSA, which is anticipated to be full-scope level 1, 2, and 3 for internal events and hazards. The operational PSA is anticipated to be sufficiently refined to support a wide range of risk-informed applications including a risk monitor.

Operating Reactors PSA

Status

There are currently 15 reactors operating in the United Kingdom, consisting of 14 AGRs and a single PWR, located on seven licenced sites. The PSAs for all operating reactors are "living PSAs", which are updated approximately every three years, or sooner if there are significant changes to plant or operations that require a more frequent update. The updates include revisions to Initiating Event Frequencies (IEFs), plant reliability data, hazards analysis and other modelling aspects.

EDF Energy, the sole licensee is managing the UK fleet to the end of operating life, which includes Plant Life Extension (PLEX).

Scope

The PSAs for the AGRs are hybrid PSAs and include a Level 1 PSA and elements of a Level 3 PSA in the form of off-site dose estimates. A Level 2 PSA has recently been carried out for one AGR (Hunterston B) that is representative of the fleet. Given that most of the AGR severe accident phenomena and mitigating actions are insensitive to the design of individual AGRs, the insights are being read across to other AGR stations to identify and implement improvements (for example to the Symptom Based Emergency Guidelines (SBERGs), which provide guidance on actions that should be attempted to restore the reactors to a safe shutdown state following a beyond-design-basis accident scenario).

AGR safety cases have evolved over their operational life and the PSAs have been used to justify that the risks are reduced ALARP. The current AGR PSAs cover at-power operations, supplemented by more simplistic risk assessments for shutdown operations and refuelling activities. External hazards, including seismic events, are also represented in the AGR PSAs.

The PWR at Sizewell B has a full-scope Level 1, 2 and 3 PSA. The Level 1 PSA is updated to provide an estimate of the core damage frequency (CDF) as part of the living PSA programme and this used to provide revised Level 2 and 3 dose/risk information.

PSA Results

The CDF for the PWR at Sizewell B is currently predicted to be ~ $1x10^{-5}$ per year. The CDF is an order of magnitude lower than the objective of $1x10^{-4}$ per reactor-year for existing plants identified in IAEA - Specific Safety Guide - SSG -3 [12], [13].

The individual risk to a person off-site from an accident on site resulting in exposure to ionising radiation is predicted to be ~ $2\ x10^{-7}$ per year. Target 7 of ONR's SAPs [6] provides the individual risk targets to a person off-site in terms of a Basic Safety Level (BSL) and a Basic Safety Objective (BSO), which are set at $1x10^{-4}$ per year and $1x10^{-6}$ per year respectively. The predicted individual risk at Sizewell B is a factor of 5 below the BSO, and therefore below the level considered to be broadly acceptable.

The risks from operation of the AGRs are presented in a different format and are reported as the frequency of accidents on a facility that could result in an off-site dose to a person in five dose bands (Target 8 of ONR's SAPs). Dose Band 5 represents an off-site dose greater than 1Sv, which has a BSL and BSO of $1x10^{-4}$ and $1x10^{-6}$ per year respectively. Fault sequences that are predicted to result in significant damage to the AGR fuel pins reside in the Dose Band 5 category. The predicted Dose Band 5 frequency is different for each AGR, to reflect design and operational differences. However, for all AGRs, this frequency is below the BSL of $1x10^{-4}$ per year and in the tolerable region as defined in the framework within the Tolerability of Risk from Nuclear Power Stations (TOR) [14], which has been translated into specific numerical targets within ONR's SAPs.

Future developments

Notable future developments to enhance PSA methods and approaches and provide additional risk insights, taking account of post-Fukushima improvements, include:

- Developing appropriate methods for incorporating long-term scenarios into PSA, modelling repair/recovery
- Developing appropriate PSA taking account of shared systems between facilities on multi-reactor sites and common initiating events

- Developing/enhancing approaches for representing intersystem common-cause failures (CCFs) and modelling digital C&I
- Developing PSA to end of station life

References

1. Summary of the GDA of the Électricité de France SA and AREVA NP SAS UK EPR™ nuclear reactor reports:

    - ONR, New nuclear power stations: Generic Design Assessment; Design Acceptance Confirmation for the UK EPR™ Reactor, EPR70475N, December 2012, www.onr.org.uk/new-reactors/reports/step-four/close-out/epr70475n.pdf

    - Summary of the GDA Issue close-out assessment of the Électricité de France SA and AREVA NP SAS UK EPR™ nuclear reactor. 13 December 2012. www.onr.org.uk/new-reactors/reports/step-four/close-out/summary.pdf

    - Summary of the detailed design assessment of the Électricité de France SA and AREVA NP SAS UK EPRTM nuclear reactor (Step 4 of the Generic Design Assessment process). 14 December 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ukepr-onr-gda-sr-11-001-rev-0.pdf

2. ONR-GDA-AR-11-019. Step 4 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR™ Reactor. 10 November 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ukepr-psa-onr-gda-ar-11-019-r-rev-0.pdf

3. Summary of the GDA of the Westinghouse Electric Company AP1000® Nuclear Reactor:

    - Summary of the GDA issue close-out assessment of the Westinghouse Electric Company AP1000® Nuclear Reactor. March 2017. www.onr.org.uk/new-reactors/ap1000/reports/ap1000-close-out-assessment-summary.pdf

    - Summary of the detailed design assessment of the Westinghouse Electric Company LLC AP1000® nuclear reactor (Step 4 of the Generic Design Assessment process). 14 December 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-onr-gda-sr-11-002-rev-0.pdf

4. GDA of the Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor:

    - ONR-NR-AR-16-017. Success Criteria for the Probabilistic Safety Analysis for the Westinghouse AP1000® Reactor (Internal Events At-Power). March 2017. www.onr.org.uk/new-reactors/ap1000/reports/assessment-reports/onr-nr-ar-16-017.pdf

    - ONR-NR-AR-16-018 . GDA close-out for the AP1000® Reactor GDA Issue GI-AP1000-PSA-02 (Fire PSA). March 2017. www.onr.org.uk/new-reactors/ap1000/reports/assessment-reports/onr-nr-ar-16-018.pdf

- ONR-GDA-AR-11-003. Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor. 10 November 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-psa-onr-gda-ar-11-003-r-rev-0.pdf

- Westinghouse, UKP-GW-GL-793 Revision 1. AP1000 Pre-Construction Safety Report. Chapter 10. www.westinghousenuclear.com/Portals/5/Other%20PDFs/UKP-GW-GL-793NP-sm.pdf

5. GDA of the Probabilistic Safety Analysis Assessment of Hitachi-GE's UK Advanced Boiling Water Reactor (ongoing):

    - ONR-NR-AR-16-091. Assessment of the response to RI-ABWR-0002 - UK ABWR Probabilistic Safety Analysis: Project Plan and Delivery. 23 February 2017. www.onr.org.uk/new-reactors/uk-abwr/reports/ri-abwr-0002-assessment-of-responses.pdf

    - ONR-GDA.-AR-14-003. Step 2 Assessment of the Probabilistic Safety Analysis (PSA) and Severe Accident Analysis (SAA) of Hitachi-GE's UK Advanced Boiling Water Reactor (UK ABWR). 28 August 2014. www.onr.org.uk/new-reactors/uk-abwr/reports/step2/uk-abwr-psa-step-2-assessment-executive-summary.pdf

6. Safety Assessment Principles for Nuclear Facilities 2014 Edition, Revision 0. November 2014. www.onr.org.uk/saps/saps2014.pdf

7. Technical Assessment Guides – Probabilistic Safety Analysis. NS-TAST-GD-030, Revision 5, November 2016. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-030.pdf

8. RI-ABWR-0002, UK ABWR Probabilistic Safety Analysis: Project Plan and Delivery. Revision 1, July 2015. www.onr.org.uk/new-reactors/uk-abwr/reports/ri-abwr-0002.pdf

9. UK ABWR PSA Regulatory Observations (www.onr.org.uk/new-reactors/uk-abwr/ro-res-plan.htm):

    - RO-ABWR-040, UK ABWR Probabilistic Safety Analysis: Identification of Applicable Internal Hazards, Revision 0, March 2015.
    - RO-ABWR-041, UK ABWR Probabilistic Safety Analysis: Identification of Applicable External Hazards, Revision 0, March 2015.
    - RO-ABWR-0042, Probabilistic Safety Analysis (PSA) internal initiating events at power, Revision 0, March 2015.
    - RO-ABWR-0046, Containment Performance Analyses, Revision 1, April 2016.
    - RO-ABWR-0048, Level 2 PSA methodology, Revision 0, April 2015.
    - RO-ABWR-0076, PSA ALARP Demonstration and Optioneering, Revision 0, November 2016.

10. ONR, Application for a Nuclear Site Licence to install and operate two EPRTM reactor units at Hinkley Point, ONR-HPC-PAR-12-043, Revision A, November 2012, www.onr.org.uk/pars/2012/hinkley-point-c-1.htm.

11. EDF and AREVA, UK EPR^{TM} Pre-Construction Safety Report (GDA 2011), www.epr-reactor.co.uk/scripts/ssmod/publigen/content/templates/show.asp?P=290&L=EN&id_cat=1.2.

12. IAEA Safety Standards - Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants for protecting people and the environment. No. SSG-3, Vienna (2010). www-pub.iaea.org/MTCD/publications/PDF/Pub1430_web.pdf

13. International Nuclear Safety Advisory Group - Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

14. The Tolerability of Risk from Nuclear Power Stations. The Stationery Office 1992 ISBN 0 11 886368 1. www.hse.gov.uk/nuclear/tolerability.pdf

UNITED STATES

1. INTRODUCTION

2. PRA FRAMEWORK AND ENVIRONMENT

The PRA Policy Statement

The US 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)[15] in US 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 defence-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, licence commitments, and staff practices. Where appropriate, PRA should be used to support the proposal of additional regulatory requirements in accordance with 10 CFR 50.109[16] (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.

PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

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 judgements 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 recognises that a single approach for incorporating risk analyses into the

[15] In the context of this report, the terms PSA and PRA are used interchangeably.

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

regulatory process is not appropriate. However, PRA methods and insights will be broadly applied to ensure that the best use is made of available techniques to foster consistency in NRC risk-based decision-making."

In issuing the policy statement, the Commission said it expected that the "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 towards 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) prioritising these challenges on the basis of risk significance, operating experience, and/or engineering judgement; (c) considering a broader range of countermeasures 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 PRA 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 characterises how risk information is used. In particular, they state that such information is one principle 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 PRA needed to support regulatory decisions can vary, stating that the "scope, level of detail, and technical adequacy of the PRA is to be commensurate with the

application for which it is intended and the role the PRA results play in the integrated decision process." For some applications and decisions, only particular parts of the PRA need to be used. In other applications, a full-scope PRA may be needed. General guidance regarding PRA scope, technical elements and their associated attributes and characteristics, level of detail of a PRA, and development, maintenance and upgrade of a PRA (i.e. plant representation) for a PRA is provided in the documents and in RG 1.200.

- While the documents are written in the context of one reactor regulatory activity (licence 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).[17] 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 categorising 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 programme. RG 1.205 and SRP 9.5.1.2 provide guidance on implementing this alternative to the traditional fire protection programme. 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.

Regarding advanced reactors (e.g. high-temperature gas-cooled reactors, liquid metal reactors, and small modular LWRs), the NRC staff has developed a plan that could be used 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 defence in depth to address uncertainties.

Regarding Post-Fukuhima efforts, the NRC established a Near Term Task Force (NTTF) to complete a near-term review required by the Chairman's March 23, 2011 tasking memorandum (COMGBJ-11-0002, "NRC Actions Following the Events in Japan"). In SECY-11-0093, "Near-Term Report and Recommendations for Agency Actions Following the Events in Japan," dated 12 July 2011, the NTTF provided its recommendations to the Commission. The first recommendation from the NTTF recommended establishing "a logical, systematic, and coherent regulatory framework for adequate protection that appropriately balances defense-in-depth and risk considerations." The staff recommended that 1) a design-basis extension category of events and requirements and associated internal

[17] 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).

NRC guidance, policies, and procedures be established; 2) Commission expectations for defence-in-depth through the development of a policy statement that includes: the definition, objectives, and principles of defence in depth; associated implementation guidance containing decision criteria for ensuring adequacy of defence in depth; and conforming guidance to ensure integration of defence in depth with risk be established, and (3) the role of voluntary industry initiatives in the NRC regulatory process be clarified by specifying when these initiatives may be credited and providing guidance regarding what type and level of licensee documentation and NRC oversight is appropriate for future industry initiatives. This recommendation was not accepted by the Commission to be handled under NRC's post-Fukushima actions (SRM SECY-13-0132), but instead to be addressed under staff activities in response to NUREG-2150, "A Proposed Risk Management Regulatory Framework." Although defense-in-depth was not formally addressed under post-Fukushima activities, the Commission directed the staff to develop a knowledge management tool of defence-in-depth observations and detailed history (this was published as NUREG/KM-009 "Historical Review and Observations of Defense-in-Depth" in April 2016). Regarding activities related to implementing a risk management regulatory framework (RMRF), in SRM SECY-15-0168, the Commission approved the staff's recommendation to maintain the existing regulatory framework and refrain from developing an overarching risk management policy statement. The Commission also directed the staff to complete expeditiously a revision to RG 1.174, "An Approach for Using Probabilistic Risk Assesment in Risk-Informed Decisions on Plant Sepecific Changes to the Licencing Basis," to clarifying defence-in-depth guidance. As a result, RG 1.174 is currently being revised.

Requirements for a PRA

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 PRA for operating plants (see discussion below on the MSPI, however). However, if a licensee chooses to adopt a risk-informed approach, then a PRA is required as discussed, for example, in RG 1.174. A condition for using PRA results in a risk-informed regulatory application is that the PRA is of sufficient technical adequacy to support the specific decision. The NRC's expectations for the technical adequacy of a PRA 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 5.US.

Regarding new reactors, 10 CFR 52.47 requires that an application for standard design certification contain, among other things, a design-specific PRA. Similarly, 10 CFR 52.79 requires that an application for a combined license contain a design-specific PRA. Additional requirements for PRA maintenance and upgrade are provided in 10 CFR 50.71 for holders of a combined license under 10 CFR 52.

Development of PRAs

As discussed further in Section 6.US, most US PRAs were developed by the licensees in response to Generic Letter (GL) 88-20 and to Supplement 4 of GL 88-20. GL 88-20 requested licensees to perform an Individual Plant Examination (IPE) for severe accident vulnerabilities associated with internal hazards (including internal flooding hazards but not internal fire hazards). Supplement 4 to GL 88-20 requested licensees to perform an Individual Plant Examination of External Events (IPEEE) for severe accident vulnerabilities associated with seismic events, internal fires, high winds and tornadoes, external floods, transportation and nearby facility accidents. 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 PRA. Prior to the implementation of the MSPI, the licensees had to demonstrate that their PRA models were of sufficient technical adequacy 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 PRAs. These primarily Level 1 PRAs 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 prioritisation of modelling issues to support agency efforts to improve PRA technical adequacy; providing support for the resolution of generic safety issues; and providing support to risk-informed reviews of licensing applications. SECY-15-124 discusses the status of the Accident Precursor Program and the SPAR models as of 2015.

3. SAFETY CRITERIA

As a result of the recommendations from the President’s Commission on the Accident at Three Mile Island (Kemeny, 1979), 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 defence 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 follow:

- 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 US 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 of core damage frequency (CDF) of 10^{-4}/reactor- year for latent cancer fatalities and a subsidiary objective of large early release frequency (LERF) of 10^{-5}/reactor- year for early cancer fatalities. 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, (ΔCDF) and LERF and changes in LERF (ΔLERF) for licence 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 (10^{-6}/reactor- year and 0.1, respectively) 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. STATUS AND SCOPE OF ONGOING PRA STUDIES

Since the publication of the landmark Reactor Safety Study (WASH-1400) in 1975, plant-specific PRAs have been completed for all operating US 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 PRAs. 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 programme 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 programme 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 programmes 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 PRA results and covering all operating US plants. The key results of the IPE programme are summarised in NUREG- 1560. Key results of the IPEEE programme are summarised in NUREG-1742.

Since the completion of the IPE and IPEEE programmes, licensees have continued to update their PRAs 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 PRAs, as well as example plant changes spurred or enabled by these PRAs.

The NRC has developed 79 Standardized Plant Analysis Risk (SPAR) models representing all operating commercial nuclear plants in the United States. and has performed a limited scope validation and verification of these models against licensee PRAs and other studies. Twenty-two of the SPAR models (representing 28 nuclear power units) include other hazard groups and are referred to as SPAR All-Hazard (SPAR-AHZ) Models. Eighteen of the SPAR-AHZ models are based on IPEEE information and the remainder are based on more recent external hazard information. 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 co-operative research with the Electric Power Research Institute (EPRI), and through industry peer reviews. The NRC has also developed a new reactor SPAR model for the AP1000 (internal hazards, seismic, flooding, internal fire, low power/shutdown, and Level 2 PRA), for the advanced BWR (GE & Toshiba), for the US advanced PWR and the US EPR. The NRC is in the process of developing plant-specific SPAR models for V.C Summer and Vogtle (AP1000 designs).

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

PRA objectives

The preceding PRAs 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 prioritise and justify safety changes. The Zion, Indian Point and Limerick studies addressed the risk to large nearby populations; the first two studies also addressed the risk reduction potential of particular accident mitigation strategies (e.g. filtered vented containments). The Oconee PRA was performed to demonstrate PRA methods, train PRA practitioners for utilities, and provide a model for future utility studies. NUREG/CR-4832 was performed to, in addition to characterising the risk for the LaSalle plant, develop, apply, and evaluate improved PRA 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 behaviour 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 standardised methods and data.

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

PRA level

All US 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 PRAs have been performed only for a few plants. For new reactors licensed under 10 CFR 52, each holder of a combined licence is required to develop a Level 1 and a Level 2 PRA before initial loading of the fuel. The PRA must cover those initiating events and modes for which NRC-endorsed consensus standards on PRA exist one year prior to the scheduled date for initial loading of fuel. NRC’s SPAR models are Level 1 PRAs; a small number of extended Level 1 models (to support LERF and Level 2 modelling) have also been developed.

Initiating hazards addressed

Most of the licensees’ PRAs for US plants address the full range of initiating events usually considered for internal hazards analyses (including different classes of loss-of-coolant events, transients, and support system failures).

Some of the US plant PRAs address seismic initiating events and others do not. As discussed in Section 5, US, some plants used simplified approaches, e.g. seismic margins studies aimed at identifying vulnerabilities to satisfy the requirements of the IPEEE programme, while not providing quantitative estimates of risk. In 2014, as part of its implementation of lessons learnt from the 2011 Fukushima accident in Japan, licensees submitted updated seismic hazard information in response to an NRC request for information. This information was requested per the NRC's NTTF recommendation 2.1 on re-evaluating seismic and flooding hazards by the 60 reactor sites. Based on the findings of its review of the updated seismic hazard, the NRC has requested that 21 reactor plants submit the results of a plant-specific seismic PRA and the insights related to updated earthquake risks. Similarly, 28 sites (44 units) have developed fire PRA models to support adoption of the NFPA 805 performance-based fire protection programme under 10 CFR 50.48(c). Only a limited number of plants have performed PRAs for other external hazards (e.g. high winds, external flooding, accidental aircraft crashes). Regarding high winds, the Nuclear Energy Institute (NEI) has proposed a simplified risk-informed approach to address instances where some portions of safety-related SSCs were not protected from tornado missiles. This approach would develop a generic "missile hit parameter" that could be used to estimate failure probabilities to be put into the plant-specific, internal hazards PRA. This work is under development and has not received NRC approval at this time. As discussed above, new reactors are required to address external hazards since the NRC staff has endorsed the latest combined ASME/ANS Standard on PRA.

