JRC Scientific and Technical Reports

Application of Advanced Safety Methods Conclusions of the IAEA OECD JRC joint Technical Meeting

Andrea Bucalossi

EUR 24648 EN - 2010

EUROPEAN COMMISSION

Institute for Energy

The mission of the JRC-IE is to provide support to Community policies related to both nuclear and non-nuclear energy in order to ensure sustainable, secure and efficient energy production, distribution and use.

European Commission
Joint Research Centre
Institute for Energy

Contact information
Address: SDME 10/62, 1049 Brussels, Belgium
E-mail: andrea.bucalossi@ec.europa.eu
Tel.: +32 2 298 83 09

http://ie.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 61783

EUR 24648 EN
ISBN 978-92-79-18792-6
ISSN 1018-5593
doi:10.2790/29775

Luxembourg: Publications Office of the European Union

Printed in Luxembourg

AKNOWLEDGEMENTS

The Author would like to acknowledge all the participants of the workshop for their constructive input in finalising the findings of the Technical Meeting. Without their proactive attitude it would have not been possible to reach such a broad consensus and a complete and overarching text.

Executive Summary

The International Atomic Energy Agency (IAEA) together with the Organization for Economic Co-operation and Development - Nuclear Energy Agency (OECD/NEA) and the European Commission's Joint Research Centre - Institute for Energy, have been organizing several Technical Meetings regarding the use of Modern Safety Methods for the Licensing of Nuclear Power plants.
This document presents the main results of the Technical Meeting on "Application of Advanced Safety Methods" held on 7-11 June 2010 in Bled, Slovenia. This meeting was the fourth of a specific technical meeting series dedicated to these methods. The previous Technical Meetings on the same topic were:

- "Use of Best Estimate Approach in Licensing with Evaluation of Uncertainties", Pisa, 12-16 September 2005, Pisa, Italy
- "Use of Safety Margins and Advanced Safety Analyses Methods for Plant Modifications", 14 -19 September 2008, Budapest, Hungary,
- Application of Deterministic Best Estimate Safety Analyses**",** 21-25 September 2009, Pisa, Italy

The main objective of these Technical Meetings is to provide a forum to exchange results and present issues associated with the use of Advanced Safety Methods. More specifically focus is set on Deterministic Safety Analysis (DSA) using Best Estimate plus Uncertainty (BEPU) methods and on Probabilistic Safety Analysis (PSA).
All domains are covered (research, benchmarking, licensing) as the main goal is to provide advances in each.

With respect to the conservative methods of the 80's and 90's, the use of BEPU methods is possible today due to the increase in knowledge in Thermal-hydraulic phenomena. This is due to the extensive international experimental campaigns in Separate Effect and in Integral Test Facilities followed by a huge verification and validation effort done by the code developers and the independent users.
The use of these tools is also possible due to the availability of economical high performance computational tools. The two factors have allowed a much clearer understanding of the phenomena and a better estimation of the available safety margin during Design Base Accidents.

Industry today is moving rapidly in this direction in order to be able to demonstrate compliance to safety limits after power uprates as the older conservative methods were shown to be too pessimistic and limiting. Generally, due to the large effort in having a BEPU methodology accepted by the national nuclear licensing authority and in performing these calculations, this methodology is used only for the most limiting accident (generally a Large Break Loss of Coolant Accident (LOCA)). Currently a pioneering effort is ongoing for fully licensing of the Argentinean reactor Atucha-2 with a BEPU method.

The use of probabilistic and deterministic methods is starting to be used for defence in depth concept and also more often in combination with Deterministic Safety Analysis.

All levels of defence such as Control of abnormal plant conditions, Control of Deign Basis Accidents, Accident management (including PSA level 2), and Offsite emergency management can be addressed

The Integration of Probabilistic Safety Assessments and Deterministic Safety Analysis can also be used for improvement of the human reliability analysis. Best Estimate safety analyses can be used for a precise PSA modelling.

TABLE OF CONTENT

1. Introduction

The International Atomic Energy Agency (IAEA) together with the Organization for Economic Co-operation and Development - Nuclear Energy Agency (OECD/NEA) and the European Commission's Joint Research Centre - Institute for Energy have been organizing several Technical Meetings regarding the use of Advanced Safety Methods for the Licensing of Nuclear Power plants.
This document presents the main results of the Technical Meeting on Application of Advanced Safety Methods held on 7-11 June 2010 in Bled, Slovenia. This meeting was the fourth of a specific technical meeting series dedicated to these methods. The previous Technical Meeting on the same topic were:

- "Use of Best Estimate Approach in Licensing with Evaluation of Uncertainties", Pisa, 12-16 September 2005, Pisa, Italy
- "Use of Safety Margins and Advanced Safety Analyses Methods for Plant Modifications", 14 -19 September 2008, Budapest, Hungary,
- Application of Deterministic Best Estimate Safety Analyses**",** 21-25 September 2009, Pisa, Italy

The participants, after 3 days of presentations were requested to draft a document summarizing the main finding. A. Bucalossi and G. Vayssier were responsible for the Deterministic and Probabilistic parts, respectively. The following chapters are the summary of the Technical Meeting findings.
The Deterministic Safety Analysis section is based on the structure of IAEA Specific Safety Guide 2 (SSG-2) [1]: "Deterministic Safety Analysis for Nuclear Power Plants" whereas the Probabilistic section is based on specific findings during the meeting.

2. Application of Deterministic Safety Analysis

2.1. Areas of Application

Deterministic Safety Analyses (DSA) should be carried out for the following areas:

Design of nuclear power plants
Either a conservative approach or a best estimate methodology combined with accounting for uncertainties in prediction of margin parameters could be used to confirm that the design meets its intent.

Safety Analysis Reports
A Safety Analysis Report is required as part of licensing a new reactor design, obtaining regulatory approval for plant design or operational modifications, and finally as part of the periodic safety review. Either a conservative approach or a best estimate methodology combined with accounting for uncertainties in prediction of margin parameters could be used to perform the analysis.

Regulatory Assessment of the Analysis in the Safety Reports
The regulator, as part of the licensing review of the analysis in the Safety Reports, could perform their own analysis in order to confirm validity of the conclusions reported in the safety reports. Either a conservative approach or a best estimate methodology combined with accounting for uncertainties in prediction of margin parameter could be used towards this assessment.

Design or Operational Modifications
As part of ongoing improvements in a Nuclear Power Plant, including periodic refurbishments, safety analysis may be performed to assess the extent of the proposed modifications and their subsequent benefit. Either a conservative approach or a best estimate methodology combined with accounting for uncertainties in prediction of margin parameters could be used to perform the analysis

Root Cause Analysis and preparation of Abnormal Operation Procedures (AOP)
A best estimate methodology could be used to prepare Abnormal Operation Procedures or to perform root cause analysis of incidents which have already occurred in a Nuclear Power Plant. To better understand the behaviour of the Nuclear Power Plant, analysis of such incidents could include hypothetical failure of some components or systems.

The development and maintenance of emergency operating procedures and accident management procedures.
Best estimate codes together with realistic assumptions should be used in these cases.
Severe Accident Management: A best estimate methodology could be used to perform Severe Accident Management Guidalines (SAMG) analysis. To better understand the behaviour of the Nuclear Power Plant, analysis of such incidents could include hypothetical failure of some components or systems.

Periodic Safety Review
The refinement of previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid.

Safety Analysis should be performed using validated computational toolsets. During the licensing period, the computer codes should be maintained in a frozen state in order to ensure consistency and audit-ability of the safety analysis reported in the safety reports, although minor changes that do not impact the qualification of the code can be acceptable. Better understanding of the underlying phenomena as a result of the on-going research and development activities could be incorporated in these codes in form of new models. However, unless these findings have an adverse impact on the conclusions in the Safety reports, a revision to the analysis would have to wait until the next licensing period.

2.2. Application of Deterministic Safety Analysis to the Design of Nuclear Power Plants

The Design Basis (DB) for Systems, Components and Structures (SSC) which are important to safety is required to be established and confirmed by means of a comprehensive safety assessment. The design basis includes design requirements that must be met to ensure safe operation of a nuclear power plant. Deterministic safety analysis, either in form of a conservative approach or a best estimate methodology combined with accounting for uncertainties in prediction of margin parameters, is used to confirm that the design meets its intent. Applicability of the analytical assumptions, methods and degree of conservatism used in the safety analysis must be verifiable.

2.3. Application of Deterministic Safety Analysis to the Licensing of Nuclear Power Plants

Compliance with all applicable regulations and standards and other relevant safety requirements is essential for the safe and reliable operation of a nuclear power plant. This should be demonstrated by means of an initial or an updated safety analysis report.
The safety analysis of the plant design must be consistent with the current or ‘as built’ state. The safety analysis examines:

- All planned modes of the plant in normal operation;
- Plant performance in anticipated operational occurrences;
- Design basis accidents;
- Event sequences that may lead to beyond design basis accidents.

On the basis of this analysis, the robustness of the engineering design to perform its safety functions during postulated initiating events and accidents should be established. In addition, the effectiveness of the safety systems and safety related systems should be demonstrated, and guidance for emergency response should be provided.

Analyses should be performed for transients that can occur in all planned modes of the plant in normal operation, including operations during shutdown. This plant state was sometimes neglected in early safety analyses. For this mode of operation, the contributors to risk include: the inability to start some safety systems automatically; equipment in maintenance or in repair; reduced amounts of coolant in the primary circuit as well as the secondary circuit for some modes; instrumentation switched off or non-functional and measurements not made; open primary circuit; and open containment. Where appropriate, the specific features of a best estimate analysis of shutdown transients should include thermal stratification of coolant in the reactor pressure vessel, low power, low inventory conditions, the presence of non-condensable gases and long term evolution of a transient. Every configuration of shutdown modes should be analysed. The main objectives of the analysis are to evaluate the ability of plant systems to perform safety functions and to determine the time available for the operators to establish safety functions. These safety functions include controlling the reactivity of the fuel, maintaining the ability to remove heat from the fuel, confinement of radioactive materials. The range of scenarios should be evaluated to determine whether abrupt changes in the results of the analysis occur for a realistic variation of inputs (usually termed bifurcation or cliff edge effects).