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 hazards. Work is ongoing to develop models to address internal fires.

Modes of operation addressed

Most of the current licensee PRAs are limited to consideration of events occurring during full- power operation. Only a few PRAs 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 PRAs 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.

PRA updates

When used to support risk-informed regulatory applications, PRAs are required to reflect current plant conditions relevant to the application. For example, if a licensee implements a risk-informed fire protection programme, the PRA it uses to evaluate risk is required to reflect the as-built, as-operated plant. However, NRC does not require periodic upgrades for currently operating reactors. For new reactors licensed under 10 CFR 52, each holder of a combined licence is required to maintain and upgrade the PRA. The upgraded PRA must cover initiating events and modes of operation contained in NRC-endorsed consensus standards on PRA in effect 1 year prior to each required upgrade. The PRA 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.

5. PRA METHODOLOGY AND DATA

PRA standards and guidance

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

Figure [5.1 US] 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 PRA. There are, of course, numerous sources of guidance on other PRA-related aspects, e.g. methods to perform specific PRA analyses. Some of these latter guidance documents are discussed in Section 5.US of this report.)

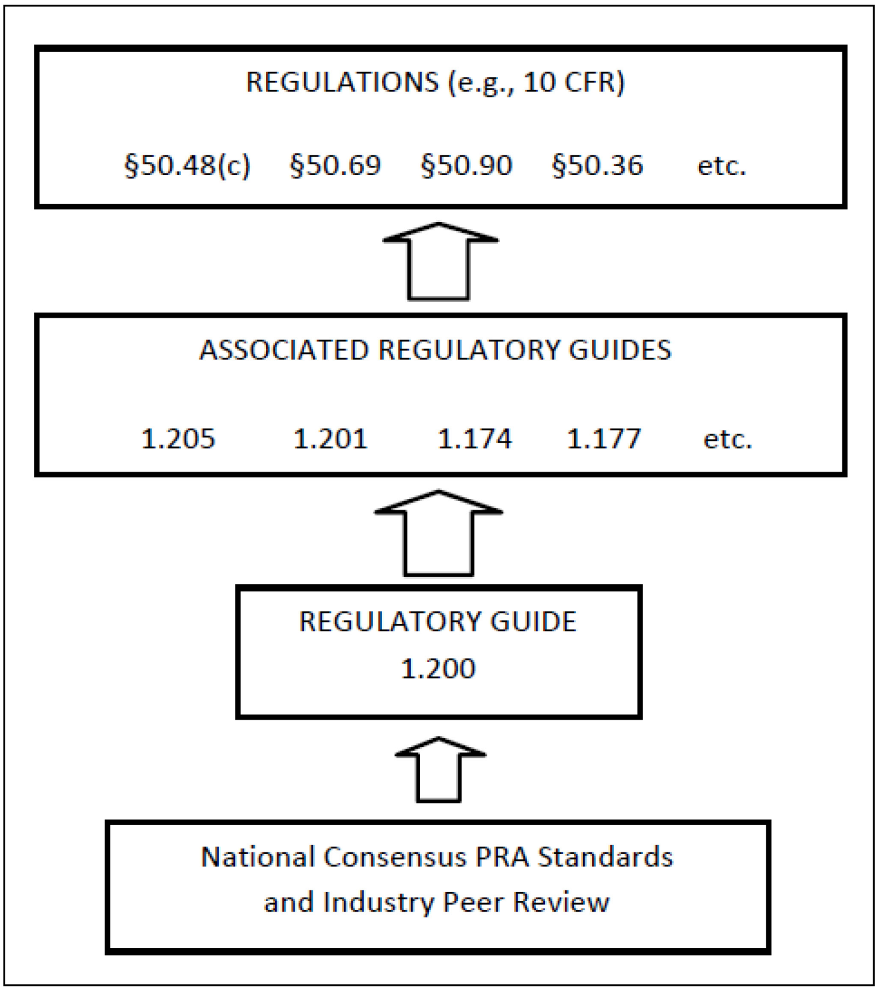

REGULATIONS (e.g., 10 CFR)
§50.48(c) §50.69 §50.90 §50.36 etc.
ASSOCIATED REGULATORY GUIDES
1.205 1.201 1.174 1.177 etc.
REGULATORY GUIDE
1.200
National Consensus PRA Standards
and Industry Peer Review

Figure 5.1.US. relationship of regulations, RGs, and standards for risk-informed activities (source: NUREG-1925, Rev. 1, Figure 5.4)

The top two levels of Figure [5.1 US] 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 PRA.[18] As summarised in NUREG-1925, RG 1.200 provides guidance on the technical acceptability of PRA by:

1. Establishing the attributes and characteristics of a technically acceptable PRA.
2. Endorsing consensus PRA standards and the industry peer review process.
3. Demonstrating technical acceptability in support of a regulatory application.

4. Documentation to support a regulatory submittal

Regarding the attributes and characteristics of a technically acceptable PRA, RG 1.200:

- Defines the scope of a base PRA 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 PRA.
- Provides guidance to ensure that a PRA 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 PRA to ensure that the model represents the as-built, as-operated (or as-designed) plant.

Regarding consensus PRA standards and the industry peer review process, RG 1.200:

- Allows the use of consensus PRA standards and peer reviews (as endorsed by the NRC in RG 1.200) to demonstrate the technical acceptability of a base PRA.
- Provides guidance for an acceptable peer review process and peer reviewer qualifications.
- Endorses the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) PRA 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 PRA needs to address the staff objections in RG 1.200, where applicable, if the PRA standard is to be considered met.

Regarding regulatory applications, RG 1.200:

[18] An NRC Regulatory Guide provides one way that the NRC staff finds acceptable to meet a regulatory requirement. The staff recognises that there may be alternate, equally acceptable ways.

- Recognises that the needed PRA scope (i.e. risk characterisation, plant operating states, initiating events and hazards) 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 PRA, whereas other applications (e.g. safety significance categorisation of structures, systems, and components) may require the complete model.
- Demonstrates one approach for technical acceptability of a PRA, independent of application. Inherent in this definition is the concept that a PRA need only have the scope, technical elements, level of detail, and plant representation necessary to support the application for which it is being used, but it always needs to be technically acceptable.
- The staff position in Revision 3 is being expanded to address the use of an industry process for closure of peer review Facts and Observations, industry guidance for the acceptability of new PRA methods.

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 PRA 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, RG1.200 is meant to provide for a more focused and consistent review process. Regarding consensus standards and industry peer review (the fourth level in Figure [5.1 US]:

- 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 PRAs for operating LWRs. The scope of the standard includes a Level 1 (plus LERF) PRA for at-power conditions addressing both internal hazards (including internal events, internal floods and internal fires) and external hazards (seismic events, external floods, high winds, etc.). A new edition is expected to be published in 2019 that will address issues with internal hazards, internal flood, internal fires, and seismic events. Work is ongoing to extend ASME/ANS RA-Sa-2009 to low-power shutdown conditions and to support new LWRs. In addition, PRA standards for Levels 2 and 3 are under development. Draft standards for trial use have been issued by ASME/ANS for Level 2, Level 3, LPSD, and non-light water reactors.
- 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 programme. The standard does not establish requirements for a fire PRA - 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";; and NEI-07-12, Fire Probabilistic Risk Assessment (FPRA) Peer Review Process Guidelines," which include a peer review process for Level 1 LERF PRA for internal hazards and internal floods, PRA updates and upgrades, and fire PRA, respectively. NEI revised NEI-07-12 in June, 2010 and published NEI-12-13, "External Hazards PRA Peer Review Process Guidelines," in August 2012. NEI is revising NEI-05-04, "Process for

Performing Follow-on PRA Peer Reviews Using the ASME PRA Standard" to address closure facts and observations made by the peer review. NEI is also developing NEI-16-04, "New PRA Methods Acceptance Process Guidance".

A draft Revision 3 to RG 1.200 is expected to be published in 2018 to provide draft staff positions on the trial use standards for PRAs on Level 2, low power and shutdown, and advanced LWRs; and the revised NEI-05-04, NEI-07-12, NEI-12-13, and the new NEI-16-04. Insights from the trial use of these standards and pilots of the NEI guidance documents will be incorporated into Revision 3 of RG 1.200.

PRA methodology

Licensee and NRC PRA models for nuclear power plants in the United States. use the classical PRA framework first established by WASH-1400. This involves an event tree/fault tree analysis for Level 1 PRA, a containment (or accident progression) event tree analysis for Level 2 PRA, and, for those plants having a Level 3 analysis, a simulation-based accident consequence analysis for Level 3 PRA.

All US plants have Level 1 and Level 2 PRA models for internal hazards (including internal flooding events) occurring during full-power operation. As discussed in section 4.US, many of these models were created in response to GL 88-20. Also as discussed in Section4.US, the NRC has developed Level 1 PRA models for all plants under the Standardized Plant Analysis Risk (SPAR) programme and has benchmarked these models against licensee PRAs. All operating plants also have external hazard 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 PRAs for new reactor design certification applications typically have an SMA, while new combined licence holders are required to have a full seismic PRA at the time of initial fuel load. A small number of operating 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 hazards, internal fires, and accident progression (containment performance) analyses than for Level 1 internal hazards PRA. As discussed in section .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 PRA analyses intended to support risk-informed decision making. As discussed in section 8.US, a number of activities are also underway to improve current methods, tools, and data.