Use of Deterministic Analysis for the Licensing of Nuclear Power Plants (NPP) implies the use of qualified tools, tool's users and methodologies. Such qualification process should be fixed and detailed by the corresponding nuclear safety regulator, taking into account, as much as possible, the best practices at the international levels. For keeping the qualification level at a state-of-the-art, the active participation of the technical support organizations of the nuclear regulatory body to international computational benchmarks, experimental campaigns and methodologies assessment projects should be recommended.

Therefore, Final Safety Analyses Report should be submitted with a series of supporting documents in which a proof of the conducted validation campaign is demonstrated. Proper use of best-estimate codes should be encouraged for the licensing analyses. Analysis by the three dimensional neutron kinetics coupled thermal-hydraulic codes should also be recommended where accident progression results in asymmetric distribution of power, thermalhydraulic properties or poison load. Investigation of the effects of the power shape changes during the transients on the peak cladding temperature should be performed and used for a better understanding of the available safety margin. Beneficial actions from the control system should not be considered during this kind of calculations.

Uncertainties sources and their quantifications should be carefully evaluated. A clear distinction between which are the code uncertainties and the input uncertainties should always be provided in the documentation. Effects of different software operating systems on the results should also be checked and clearly documented.

2.4. Application of Deterministic Safety Analysis to the Assessment of Safety Analysis Reports

The operating organization must ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body. Additional independent analyses of selected aspects may also be carried out by or on behalf of the regulatory body. The use of multiple fully independent computational tools and methodologies by these independent individuals or groups should be pursued. Advanced best-estimate computational techniques should be used only when both the code and user are qualified.

2.5. Application of Deterministic Safety Analysis in Plant Modifications

A nuclear power plant may be modified on the basis of feedback from operational experience, the findings of periodic safety reviews, regulatory requirements, advances in knowledge or developments in technology. To comply with the requirements, a revision of the safety analysis of the plant design should be made when major modifications or modernization programmes are implemented, when advances in technical knowledge and understanding of physical phenomena are made, when changes in the described plant configuration are implemented or when changes are made in operating procedures owing to operational experience.

The modification of existing nuclear power plants is normally undertaken to counteract the ageing of the plant, to justify the continued operation of the plant, to take advantage of developments in technology or to comply with changes to the applicable rules and regulations. More specifically a nuclear safety related modification refers to a permanent or temporary alteration from the original design of structures, systems, components, operations, processes, operating and emergency procedures, operating limits and conditions, technical specifications that could influence nuclear safety. The following, for example, are excluded from the definition:

- Replacement of a component with a new one that is exactly the same.
- Normal maintenance
- Operational changes within the existing safety justification, without changing the operating procedures or other safety documentation.

Other important applications of deterministic safety analysis are aimed at the more economical utilization of the reactor and the nuclear fuel. Most of the major modifications performed in the industry deal with power up rates, Steam Generator Replacement (even without power uprating but due to technological aging), new type of fuel and replacement of major systems (e.g. Instrumentation & Control). Such applications often imply that the safety margins to operating limits are reduced and special care should be taken to ensure that the limits are not exceeded.

All the effects of plant changes should be considered and the analysis should cover all possible aspects of the plant changes. In addition, it should be demonstrated that the cumulative effects of changes are acceptable.

Deterministic safety analyses should be used both for safety improvements and to support modifications to improve the economy of the plant. In all cases, the safe operation of the plant in accordance with the assumptions and intent of the design should be verified and this should be the main focus of the deterministic safety analyses.

The impact of major plant modifications on Operating Limits and Conditions (OLC) and on Operating Instructions and Procedure (OIP) will differ from depending on the exact plant modification performed. Experience showed that in most cases the safety margins and set-points of the plant have been modified (e.g. former constant linear power limit replaced by one decreasing with burn-up; the set-points of: average temperature, the water level in the pressurizer, the pressure in the steam generators, the water level in the steam generators, etc) but on the contrary only minor changes to the OIP occurred.

2.6. Application of Deterministic Safety Analysis to the Analysis of Operational Events

Accident analyses may be used as a tool for obtaining a full understanding of events that occur during the operation of nuclear power plants, and should form an integral part of the feedback from operational experience. Operational events may be analysed with the following objectives:

- As an aid to the traditional root-cause methodologies to the analysis of an Operational event
- To check the adequacy of the selection of postulated initiating events;

- To determine whether the transients that have been analysed in the safety analysis report bound the event;
- To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;
- To check whether the plant operators and plant systems performed as intended and evaluate the impact of operator interaction and automatic procedures;
- To check and review emergency operating procedures;
- To have a better understanding and identify any new safety issues and questions arising from the analyses;
- To support the resolution of potential safety issues that are identified in the analysis of an event;
- To analyse the severity of possible consequences in the event of additional failures (such as severe accident precursors);
- To validate and adjust the models in the computer codes that are used for analyses and in training simulators.

The analysis of operational events requires the use of a best estimate approach. Actual plant data should be used.

Since very often plant measurement recordings are not sufficient for the operational event analyses sensitivity studies, should be performed to acquire confidence with the predictions. The evaluation of safety significant events is a very important aspect of the feedback of operational experience. Modern best estimate computer codes make it possible to investigate and to gain a detailed understanding of plant behaviour. Conclusions from such analyses should be incorporated into the plant procedures that address the use of feedback from operational experience.

Most of the large number of operational events that have occurred in nuclear power plants have been analyzed qualitatively to establish root causes but only a few were investigated by using deterministic computer codes. Only when the phenomena were not understood and the root cause was not identified or the safety margin was challenged the need for a deterministic safety analysis was required. Typical events that fall into this category are:

- Malfunction of valves, pumps or other components, resulting in a complex transient response
- Inadequate/unexpected response of a control or safety system
- Pipeline leakage, rupture or thermal fatigue
- Reactivity events

The deterministic safety analysis may be performed either on a dedicated training simulator (plant analyzers) or on a dedicated specific input deck depending on the complexity of the transient.

2.7. Application of Deterministic Safety Analysis to the Development and Validation of Emergency Operating Procedures

Best estimate deterministic safety analyses should be performed to confirm the strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and design basis accidents. These strategies are reflected in the Emergency Operating Procedures (EOPs) that define the actions that should be taken during such events. Deterministic safety analyses are required to provide the input that is necessary to specify the operator actions to be taken in response to some accidents, and the analyses should be an important element in the review of accident management strategies. In the development of the recovery strategies, to establish the available time period for the operator to take effective action, sensitivity calculations should be carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures.

After the EOPs have been developed, a validation analysis should be performed. This analysis is usually performed by using a qualified simulator. The validation should confirm that a trained operator can perform the specified actions within the time period allowed and that the reactor will reach a safe end state. Possible failures of plant systems and possible errors by the operator should be considered in the sensitivity analyses.

When the predictions of a computer code that has been used to support or to verify a EOPs do not agree with observed plant behaviour during an event, the code and the procedure should be reviewed. Any changes that are made to the emergency operating procedure should be consistent with the observed plant behaviour.

EOPs provide predefined and prioritized event and symptom based response procedures that give guidance to the operator in management of accidents, and diagnosis to guide plant recovery to the optimal end state. Accident analysis is an important step in the EOP development because computer simulation is the most comprehensive way of knowing the response of the plant in various transient conditions to the recovery strategies. Best estimate deterministic safety analysis can provide general trends of plant parameters, available symptoms, states, timing of actions, and as such play a role in strategy development as well as verification of some safety criteria. The deterministic safety analysis can be applied to analytical support tasks in development of EOPs such as: identification of plant vulnerabilities, success criteria[1], time and means available to operator for the success of the applied measures and specifics of plant behaviour. Determining and validation of strategies, or selecting the strategy among different possibilities for the individual EOPs could involve a large number of best estimate analyses.

Defining the time window in which one action is successful is very important for defining and validation of the procedure. Uncertainty of one event could play a large role in the overall plant recovery. This estimate is usually based on the sensitivity studies, also the definition of the strategies and set-point values. The various uncertainty methodologies can be implemented for determining strategies and set-point values, and also the operator actions in order to give the minimum time window for operator actions which will ensure successful completion of the recovery procedure.

[1] i.e. what equipment is needed to remain inside acceptance criteria – this can be different from the equipment analysed by conservative codes. In addition, EOPs may cover events which are beyond the plant licensed design basis.

Importance of using best estimate deterministic analysis in development and validation of EOPs lies in addition in analysis of Pressurized Thermal Shock transients (PTS), transients with high pressure in reactor coolant system and interaction of cold safety injection water and hot vessel wall. Operator actions undertaken to mitigate consequences of the accidents should not increase the probability of the reactor pressure vessel failure. Integrity of the RPV must be preserved throughout the plant operation during all operational states and accident conditions. In order to address this issue and to provide bounding analysis for the development of the EOPs deterministic best estimate analysis should be applied for the screening of the most severe PTS scenarios caused by operator's actions. PTS screening methodology based on the application of the determined PTS criteria on the results of the deterministic analysis will screen out the most severe PTS transients for which, in development of EOPs, special care has to be provided in order to avoid increasing of the probability that the operator's actions, which they are instructed to perform in order to mitigate accidents, could adversely affect integrity of the reactor pressure vessel.

2.8. Application of Deterministic Safety Analysis to the Development of Guidelines for the Management of Severe Accidents

Deterministic safety analyses should also be performed to assist the development of the strategy that an operator should follow if the emergency operating procedures fail to prevent a severe accident from occurring. The analyses should be carried out by using one or more of the specialized computer codes that are available to model relevant physical phenomena. Physical phenomena in case of severe accidents are strongly interdependent, e.g. thermal hydraulics, chemical interactions, material liquefaction during the flooding of hot damaged cores.

For light water reactors, these include thermohydraulic effects, heating and melting of the reactor core, the retention of the molten core in the lower plenum, molten-core–concrete interactions, steam explosions, hydrogen generation and combustion, fission product behaviour and containment direct heating to confirm the risk of containment failure if in-vessel retention is not available.

The analyses should be performed using a number of validated best estimate computer codes as, usually, no single code can represent all the concerned phenomena. During the analysis unique features of the plant should be taken into account. The analyses should be used to identify what challenges to fission product boundaries can be expected during progression of accidents and which phenomena will occur. These should be used to provide the basis for developing strategies, followed by the development of a set of guidelines for managing accidents and mitigating their consequences.