Current approaches used for a number of PRA topics of interest can be summarised as follows.

Common cause failure: PRA 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 modelled in the PRA. In current US PRAs, 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, modelling 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 US PRAs 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 multidisciplinary effort involving extensive interactions between the HRA analysts and other domain experts (e.g. PRA 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 PRA 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 characterisation and assessment method, the technique for human error prediction (THERP) method and the related accident sequence evaluation programme (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 pressurised 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). Also, two studies, one international and one US, comparing simulator data to HRA results have been completed: 1) NUREG/IA-0216, *International HRA Empirical Study*, and 2) *NUREG-2156, The U.S. HRA Empirical Study - Assessment of HRA Method Predictions Against Operating Crew Performance on a U.S. Nuclear Power Plant Simulator*. As described in Section 8.US, efforts are underway to collect and analyse empirical data (both operational and experimental) needed to improve confidence in the modelling and quantification of HFEs, and to address the issue of HRA diversity as related to NRC applications.

Fire PRA: Current guidance for performing fire PRA 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 learnt from the IPEEE programme and subsequent fire-related research, recommend a general fire PRA framework and approach consistent with those used in past US fire PRAs. Perhaps more importantly, they also provide improved guidance on the treatment of specific, difficult fire PRA 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 PRAs using these reports.

Seismic PRA: The NRC's Office of Research in conjunction with Idaho National Lab have been involved in the development of the seismic framework for Standardized Plant Analysis Risk (SPAR) PRA models, which use five hazard bins. These models are quantified using the "Systems Analysis Programs for the Hands-on Integrated Reliability Evaluations" (SAPHIRE) computer code. The "SPAR 5 Bins Methodology" adopts standard modelling techniques, uses readily available data, is informed by current PRA standards and requirements, and is intended for use in reactor oversight activities. A number of these models have been developed, and additional SPAR models may be upgraded to include seismic event trees in future.

PRA Data: Most US PRAs use generic and plant-specific data to estimate initiating event frequencies, equipment failure probabilities, and equipment unavailabilities due to testing and maintenance. Some PRAs (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),[19] licensees' monthly operating reports (MORs), and the Institute of Nuclear Power Operations (INPO) Consolidated Event Database (ICES), formerly known as 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 5.2.US, 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.

[19] LERs can be individually searched using the LERSearch program, accessible through the NRC's public website: https://nrcoe.inel.gov/secure/lersearch/index.cfm. Current operating experience information can be found on NRC's Reactor Operating Experience Results and Databases website (http://nrcoe.inel.gov/results/).

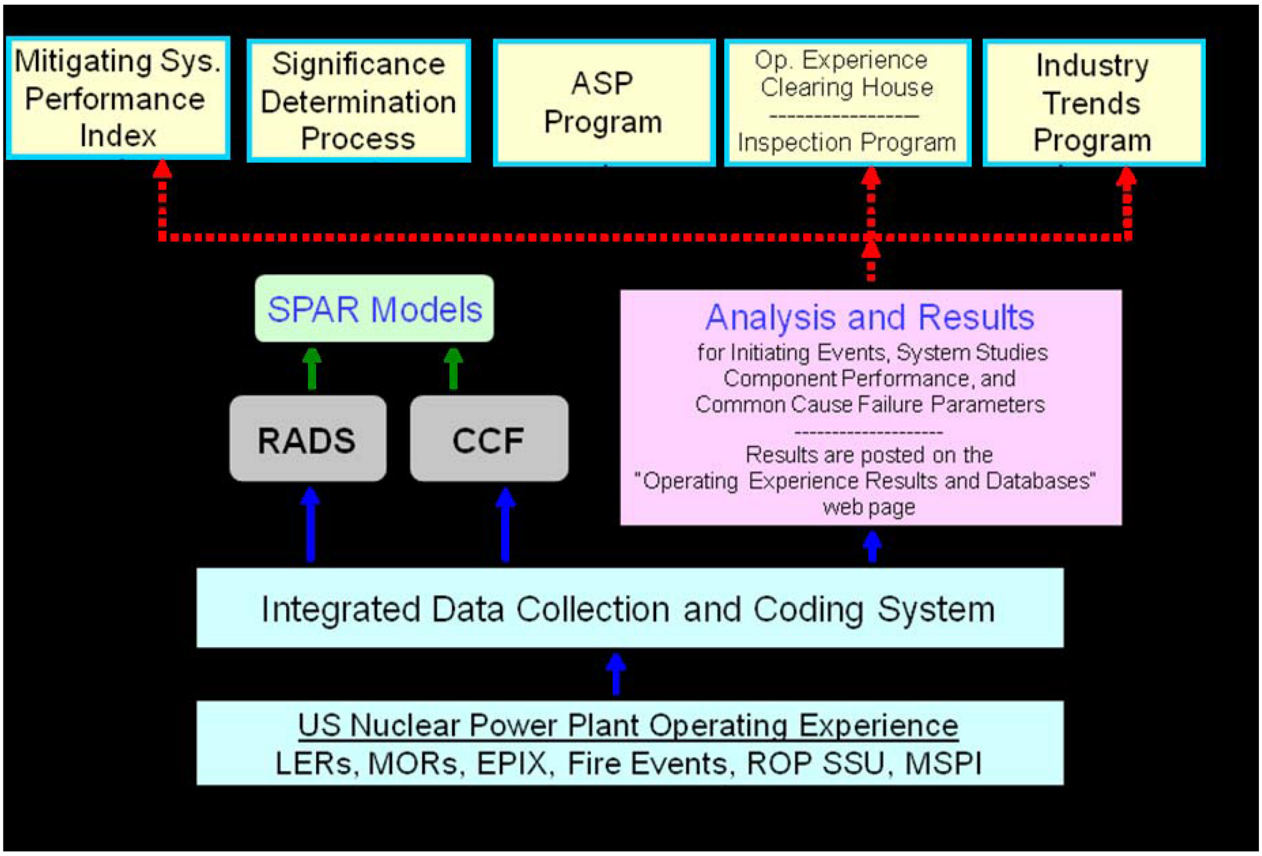

Mitigating Sys. Performance Index
Significance Determination Process
ASP Program
Op. Experience Clearing House
Inspection Program
Industry Trends Program
SPAR Models
RADS
CCF
Analysis and Results
for Initiating Events, System Studies Component Performance, and Common Cause Failure Parameters
Results are posted on the "Operating Experience Results and Databases" web page
Integrated Data Collection and Coding System
US Nuclear Power Plant Operating Experience
LERs, MORs, EPIX, Fire Events, ROP SSU, MSPI

Figure 5.2.US. Sources and uses of operating data and analyses in NRC regulatory programme[20]

Characterisation of Results: Most current PRAs use a combination of methods to characterise 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.

PRA 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.

[20] Figure 5.2.US makes reference to the Equipment Performance and Information Exchange System (EPIX), the equivalent system is now called the Consolidated Event Database (ICES).

The NRC staff initiated the Risk Assessment Standardization Project (RASP) to establish standard procedures, improve the methods, and enhance risk models that are used in risk assessment in various risk-informed regulatory applications. The major RASP activities include:

- developing standard procedures and methods for the analysis of internal hazards, internal fire and flooding hazards, external hazards, and shutdown events;
- providing enhanced-quality, integrated SPAR models for internal and external hazards, 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.

6. NOTABLE RESULTS OF PRAs

As is widely recognised and confirmed by the PRAs discussed in Section 4.US, the results and insights of PRAs 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 modelling approaches (e.g. assumptions regarding the allowable credit for alternative mitigation systems) can have an observable effect on PRA 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 hazards, internal fires) potentially important to risk, their general importance to risk for different classes of plants (e.g. boiling water reactors vs. pressurised water reactors), and the reasons for their importance, are reasonably well understood.
- 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 hazards are important CDF contributors for many plants. The CDF contribution from seismic or fire hazards can, in some cases, approach (or even exceed) that from internal hazards. As discussed in NUREG-1742, the important seismically-induced failures reported by the IPEEEs include failures of offsite power, electrical system components (e.g. motor control centre, 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 PRAs have been considered sufficiently robust to support changes to plant design and operations. Some specific examples of PRA-spurred improvements reported by Gaertner et al include the replacement of pressurised 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 (Dube, 2008) 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, US 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 condtioning (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.

It should be noted that Dube based his conclusions on insights derived from NRC design certification reviews rather than actual operating experience. With the exception of the ABWR design, there is currently no operating experience available for the new LWR designs considered by Dube. As these new designs enter operational status, it is anticipated that the confidence in new LWR designs will increase over time, particularly for features unique to these designs (e.g. passive safety systems).

Finally, it should be emphasised that comparisons of PRA results should be made with great caution. As mentioned previously, the PRA results are dependent on design- and operations-specific details, and on modelling approaches and assumptions. (Variations in modelling can be due to a number of reasons, including differences in the purpose of the PRA, associated differences in the PRA scope and level of detail, and differences in the level of maturity of the state of the art for analysing 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 significant contributors to risk and the reasons for their significance (including modelling approaches and key assumptions as well as physical factors) will enable the reader to better compare and contrast study results.

7. PRA APPLICATIONS AND DECISION MAKING

This section provides examples of PRA applications. In addition to the specific examples given below, PRAs 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 programmes and processes on a risk-informed sampling basis to obtain representative information. PRA results are used in many ways to support the oversight programme, 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. PRA methods are used to determine the risk significance of inspection findings using the Significance Determination Process (SDP). This process has evolved to rely on the NRC's SPAR models with the ability of the licensee to provide insights from their 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 PRAs for the CDF estimates (internal hazards at power only) to be used in the calculation of the index.

Additional information can be found at: www.nrc.gov/reactors/operating/oversight.html.

Maintenance Rule – 10 CFR 50.65, "Requirements for monitoring the effectiveness of maintenance at nuclear power plants": The Maintenance Rule paragraph (a)(4) 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 PRA 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 PRA 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 PRA 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 US 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 utilise 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 hazards 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 programme. The NRC is required to report significant precursors to Congress if core damage frequency (CDF) is greater than or equal to 1E-3 per year. The ASP programme provides the Commission with annual assessments of the significance of events/conditions occurring at commercial power plants and the trends in industry performance.

The latest ASP Report (SECY15-0124) can be obtained from NRC's website:

www.nrc.gov/docs/ML1518/ML15187A434.html

Using PRA results and perspectives to identify possible changes to NRC's reactor safety requirements

Search for Vulnerabilities: The Individual Plant Evaluation (IPE) programme and the Individual Plant Evaluation for External Events (IPEEE) programme 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 programme. These voluntary licensee improvements have led to enhanced plant capability to respond to external hazards (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 PRA guidance and standards, while plant-specific risk information is supporting the risk-informed reactor oversight programme. NRC issued "requests for information" pursuant to 10 CFR 50.54(f) to all licensees, which requested that licensees re-evaluate seismic and flooding hazards using present day information and guidance. This was to implement the NTTF recommendation 2.1. In 2015, the NRC staff has completed the review of the updated plant-specific seismic hazard. Licensees generated a "ground motion response spectrum" (GMRS) using the new hazard and current methods. The GMRS was compared to the original plant seismic design spectrum safe shutdown earthquake (SSE). No action was required if the SSE bounded the GMRS, but a seismic risk evaluation was required depending upon how much the GMRS exceeded the SSE. As a result of hazard re-evaluation, it is anticipated that 21 licensees will perform a seismic PRA and provide the risk insights to the NRC for further review. For the flooding portion of NTTF recommendation 2.1, the NRC staff proposed that flooding hazard reevaluations be integrated with Mitigation Strategies for Beyond Design-Basis External Events. The majority of sites that have submitted re-evaluated flood hazard reports have indicated that they will perform integrated flooding assessments. However, these will likely not be flooding risk assessments.

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 (SAMDAs), and the bases for not incorporating SAMDAs 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 categorisation (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 22 November 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." A pilot application was completed in December 2014.

In general, 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 categorisation 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, augmented by a series of qualitative "questions" used to identify the safety significant of the SSC on accidents and mitigating capabilities not modelled in the PRA.

Combustible gas control (10 CFR 50.44): As part of the NRC staff's programme 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 programme. 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 pressurised 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 programme 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.

The proposed rule that would have allowed licensees to adopt a risk-informed LOCA break size has not been issued and work on this effort has been discontinued. This is because licensees have indicated that the rule as proposed would not provide them the benefits that were originally expected and because the NRC is focused on higher priority work.

Pressurised thermal shock rule (10 CFR 50.61): In 1986, the NRC established the pressurised thermal shock (PTS) rule (10 CFR 50.61) in response to an issue concerning the integrity of embrittled reactor pressure vessels in pressurised 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 re-evaluate 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 PRA methodology and the application of this methodology to the Oconee, Beaver Valley, and Palisades plants. The PTS PRAs 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 behaviour 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 summarises 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 programme to re-evaluate and update the technical basis of the risk of through-wall 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 25 June 2007. On 11 September 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 3 October 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 11 August 2008 (73 FR 46557). The comment period for the supplemental proposed rule closed on 10 September 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 22 September 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, 4 January 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 PRA 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 programme element.

The revised rule provides a means to establish well-defined fire protection licensing bases and enables licensees to manage their fire protection programmes 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, 19 plants sites (29 nuclear units) have transitioned their fire protection programmes to meet the requirements of 50.48(c) (NFPA 805), 9 plants sites (15 nuclear units) have submitted licence amendment requests to make this transition, and 1 plant site (2 nuclear units) has indicated its intent to make this transition and submit a future licence amendment request. Supporting guidance for performing fire PRA in this application is provided in NUREG/CR-6850 (EPRI 1011989) and in Supplement 1 to that document, as discussed in Section 5.US.

Risk-informed technical specifications (RITS): Consistent with the Commission's policy statements on technical specifications and the use of PRA, 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 programme (CRMP); 5) replace fixed surveillance frequencies with a licensee-controlled programme to permit optimisation 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) programme 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 authorisation of alternative ISI programmes by the Director of NRR. The staff and industry recognised 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 programmes have referenced one of the two approved Topical Reports.

The use of an alternative is only authorised 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 authorisation for all alternatives proposed for the next interval. Licensees briefly discuss updates to their RI-ISI programme 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 programmes. The BER inspection programmes are normally part of the licensing basis as described in the Final Safety Analysis Report (FSAR). When the BER programme is in the FSAR, the application of RI-ISI to the BER programme may be done via the 10 CFR 50.59 process.

The NRC has also approved RI-ISI programmes 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 PRA 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 technical adequacy of the flooding PRA that the staff finds acceptable to use in RI-ISI programmes. NRC has endorsed Code-Case-N716 in RG 1.147, with limitations and conditions (e.g. that the technical adequacy of the PRA is acceptable as measured against the EPRI Topical report). As licensees perform their ten year interval inspections, some are using the endorsed code case, other are submitting relief requests.

<u>Risk-informed in-service testing (RI-IST)</u>: 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 programme. 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 flexible 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 programme.

<u>Risk-informed containment integrated leak rate test (ILRT) interval</u>: 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.

Risk-informed Seismic PRA: NRC requested that plants provide information on the updated seismic hazard as part of the resolution of Fukushima NTTF Recommendation 2.1. In 2015, the NRC staff completed the review of the re-evaluated seismic hazard for 60 reactor sites. As a result of this assessment, 21 plants are anticipated to submit their plant-specific seismic PRA for further review during 2017-2019. The objective of reviews are to ensure that the plants' systems and key components, particularly cooling systems, could ensure a safe shutdown if an earthquake were to occur at a higher seismic ground motion than allowed for in their original design.

Risk-informed GSI-191: This generic issue concerns the debris blockage on the containment sump strainer following a LOCA. As part of the lengthy resolution process, the risk-informed approach has been proposed and is being piloted by South Texas Project (STP). The NRC staff has continued to review the STP pilot and has published draft guidance (DG-1322) for licensees choosing to implement the optional, risk-informed provision in 10 CFR 50.46c. Tentatively, 14 reactor units will be performing additional testing to implement a risk-informed evaluation for closing GSI-191.

8. 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 co-ordinate 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, 2015 version of the RPP is available in SECY-15-0135. The RPP database as well as general information on the NRC's use of risk in regulation can be obtained from NRC's website:

www.nrc.gov/about-nrc/regulatory/risk-informed.html

Regarding future industry work relevant to the use and development of PRA, 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 (www.epri.com/Our-Portfolio/Pages/Portfolio.aspx?program=061177) these activities include:

- A comprehensive research review examining how severe accidents in nuclear power plants evolve. In conjunction with detailed analyses using the MAAP code, this research provides insights into measures (including filtered containment vents) that might be effective in managing severe accidents, reducing the potential for serious releases. This report, and the supporting research, also informs regulatory decisions, forms the basis for analysing accident risks to the new generation of reactors, and will help ensure the safety of currently operating nuclear plants over their lifetimes.

- Enhancement to the MAAP5 code for performing severe accident analysis, addressing insights from the Fukushima accident and other recent developments. Performed detailed technical analysis of the Fukushima accident to gain insight into the course of events.
- Continued training to the next generation of risk professionals.
- Methods for assessing the hazards associated with external flooding
- Development of new fire ignition frequencies with a substantially improved technical basis to support more realistic risk assessment for internal fires. Improved methods for developing fire probabilistic risk assessments in support of risk-informed regulation, including transition to National Fire Protection Association (NFPA) Standard 805.
- Enhancement of software used in risk management to support valuable risk-informed application.
- Development of the first modules for the Phoenix software, an advanced risk code that would enable analysis of all modes and hazards and an integrated risk profile of the entire plant.
- Guidance for conducting human reliability analysis in support of fire PRA, and developed analogous guidance for use in seismic PRAs.
- Guidance that can be used to perform seismic evaluations and perform seismic walkdowns in response to regulatory or other actions following the Fukushima accident.
- Update to the guidance for addressing post-earthquake restart of nuclear power plants.
- Framework for conducting PRAs for spent fuel pools in BWRs and PWRs, and applied the framework at pilot plants

Current specific activities include:

- Continued development of the next generation of risk professionals through its Education of Risk Professionals course;
- Significant improvements to the methods for performing elements of seismic PRAs, with an emphasis on fragility assessment;
- Development of new consensus methods for evaluating external flooding and initiating development of such methods for other hazards (such as high winds).
- Further enhancement to methods for assessing the risk of fires, including better methods and guidance for modelling fire growth and propagation and for assessing the risks associated with fires that necessitate evacuation of the control room; and
- Continued detailed evaluations of the Fukushima accident to capture insights and to improve modelling capabilities.

The remainder of this section addresses some noteworthy examples of ongoing developmental activities.

PRA Models

As discussed in Section 5.US, the NRC and industry are continuing to make a significant effort to develop PRA 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 revision 2 of RG 1.200 in March, 2009 completed the final phase of the plan.. With this work completed, it is expected that the industry will have full-scope (i.e. internal and external hazard) PRAs 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 PRA models.

In addition to PRA-technical adequacy 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.