In the analyses uncertainties in timing and magnitude of phenomena should be considered. The analysis should start with the selection of the accident sequences which, without intervention by the operator, would lead to core damage.

All core damage sequences identified in the PSA, if available, should be considered and also operator errors, which can lead to severe accident conditions should be analysed.

A grouping of accident sequences with similar characteristics should be used to limit the number of sequences that need to be analysed. Such a categorization may be based on several indicators of the state of the plant: the postulated initiating event, shutdown status, the status of the emergency core cooling systems, the coolant pressure boundary, the secondary heat sink, the system for the removal of containment heat and the containment boundary.

The measures can be broadly divided into preventive measures and mitigatory actions. Both categories should be subject to analysis.

Preventive measures are recovery strategies to prevent core or fuel damage. They should be analysed to investigate what actions are possible to inhibit or delay the onset of core damage. Examples of such actions are: various manual restorations of systems; primary and secondary feed and bleed; depressurization of the primary or secondary system; and restarting of the reactor coolant pumps. Conditions for the initiation of the actions should be specified, as well as criteria for when to throttle or stop the actions, or to change to another action.

Mitigatory measures are strategies for managing severe accidents to mitigate the consequences of core melt. Such strategies include: coolant injection to the degraded core; depressurization of the primary circuit; operation of containment sprays; and the use of the fan coolers, hydrogen recombiners and filtered containment venting. Such measures are available in reactors of different types that are in operation or being constructed. Possible adverse effects that may occur as a consequence of taking mitigatory measures should be taken into account, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen deflagration or detonation.

2.9. Periodic Safety Reviews (PSR)

New deterministic analyses may be required to refine previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid or, otherwise, initiate corrective actions. In such analyses, account should be taken of any margins that may have become reduced and may continue to be reduced owing to ageing over the period under consideration or to newer safety insights, changes in regulations, or to other processes that may influence previously defined or understood safety margins.

Usually, there is no reduction of calculated margin in deterministic analysis used as licensing bases (currently conservative approach in respect to parameters and equipment availability – option 1 and 2) because via appropriate maintenance, surveillance and configuration management (which are obviously subject of PSR activities) the real parameters and equipment status are kept sufficiently distant from limiting values incorporated in licensing analysis. Certain margin exists between SSC's status and parameters used in safety analysis (which is changing by ageing etc.). It is ensured that existing margin between calculated results by safety analysis and the criteria remains the same. Best estimate analyses together with an evaluation of the uncertainties may be appropriate to demonstrate that the remaining margins are adequate.

The objective of a PSR is to determine by means of a comprehensive assessment of an existing nuclear power plant:

- the extent to which the plant conforms to current international safety standards and practices;
- the extent to which the licensing basis remains valid;
- the adequacy of the arrangements that are in place to maintain plant safety until the next PSR or the end of plant lifetime;

- and the safety improvements to be implemented to resolve the safety issues that have been identified (NS-G-2.10 [2] par. 2.8).

The PSR is a full scope comprehensive safety assessment method, which covers all safety important aspects of nuclear power plant. According to NS-G-2.10 the hereinafter areas of review should b considered: (1) Plant design, (2) Actual condition of SSCs, (3) Equipment qualification, (4) Ageing, (5) Deterministic safety analysis, (6) Probabilistic safety analysis, (7) Hazard analysis, (8) Safety performance, (9) Use of experience from other plants and research findings, (10) Organization and administration, (11) Procedures, (12) The human factor, (13) Emergency planning. (14) Radiological impact on the environment (NS-G-2.10 par. 2.8).

Because the typical frequency of a periodic safety review is 10 years, a possibility exists of significant increase of knowledge, standards and technologies. Effects of ageing, cumulative effects of modifications (technical and organizational) etc. could become significant. Taking into account all these changes, the task of PSR is to provide assurance that measures either already present at the plant or adopted as a corrective measure will ensure safe operation for the period of time until the next PSR.

2.9.1. Deterministic safety analysis – PSR review area 5 (in NS-G-2.10, para 4.1)

The objective of the deterministic safety analysis review is to determine to what extent the existing deterministic safety analysis remains valid when the following aspects have been taken into account:

- actual plant design;
- the actual condition of SSCs and their predicted state at the end of the period covered by the PSR;
- current deterministic methods; and
- current safety standards and knowledge.

In addition, the review should also identify any weaknesses relating to the application of the defence in depth concept (NS-G-2.10 par. 4.26).
The deterministic analysis in this PSR review area can be used in these cases:

- update of analysis performed by outdated computational tools
- evaluating new Postulated Initiating Events (PIE) based on plant's own e.g. PSA studies (PSR review area No. 6), new legislative requirements or hazard analysis (PSR review area No. 7)
- new approaches and presumptions based on latest research and development could be required by the regulatory authorities
- PSR usage as a source of input for Long Term Operation (LTO), BEPU methods could be advantage for assurance that safety margins will remain acceptable.

2.9.2. Other PSR review areas

Usage of deterministic analysis in a framework of PSR is not bound to deterministic safety analysis area only. It can be used in:

<u>Area 1 – plant design.</u>
Example could be the situation when Design Bases information is not fully available at plant. In certain situation the necessary Design Bases information (parameters) could be reconstituted using deterministic analysis. The Design Bases information is not only

necessary for safe configuration management, but the PSR itself uses Design Bases information e.g. to confirm adequacy of current (and predicted) status of SSC's.