PRA Data

The NRC's routine data collection and analysis activities are described in Section 4.US of this report. On the developmental side, the NRC's Office of Nuclear Regulatory Research (RES) is continuing its work on the human performance data collection method and tool (i.e. Scenario Authoring, Categorization, and Debriefing Application [SACADA]) with emphasis on collecting the licensed operator simulator training data to inform the human error probability (HEP) estimations in human reliability analysis (HRA)/probabilistic risk assessment (PRA). A US nuclear power station has used the SACADA tool in its operator simulator training since 2012. The collected data are accessible to NRC under a bilateral agreement. The SACADA tool is also used by the Halden Reactor Project (HRP) to collect the data of operator simulator experiments.

Modelling of Physical Processes to Support PRA

To improve the realism of PRA models, RES, industry, and the US Department of Energy (DOE) are working on a number of efforts involving the use of phenomenological models in PRA. 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 working on a study of thermal hydraulics PRA success criteria. Recently completed activities include: analysis for the Byron station including small- and medium break loss-of-coolant accidents, loss of a direct current bus, steam generator tube rupture, and loss of decay heat removal during shutdown operations documented in NUREG-2187, "Confirmatory Thermal-Hydraulic Analysis to Support Specific Success Criteria in the Standardized Plant Analysis Risk Models—Byron Unit 1," issued in 2016; and the analysis for the Vogtle station (Units 1 and 2), for a mix of issues of importance to the Vogtle Level 3 PRA project (SECY-11-0089), - documented in project documents to be issued at the completion of the Level 3 PRA project

In the area of fire PRA, RES is continuing to work with EPRI and NIST to develop technical guidance to support fire modelling for nuclear power plant scenarios. Research is working with EPRI as the methodology presented in NUREG/CR-6850 continues to mature and other fire research programmes advance the state-of-the-art knowledge.

In the area of seismic PRA, RES is continuing research for sites located in the CEUS with the Next Generation Attenuation (NGA) East project. The goal of this co-operative agreement between the NRC, US Department of Energy (DOE), Electric Power Research Institute, and the US Geological Survey is to produce the most up-to-date ground motion prediction equations (GMPEs) to be used in probabilistic seismic hazard analyses (PSHA). Research is also being conducted to develop updated software tools for calculating site-specific PSHA results and for refinement of the guidance for performing structured hazard studies following the Senior Seismic Hazard Analysis Committee (SSHAC) guidelines

Regarding other external hazards, RES is working a multi-year, multi-project research programme on probabilistic flood hazard assessment (PFHA). The main focus areas of the PFHA research programme are: 1) leverage available frequency information on flooding hazards at operating nuclear facilities and develop guidance on its use; 2) develop and demonstrate PFHA framework for flood hazard curve estimation, ;3) assess and evaluate application of improved mechanistic and probabilistic modelling techniques for key flood-generating processes and flooding scenarios; 4) assess and evaluate methods for quantifying reliability of flood protection and plant response to flooding hazards; and 5) assess potential impacts of dynamic and nonstationary processes on flood hazard assessments and flood protection at nuclear facilities.

PRA Methods

Human Reliability Analysis (HRA)

Recognising 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 an 8 November 2006, memorandum from the Commission (SRM-M061020), is pursuing a formalisation approach and a quantification tool capable of performing HRA in a consistent and efficient manner. The formalisation approach incorporates behavioural science knowledge by providing decompositions of human failures, failure mechanisms, and failure factors that reflect both PRA-relevant contextual information and findings from scientific papers documenting theories, models, and data of interest. For quantification, the project uses a conventional PRA 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). Thus far, one report has been published that providing a survey of psychological literature useful to HRA analysts: NUREG-2114, Cognitive Basis for Human Reliability Analysis (January 2016).

Fire PRA

As discussed in Section 7.US, a number of plants are risk-informing their fire protection programmes, supported by fire PRA guidance provided in NUREG/CR-6850 (EPRI 1011989) and Supplement 1 to that document. Observing the application of this guidance in developing fire PRAs 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 hazard data characterisation, fire severity characterisation, detection and suppression, fire growth and damage modelling, fire-induced circuit failures, HRA, and PRA plant modelling).

RES and EPRI have worked jointly to update and improve fire modelling tools, methods and data to enhance realism supporting NUREG/CR-6850/EPRI 1011989. The guidance provided in NUREG/CR-6850 continues to mature and other NUREG Publications and fire research programmes advance the state-of-the-art fire PRA knowledge. Since the publication of NUREG/CR–6850 and NUREG/CR–6850 supplement 1 there have been multiple publications which affect the methodology and guidance presented in NUREG/CR 6850 such as;

- NUREG/CR-7114- A Framework for Low Power/Shutdown Fire PRA.
- NUREG/CR-7010 Cable Heat Release, Ignition, and Spread in Tray Installations During Fire (CHRISTIFIRE) Volumes 1 & 2
- NUREG-1921 EPRI 1023001- EPRI/NRC-RES Fire Human Reliability Analysis Guidelines
- NUREG-1934, EPRI 1023259- Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG)
- NUREG/CR-7150 Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE)
- NUREG-1824- Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications Supplement 1
- NUREG-2178, Volume 1, EPRI 3002005578- Refining and Characterizing Heat Release Rates From Electrical Enclosures During Fire (RACHELLE FIRE)
- NUREG/CR-7197- Heat Release Rates of Electrical Enclosure Fires (HELEN-FIRE)
- NUREG-2169, EPRI 3002002936- Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database: United States Fire Event Experience Through 2009
- NUREG-2180- Determining the Effectiveness, Limitations, and Operator Response for Very Early Warning Fire Detection Systems in Nuclear Facilities (DELORES-VEWFIRE)-(NUREG-2180)
- NUREG/CR-7114- A Framework for Low Power/Shutdown Fire PRA.

In addition to these updates to the PRA methodology the NRC’s Office of Nuclear Regulatory Research is currently investigating several other topics to improve the realism in PRA models including; cable coating response bias, instrumentation circuit response, high energy arc fault (HEAF) zones of influence and secondary fires associated with current transformers.

Digital Instrumentation and Control Systems

It is well-recognised that US licensees are currently replacing their original analogue 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 PRAs. 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.

The US NRC has developed a comprehensive 5year Digital System Research Program Plan that defined the I&C research to support the regulatory needs of the agency. The updated research plan consists of the following research programme areas: 1) safety aspects of digital systems; 2) security aspects of digital systems; 3) knowledge management; and 4) projects supporting licence office user needs. The products of these research programmes include technical review guidance, information to support regulatory-based acceptance criteria, assessment tools and methods, standardisation, and knowledge management initiatives.

Recent activities include:

- Participation in the development of a failure mode taxonomy for a digital instrument and control (I&C) system performed by the OECD/NEA Working Group on Risk Assessment (WGRISK) (NEA/CSNI/R(2014)16
- Quantification of software reliability using BBN-based on software development cycle quality attributes, in collaboration with the Korea Atomic Energy Research Institute
- Estimation of the reliability, including software, of an example digital system using PRA-based statistical testing.

Advanced PRA Methods

As discussed above, RES investigated the feasibility of a dynamic event tree approach for Level 2 PRA. This approach is intended to: reduce reliance on unnecessary modelling 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 characterisations. 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. The results of this project are documented in Sandia Report SAND2012-9346, "Discrete Dynamic Probabilistic Risk Assessment Model Development and Application."

Treatment of Uncertainty

As part of its phased approach to PRA technical adequacy, the NRC has developed guidance for the treatment of uncertainties and the use of alternate methods in the risk-informed decision making. The guidance addresses 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

PRA techniques (e.g. regarding the propagation of uncertainties) and supplemental techniques (e.g. sensitivity studies, qualitative analyses, bounding analyses, screening methods) are 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 hazards and internal floods in at-power operating reactor including calculations of CDF and LERF. Revision 1 to NUREG-1855 better structures the guidance to licensees and further clarifies the NRC staff decision-making process in addressing uncertainties. Revision 1 also expand coverage to include internal fires, seismic, LPSD and Level 2. In parallel with NRC efforts, the Electric Power Research Institute (EPRI) developed guidance on the treatment of uncertainties (EPRI 1016737, "Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments;" and EPRI 1026511, "Practical Guidance on the Use of PRA in Risk-Informed Applications with a Focus on the Treatment of Uncertainty"). The NRC and the EPRI guidance have been developed to complement each other and are intended to be used as such when assessing the treatment of uncertainties in PRAs used in risk-informed decision-making. In support of the NRC NUREG and associated EPRI reports, training is being developed. A web-based training course (schedule for completion by the end of 2016) involves a short course focused on educating both staff and management on concepts in NUREG-1855 and associated EPRI reports. A more detailed training course (e.g. 2 days) is underway on how to implement guidance involving the use of various diverse examples (tentatively scheduled for late spring 2017).

Comprehensive Site Level 3 PRA

Although Level 3 PRAs 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 PRAs have not been conducted since the late 1980s. These Level 3 PRAs 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 PRA 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 PRA policy statements, support of risk-informed rulemaking, prioritisation 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 PRAs—both less expensive than Level 3 PRAs—and how they relate to lower level subsidiary safety goals based on CDF and LERF to risk-inform regulatory decision making.

There are several compelling reasons for conducting a new comprehensive site Level 3 PRA. 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 PRA methods, models, tools, and data— collectively referred to as "PRA 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 analyses two of the essential technical elements of a Level 3 PRA for some of the more likely reactor accident sequences–the severe accident progression and offsite consequence analyses. A new level 3 PRA could therefore seek to leverage the methods, models, and tools used in the SOARCA analysis and capitalise on the insights gained from the application of state-of-the-art practices.

In addition to these developments, the Level 3 PRAs documented in NUREG 1150 are incomplete in scope. Figure 6.2.US illustrates the scope of a complete site accident risk analysis, with the approximate scope of the NUREG 1150 PRAs shown by the grey-shaded region. These PRAs were limited to the assessment of single-unit reactor accidents initiated primarily by internal hazards occurring during full-power operations. The partial coverage of external hazards indicates that a limited set of external hazards (fires and earthquakes) were considered for only two of the five analysed nuclear power plants.

To update and improve its understanding of reactor accident risks, the NRC is evaluating accidents that might occur during any plant operating state, that are initiated by all possible internal hazards and external hazards, and that may simultaneously affect multiple units per site. Moreover, for a comprehensive site accident risk analysis, the NRC is also considering analysing 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 is currently performing a Level 3 PRA study. The objectives of this study are:

- Develop a Level 3 PRA, generally based on current state-of-practice, methods, tools, and data that 1) reflects technical advances since completion of the NUREG-1150 studies; and 2) addresses scope considerations that were not previously considered.
- Extract new risk insights to enhance regulatory decision-making and to help focus limited agency resources on issues most directly related to the agency's mission to protect public health and safety.
- Enhance PRA staff capability and expertise and improve documentation practices to make PRA information more accessible, retrievable, and understandable.
- Obtain insight into the technical feasibility and cost of developing new Level 3 PRAs.

  The current status of this project include:

- The staff completed an initial reactor, at-power, PRA models for internal hazards and internal floods (Level 1 and Level 2), high winds (Level 1), and other hazards". These models have been subjected to a PWR Owners Group (PWROG)-led peer review based on the ASME/ANS PRA standards.

- Initial reactor, at-power, PRA models for internal hazards and internal floods (Level 3); internal fires (Level1); and seismic hazards (Level 1) are underway.
- In addition, an initial reactor, low power and shutdown PRA model for internal hazards and floods (Level 1) as well as a combined Level 1 and Level 2 PRA for dry cask storage are expected to be completed in 2016.

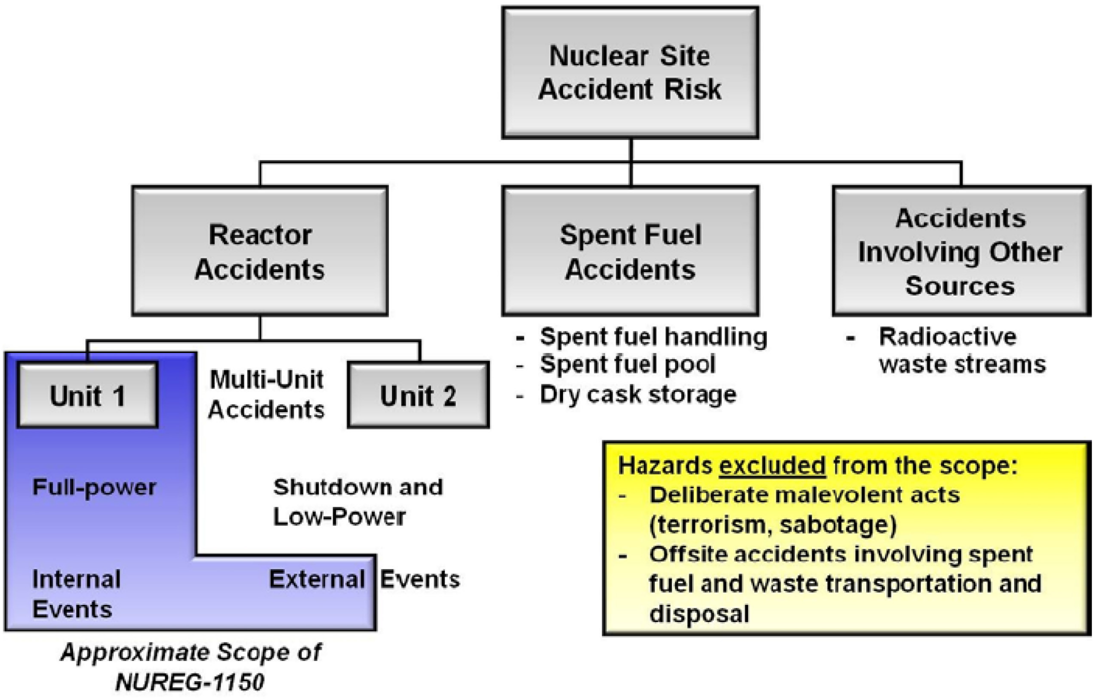

Nuclear Site Accident Risk
Reactor Accidents
Spent Fuel Accidents
Accidents Involving Other Sources
- Spent fuel handling
- Spent fuel pool
- Dry cask storage
- Radioactive waste streams
Unit 1
Multi-Unit Accidents
Unit 2
Full-power
Shutdown and Low-Power
Internal Events
External Events
Approximate Scope of NUREG-1150
Hazards excluded from the scope:
- Deliberate malevolent acts (terrorism, sabotage)
- Offsite accidents involving spent fuel and waste transportation and disposal

Figure 6.2. US. Site Accident Risk and Approximate Scope of NUREG-1150 (source: NUREG-1925, Rev. 1, Figure 5.3).

Beyond-Design-Basis Accident Mitigation

The US nuclear power industry has made various changes to plants including but not limited to procurement and installation of additional components and development of additional procedures to address the Commission orders that were put in place after the events at the Fukushima Daiichi nuclear power plant. While this equipment was procured specifically to mitigate the effects of a beyond-design-basis external hazard, the equipment can be used for other functions and could help to mitigate some design-basis events as well. The results from Probabilistic Risk Assessments developed for nuclear power plants are expected to reflect the as-built, as-operated plant to the extent possible. As such, where the mitigating strategies developed to comply with the orders noted above can, or will be used by licensees to affect the outcome of the scenarios modelled in the PRA, these strategies should be taken into account. Relying on PRA results that reflect the modelling of mitigating strategies will improve the accuracy of those results, which in turn will enhance the NRC's safety focus.

The NRC has undertaken a project to ensure that it deals with the challenges in crediting mitigating strategies in future risk-informed decision making in a predictable, reliable, and efficient manner. To that end, NRC has held public meetings and workshops with interested stakeholders to solicit feedback on crediting mitigating strategies. The NRC staff intends to develop or revise application-specific guidance for areas where risk information is used in the regulatory processes using the information that was presented during those meetings.

9. INTERNATIONAL ACTIVITIES

RES has implemented over 100 bilateral or multilateral agreements with more than 30 countries and the Organisation for Economic Co-operation and Development (OECD). These agreements cover a wide range of activities and technical disciplines including severe accidents, thermal-hydraulic code assessment and application, digital instrumentation and control, nuclear fuels analysis, seismic safety, fire protection, human reliability, and more.

RES actively seeks international co-operation to obtain technical information on potential safety issues that require test facilities not available domestically that would require substantial resources to duplicate in the United States. RES often will propose modifications to a project sponsor so that the proposed project can better meet the NRC's needs. In addition, the NRC may propose to sponsor co-operative international participation in research projects it conducts. Bilateral exchanges with counterparts multiply the amount of information available to RES staff. As an example, RES has developed an extremely beneficial relationship with the Canadian Nuclear Safety Commission in the area of environmental modelling, groundwater monitoring, and more. Similarly, the NRC and the French Institute of Radiation Protection and Nuclear Safety (IRSN) co-operate in dozens of technical areas.

The NRC has been participating in the Organisation for Economic Co-operation and Development/Nuclear Energy Agency (OECD/NEA) Halden Reactor Project (HRP) since its inception in 1958. HRP, which is located in Halden, Norway, is managed by the Norwegian Institute for Energy Technology (IFE) and operates on a 3-year research cycle, with the current programme plan running from 2015–2017. The NRC benefits directly from HRP research, which maximises the use of NRC research funds by leveraging the resources of other HRP participants. In addition, participation in the HRP facilitates co-operation and technical information exchange with the participating countries.

The Norwegian IFE research facilities also include several labs for Man-Technology-Organization (MTO) research. Among those is the Halden Man Machine Laboratory (HAMMLAB). HAMMLAB uses a reconfigurable simulator control room that facilitates research into instrumentation and control (I&C), human factors, and human reliability analysis (HRA). HAMMLAB has extensive data collection capabilities and typically uses qualified nuclear power plant operators (who are familiar with the plants being simulated) as test subjects. Currently, ongoing HRP experiments are addressing a number of topics of interest to the NRC including control room staffing strategies, the role and effects of automation in advanced control room designs, and aids to improve control room teamwork. The NRC expects that this research will contribute to the technical basis for human factors guidance, especially for new reactor designs.

The NRC also participates with the Organisation for Economic Co-operation and Development (OECD) on the fire hazards database project. The main purpose of the project is to encourage multilateral co-operation in the collection and analysis of data relating to fire hazards. Currently the event database contains more than 400 events. The objectives of the NEA Fire Project are to:

- collect fire event experience (by international exchange) in an appropriate format in a quality-assured and consistent database;
- collect and analyse fire events over the long term so as to better understand such events and their causes, and to encourage their prevention;
- generate qualitative insights into the root causes of fire events in order to derive approaches or mechanisms for their prevention and to mitigate their consequences;
- establish a mechanism for efficient operation feedback on fire event experience including the development of policies of prevention, such as indicators for risk-informed and performance-based inspections; and
- record characteristics of fire events in order to facilitate fire risk analysis, including quantification of fire frequencies.

Based on the insights from this data collection effort the NRC initiated the OECD/NEA High Energy Arcing Fault Events (HEAF) Project. The HEAF Project was conducted by USNRC at a facility in the United States. The project's aim is to conduct experiments in order to explore the basic configurations, failure modes and effects of high energy arc faults (HEAF) events. The equipment to be tested and considered primarily consists of switchgears and bussing components. Since the switchgears and other equipment necessary for testing is very expensive, the programme relies on signatories' in-kind contributions.