Area 11 – procedures

Sometimes the procedures (e.g. Abnormal Operating Procedures) could be derived mainly on engineering judgement. During the PSR the deterministic analysis using best estimate techniques may be required to confirm adequacy of these procedures. Development of Emergency Operating Procedures and SAMG's is another typical application of best estimate deterministic analysis connected to PSR area 11.

3. Application Of Probabilistic Safety Analysis

3.1. General observations of PSA applications

- For all Defence-in-Depth (DiD) levels the PSA should be a living PSA. Human reliability aspects are part of the training for operation including maintenance to obtain a low failure rate of equipment.
- Cost-benefit analyses are one of PSA applications. Apart from dose, social economic effects and environmental consequences might also be considered, as large releases may have detrimental effects on the functioning of the society and on the environment.
- Not using PSA is not beneficial for safety.
- PSA should only be used with an estimate of the uncertainties in the results.
- PSA should be executed on the base of internationally accepted standards.

3.2. Application of PSA into various levels of the did concept

INSAG 10 [3] defines the concept of Defence in Depth as follows:

The concept of defence in depth, which concerns the protection of both the public and workers, is fundamental to the safety of nuclear installations. As was stated the Basic Safety Principles for Nuclear Power Plants (INSAG-3) in relation to the safety of nuclear power plants, "All safety activities, whether organizational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth..."

Further description of Defence in Depth is provided by NS-R-1 [4] and NS-G-1.2 [5].

3.2.1. Defence in Depth Level 1 – Avoidance of abnormal plant state by good design

- Risk Informed Operational Limits and Conditions (OLC, often called Technical Specifications)
    - allowed outage time including plant outage (e.g. CANDU)
    - selection of mandatory[2] plant modes after exceeding limiting conditions for operations (LCO)
- Online maintenance and inspection
- Shutdown planning
- Risk Monitor as a support to plant state modifications[3] and to support online maintenance and inspection and shutdown planning – support also for the national regulatory authority (NRA), possibly online available
- Design reliability in normal operating systems to avoid intervention of protective systems
- PSA for proper electric grid connection: no loss of electric grid upon turbine trip or load rejection[4]

---

[2] Often, exceeding OLC mandates cold shutdown. Risk analysis may show that e.g. hot standby is also an acceptable mode, which avoids taking the plant through the large transient that the cold shutdown is.

[3] An example of an industrial tool is the EOOS risk monitor (Equipment Out Of Service) by EPRI

- Effects and control of ageing

3.2.2. Defence in Depth Level 2 – Control of abnormal plant conditions

- PSA can be used to obtain a high reliability of the control systems
- PSA can be used to optimize control action set points (plant conditions[5] II, AOO)

3.2.3. Defence in Depth Level 3 – Control of design Basis Accidents (includes Plant Conditions III and IV, AOOs and DBAs)

- PSA can be used to obtain a high reliability of the safety systems (e.g. degree of redundancy and diversity, role of spatial separation of trains and sub-trains) including finding weak points in safety systems design, such as common cause failures (traditional weak points)
- PSA can be used to optimize safety system set points (plant conditions III and IV, DBA), using for instance sensitivity analysis
- PSA may be used to identify systems and parts of systems relevant to safety, although they are not classified as safety systems. This includes auxiliary systems (e.g., for keeping lines full, for lubrication, for pneumatic air, etc.[6])
- PSA can be used for the optimization of EOPs, up to and including DBA[7]s, including human reliability aspects
- PSA can find the vulnerability of low pressure parts of supportive systems potentially subjected to high RCS pressure (by improper isolation between the high pressure and low pressure parts)
- PSA can be used to optimize the separation between SBLOCA and LBLOCA

3.2.4. DiD level 4 – Accident management (includes PSA level 2)

- PSA gives safety relevance of systems for prevention of core melt in BDBA (e.g. ATWS, SBO, Total Loss of Heat Sink)
- Optimization of EOPs (for BDBA not being core melts)
- PSA gives the scenarios that challenge fission product boundaries, i.e. plant vulnerabilities for severe accidents. Examples of such challenges are hydrogen combustion, containment pressurization, basemat melt trough, interfacing LOCA.
- PSA gives the plant capabilities to mitigate severe accidents (e.g., impact of igniters, containment vent, flooding of RPV cavity).
- PSA is an appropriate tool for developing the SAMGs in that it provides the chronology of the fission products boundary challenges and, hence, the nature and the priority of the potential counter measures
- PSA provides scenarios to train the operators for emergencies and execution of SAMG; here care should be exercised that the scenarios selected will lead to execution of an appropriate number of guidelines
- PSA is also a tool to investigate the reliability of mitigation actions (e.g. in the AP 1000 the connection from the RWST to the reactor cavity). This includes consequences of and potential counter measures against spurious actuation of the mitigative actions.

---

[4] For added reliability, connecting lines to diesels may be suspended

[5] This terminology has been superseeded, but is still frequently in use.

[6] Further information e.g. in ANS 58.14

[7] For beyond DBA, see DiD level 4

Caution: PSA-predicted plant performance may not always be what the plant operators will see and therefore, the plant operator may induce wrong actions if he deduces his actions from such plant predictions (e.g. actual containment pressure at RPV melt-through may be smaller than predicted - due to the lack of heavy thermo-hydraulic shock - and the operator may assume that the core is still in the vessel). PSA may have bifurcations that we may not see in an actual transient.

3.2.5. DiD level 5 – Offsite emergency management

- PSA provide scenarios for offsite emergency management drills
- PSA provide estimates of potential releases during real events (this pre-supposes a certain insight in ongoing accidents[8]).
- PSA can be used for regulation based on release limits (requires PSA-2 level)
- PSA can be used for regulation based on doses (requires PSA-3 level)

3.3. Limitations and improper use of PSA

- Safety systems should not be candidates for being deleted from the design basis due to the calculated low safety benefit[9]
- PSA should not be used to fill up the margins to available safety criteria
- PSA is and remains an assessment tool, and is not a design tool
- PSA should not be used to decrease sound conservative design margins.
- A PSA scenario is a sketch of the reality – it will never represent a real event
- PSA, like any other assessment tool, has inherent limitations: it can not fully take into consideration the human behaviour, e.g. the quality of different manufacturers for the same piece of equipment, etc.

[8] A program capable of providing a capability for timely estimate of the likely release of radioactivity to the environment from possible nuclear accidents is STERPS. See also the program SPRINT (e.g. at www.enconet.com).

[9] An example is a vendor who removed the originally present double-wall containment from the design, because he found through PSA that he was able to stay inside regulatory criteria with a single-wall containment

4. Conclusions

The main objective of these Technical Meetings was to provide a forum to exchange results and present issues associated to the use of Advanced Safety Methods. More specifically focus was set on Deterministic Safety Analysis using Best Estimate plus Uncertainty (BEPU) methods and on Probabilistic Safety Analysis. All domains were covered (research, benchmarking, licensing) as the main goal was to provide advances in each.

Industry today is moving rapidly in this direction in order to be able to demonstrate compliance to safety limits after power uprates as the older conservative methods were shown to be too pessimistic. Generally, due to the large effort in having a BEPU methodology accepted by the national nuclear licensing authority and in performing these calculations, this methodology is used for the most limiting accident (generally a Large Break LOCA). Currently a pioneering effort is ongoing for fully licensing of the Argentinean reactor Atucha-2 with a BEPU method.

The use of probabilistic and deterministic methods is starting to be used for defence in depth concept and also more often in combination with Deterministic Safety Analysis. All levels of defence such as Control of abnormal plant conditions, Control of Design Basis Accidents, Accident management (including PSA level 2), and Offsite emergency management can be addressed.

The Integration of Probabilistic Safety Assessments and Deterministic Safety Analysis can also be used for improvement of the human reliability analysis. Best Estimate safety analyses can be used for a precise PSA modelling.

5. References

[1] IAEA SSG-2 "Deterministic Safety Analysis for Nuclear Power Plants" , 2010, Vienna

[2] IAEA NS-G-2.10 " Periodic Safety Review of Nuclear Power Plants",2003, Vienna

[3] INSAG 10 " Defence in Depth in Nuclear Safety", 1996, Vienna

[4] IAEA NS-R-1 " Safety of Nuclear Power Plants: Design ", 2000, Vienna

[5] IAEA NS-G-1.2 "Safety Assessment and Verification for Nuclear Power Plants ", 2001, Vienna

APPENDIX 1: NATIONAL APPLICATIONS OF PSA

A1.1 India

The safety analysis of Nuclear Power Plants (NPPs) is carried out using both deterministic and probabilistic methods. The probabilistic safety analysis (PSA) level – 1 has been carried out for NPPs at full power operation with internal initiating events. Level-2 PSA at full power operation has been carried out for one NPP. Level – 3 PSA has not been done. The low power and shutdown PSA has not been done.

The initiating events (IEs) are classified as LOCA IE and transient IE. The system reliabilities are evaluated using fault tree approach. For initiating event frequencies both generic values and plant specific values have been used. The component failure data from plant and generic data has been used and also Bayesian updating carried out. Common cause failure (CCF) analysis has been carried out for pumps, valves etc. The uncertainty analysis is performed for the PSA level-1. Human errors in execution of tasks (pre initiators and post initiators) are considered in the fault trees using human reliability analysis (HRA).

The risk measure in terms of core damage frequency (CDF) is calculated from the IE event trees. These are compared against IAEA recommended value.

A1.2 Republic of Korea

Primary purposes of PSA implementation in Korea are to identify the risk level and to show that a plant operates under the safety goal (10E-4/yr CDF) (which is not a legal requirement currently, but there is no plant to violate the safety goal).

For the identification of risk level of all plants, Korean nuclear regulation authority (KINS, Korea Institute of Nuclear Safety) had pushed the licensee to implement Level 1 and Level 2 PSA for all licensed plants from the middle of 1990s. PSA reports for operating plants had been submitted to the regulation authority individually without regulation requirements (legal enforcement) and they have been being periodically updated for reliability data and model. However, for new plants under licensing process including the licensing renewal plants, licensee should submit PSA report as a part of Safety Analysis Report (SAR) to approve the operating license.