The NRC also co-ordinates the Cooperative Severe Accident Research Program (CSARP) that includes more than 20 member nations that focus on the analysis of severe accidents using the MELCOR and MACCS codes. CSARP includes MELCOR and MACCS user group meetings where participants share experience with the NRC codes, identify code errors, perform code assessments, and identify areas for code improvements, experiments, and model development.

References

[1] 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.

[2] Atwood, C.L., et al, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR- 6823, Sandia National Laboratories, 2003.

[3] Brown, T.D., et al, “Integrated Risk Assessment for the LaSalle Unit 2 Nuclear Power Plant,” NUREG/CR-5305, Sandia National Laboratories, 1992.

[4] 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.

[5] Dube, D.A., “Comparison of New Light-Water Reactor Risk Profiles,” Presented at the ANS PSA 2008 Topical Meeting, September 7-11, Knoxville, TN, 2008.

[6] Electric Power Research Institute, “2007 Portfolio: AP41.09, Safety Risk Technology and Application,” 2006.

[7] Electric Power Research Institute and US Nuclear Regulatory Commission Office of Nuclear Regulatory Research, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities,” NUREG/CR-6850/EPRI 1011989, 2005.

[8] Electric Power Research Institute and US Nuclear Regulatory Commission Office of Nuclear Regulatory Research, “Fire Probabilistic Risk Assessment Methods Enhancements,” NUREG/CR-6850 Supplement 1/EPRI 1019259, 2010.

[9] Gaertner, J., D. True, and I. Wall, “Safety benefits of risk assessment at US nuclear power plants,” Nuclear News, pp. 27-36, 2003.

[10] 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.

[11] 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.

[12] National Fire Protection Association,“Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” NFPA 805, 2001.

[13] Nuclear Energy Institute, “Guidance for Post-Fire Safe-Shutdown Circuit Analysis,” NEI-00-01 Rev. 1, 2005.

[14] Nuclear Energy Institute, “10 CFR 50.69 SSC Categorization Guideline,” NEI 00-04 Rev. 0, 2005.

[15] 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.

[16] Nuclear Energy Institute, “Roadmap for Attaining Realism in Fire PRAs,” December, 2010.

[17] 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.

[18] US. Nuclear Regulatory Commission, “Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants,” WASH-1400 (NUREG-75/014), 1975.

[19] US 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.

[20] US Nuclear Regulatory Commission, “Individual Plant Examination (IPE) for Severe Accident Vulnerabilities, 10 CFR 50.54(f),” Generic Letter 88-20, 1988.

[21] US Nuclear Regulatory Commission, “Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants,” NUREG-1150, 1990.

[22] US Nuclear Regulatory Commission, “Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationships to Current Regulatory Requirements,” Staff Requirements Memorandum SECY-90- 016, 1990.

[23] US 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.

[24] US 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.

[25] US Nuclear Regulatory Commission, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance," NUREG-1560, 1997.

[26] US Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decision-making: In-service Testing," Regulatory Guide 1.175, 1998.

[27] US Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance," Regulatory Guide 1.176, 1998.

[28] US Nuclear Regulatory Commission, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," Regulatory Guide 1.177, 1998.

[29] US Nuclear Regulatory Commission, "Options for Risk-Informing Revisions to 10 CFR Part 50 - Domestic Licensing of Production and Utilization Facilities," SECY-98-300, 1998.

[30] US Nuclear Regulatory Commission, "Reactor Oversight Program," NUREG-1649, Rev. 3, 2000.

[31] US Nuclear Regulatory Commission, "Consolidated Line Item Improvement Process For Adopting Standard Technical Specifications Changes for Power Reactors," RIS 2000-06, 2000.

[32] US Nuclear Regulatory Commission, "NRC Incident Investigation Program," Management Directive 8.3, 2001.

[33] US 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.

[34] US Nuclear Regulatory Commission, "Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program," NUREG-1742, 2002.

[35] US 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.

[36] US. 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.

[37] US Nuclear Regulatory Commission, "An Approach for Plant-Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping," Regulatory Guide 1.178 Rev. 1, 2003.

[38] US Nuclear Regulatory Commission, "Staff Requirements - COMNJD-03-0002 - Stabilizing the PRA Quality Expectations and Requirements," Staff Requirements Memorandum COMNJD-03-0002, 2003.

[39] US Nuclear Regulatory Commission, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," NUREG/BR-0058, Rev. 4, 2004.

[40] US Nuclear Regulatory Commission, "Effective Risk Communication: The Nuclear Regulatory Commission's Guidelines for External Risk Communication," NUREG/BR-0308, 2004.

[41] US Nuclear Regulatory Commission, "Effective Risk Communication - Guidelines for Internal Risk Communication," NUREG/BR-0318, 2004.

[42] US 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.

[43] US 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.

[44] US Nuclear Regulatory Commission, "Plan for the Implementation of the Commission's Phased Approach to PRA Quality," SECY-04-0118, 2004.

[45] US Nuclear Regulatory Commission, "Good Practices for Implementing Human Reliability Analysis (HRA)," NUREG-1792, 2005.

[46] US 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.

[47] US 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.

[48] US 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.

[49] US Nuclear Regulatory Commission, "Human Event Repository and Analysis (HERA) System, Overview," NUREG/CR-6903, 2006.

[50] US Nuclear Regulatory Commission, "Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants," Regulatory Guide 1.205, 2006.

[51] US Nuclear Regulatory Commission, "Changes to the Safety System Unavailability Performance Indicators," RIS 2006-07, 2006.

[52] US Nuclear Regulatory Commission, "Update of the Risk-Informed Regulation Implementation Plan," SECY-06-0089, 2006.

[53] US Nuclear Regulatory Commission, "Evaluation of Human Reliability Analysis Methods Against Good Practices," NUREG-1842, 2006.

[54] US 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.

[55] US Nuclear Regulatory Commission, "Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications," NUREG-1824, 2007.

[56] US Nuclear Regulatory Commission, "Update on the Improvements to the Risk-informed Regulation Implementation Plan," SECY-07-0074, 2007.

[57] US Nuclear Regulatory Commission, “A Phenomena Identification and Ranking Table (PIRT) Exercise for Nuclear Power Plant Fire Modeling Applications,” NUREG/CR-6978, 2008.

[58] US Nuclear Regulatory Commission, “Interim Staff Guidance, Probabilistic Risk Assessment Information to Support Design Certification and Combined License Applications,” DC/COL-ISG-3, 2008.

[59] US Nuclear Regulatory Commission, “Modifying the Risk-Informed Regulatory Guidance for New Reactors,” SECY- 10-0121, 2010.

[60] US Nuclear Regulatory Commission, "Annual Update of the Risk-Informed and Performance-Based Plan,” SECY-10-0143, 2010.

[61] US 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, US Nuclear Regulatory Commission, February 17, 2011.

[62] US Nuclear Regulatory Commission, “The U.S. HRA Empirical Study, Assessment of HRA Method Predictions against Operating Crew Performance on a U.S. Nuclear Power Plant Simulator”, NUREG-2156, June 2016.

[63] US Nuclear Regulatory Commission,, “*International HRA Empirical Study:*Volume 1, Phase 1 - Description of Overall Approach and Pilot Phase Results from Comparing HRA Methods to Simulator Performance Data”, NUREG/IA-0216, November 2009.

[64] US Nuclear Regulatory Commission,, “*International HRA Empirical Study:*Volume 2, Phase 2 - Results from Comparing HRA Method Predictions to Simulator Data from SGTR Scenarios, August 2011”, NUREG/IA-0216, August 2011.

[65] US Nuclear Regulatory Commission, “*International HRA Empirical Study:* Volume 3, Phase 3 - Results from Comparing HRA Methods Predictions to HAMMLAB Simulator Data on LOFW Scenarios”, NUREG/IA-0216, December 2014.

[66] US Nuclear Regulatory Commission, “A Framework for Low Power/Shutdown Fire PRA”, NUREG/CR-7114, September 2013.

[67] US Nuclear Regulatory Commission, “Cable Heat Release, Ignition, and Spread in Tray Installations During Fire (CHRISTIFIRE) Volumes 1 & 2”, NUREG/CR-7010, December 2013.

[68] US Nuclear Regulatory Commission, “EPRI/NRC-RES Fire Human Reliability Analysis Guidelines”, NUREG-1921, EPRI 1023001, July 2012.

[69] US Nuclear Regulatory Commission, “Nuclear Power Plant Fire Modeling Analysis Guidelines (NPP FIRE MAG)”, NUREG-1934, EPRI 1023259, November 2012.

[70] US Nuclear Regulatory Commission, “Joint Assessment of Cable Damage and Quantification of Effects from Fire (JACQUE-FIRE)”, NUREG/CR-7150, EPRI 1023259, May 2014.

[71] US Nuclear Regulatory Commission, “Verification and Validation of Selected Fire Models for Nuclear Power Plant Applications Supplement 1”, NUREG-1824, November 2014.

[72] US Nuclear Regulatory Commission, “Refining and Characterizing Heat Release Rates From

Electrical Enclosures During Fire (RACHELLE FIRE)”, NUREG-2178, Volume 1, EPRI 3002005578, April 2016.

[73] US Nuclear Regulatory Commission, “Heat Release Rates of Electrical Enclosure Fires (HELEN-FIRE)”, NUREG/CR-7197, April 2016.

[74] US Nuclear Regulatory Commission, “Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database: United States Fire Event Experience Through 2009”, NUREG-2169, EPRI 3002002936, January 2015.

[75] US Nuclear Regulatory Commission, “Determining the Effectiveness, Limitations, and Operator Response for Very Early Warning Fire Detection Systems in Nuclear Facilities (DELORES-VEWFIRE)”, NUREG-2180, June 2015.

[76] US Nuclear Regulatory Commission, “Historical Review and Observations of Defense-in-Depth”, NUREG/KM-009, April 2016.

[77] 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.

[78] 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, 7-11 September 2008.