Principal frameworks for the regulation in Korea are based on the deterministic approaches, so probabilistic approaches such as risk-informed applications have been approved case by case. A few of applications have been done and other cases are processing now. For examples, the extension of surveillance test interval (STI) of Plant Protection System (Reactor Protection System and Engineered Safety Features Actuation Systems) has been approved for some plants, but for the other plants it has been partially approved and remaining parts are processing now; Extension of the test interval for Integrated Leak Rate Test of Containment has been being approved plant by plant).

A1.3 Mexico

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 establish a methodology to assess the impact on safety of proposals for permanent changes to the licensing basis and also, changes to the technical specifications, supported only by deterministic analysis or by a combination of deterministic and probabilistic analysis. The methodology considers relevant aspects such as safety margins, defence in depth, risk criteria and monitoring performance.

A procedure to link deterministic and probabilistic tools to evaluate operational events and inspection findings was developed looking for an integral decision making process and focus resources in the most relevant event and findings including the risk point of view. Modifications to NRC/SDP were performed to include a flow chart instead of a questionnaire in the first event/finding screening, and the worksheets developed as part of the procedure were automated in order to facilitate their application; the simplified PRA model required by the procedure was validated with the LVNPP IPE model. Also, a Risk Based Inspection Guides (RBIG) has been developed to incorporate risk information into the inspections activities. The RBIG have been used to prioritize inspections and to optimize resources.

A1.4 Netherlands

The Netherlands Regulatory Authority (NRA[10]) has demanded the licensees to do a full PSA level 1 - 3. This work was completed already in the 1990's. The licensees should conform to the safety goals set by the NRA. These limits are quite strict in that they postulate a more than linear[11] decrease of probability with increasing releases. The PSAs should be kept ‘living’.

The NRA has also considered to develop and implement risk-informed regulation, departing from the USNRC approach (e.g. RG 1.174), but actual progress is limited. One application is that the licensee(s) must continuously seek to reduce risk and report back to the NRA on an annual basis.

PSA is used to develop scenarios for emergency response exercises, including SAMG execution.

A1.5 Romania

The use of PSA is made under a special regulation ‘Requirements on Probabilistic Safety Assessment for Nuclear Power Plants’, published on Official Monitor, Part I, nr. 980 from 07/12/2006. The main principles mentioned to be followed in this norm are:

1. In addition to DSA the Authorization Holder have to elaborate and use also PSA on design and operating stages of an NPP. All the hypothesis used in PSA on modelling and quantifying the accident sequences have to be as realistic as possible – Art.3;
2. […] The PSA methodology and results have to be independently evaluated – Art.5;
3. […] On developing PSA the exclusion of some initiating events have to be justified taking into consideration both the sequence of event and the consequences of these – Art.8 (3);

[10] Dutch acronym: KFD
[11] In fact, quadratic.

4. PSA should be based on a realistic model of the NPP response to events, using relevant dates for the project and taking into consideration the human operator actions according to the Operating Procedures for normal operation, and as for accident situations. The human liability analysis has to be done taking into consideration the factors that may influence the human operator actions on each NPP state – Art.9;
5. PSA have to include all the relevant connections and interactions between the NPP's systems. […] – Art.10 (1);
6. By PSA it has to be demonstrated that the NPP project is balanced […] – Art.11;
7. […] PSA has to include uncertainty analysis and sensitivity studies. – Art.12;
8. […] this database[12] has to be continuously followed, analysed and kept up to date, and the PSA has to be actualized to reflect the exploitation experience. – Art.13 (2);
9. PSA has to rely on the actualized project of the NPP. […] – Art.14.

Regarding the use of PSA, it is stipulated in these norms that the utilization of PSA has to be considered at least on the following aspects […]:

a) For the identification of factors which have impact on nuclear security, for systematic revision of safety margins and existent security reserves;
b) For the revision of Limits and Conditions for Operation;
c) For the revision of nuclear safety classification and categorization of the structures, systems, components and equipments of the NPP;
d) For the implementation of a program for monitoring the risk in exploitation;
e) For establishing and planning the inspections during the operation of the NPP, paying a great attention to the components that were identified as presenting a significant contribution to risk;
f) For the identification of practical improvements with the purpose of reducing the risk associated to NPP exploitation;
g) For evaluating of the important modifications for nuclear safety;
h) For the analysis of the events that have occurred in the NPP and for evaluating their significance for the nuclear safety;
i) For the optimization of the preventive maintenance and testing programs. – Art.22.

[12] On the DB establishing, at least the following data categories have to be taken into consideration: the frequency of different initiating events, the frequency and the duration needed for getting out of service the equipments and components important to nuclear safety, the failure rate for the equipment important to nuclear safety, the relevant data for the common cause failures and the data needed for the estimation of human errors probabilities.

Appendix 2: APPLICATIONS OF THE COMBINATION OF PSA AND DSA AT THE PRESENT TECHNICAL MEETING

The following two papers in the presentation explicitly cover the combination of PSA and DSA.

A2.1 Integration of Probabilistic Safety Assessments and Deterministic Safety Analysis for improvement of the human reliability analysis, *A. Prosek - M. Cepin*, Slovenia

Human reliability analysis is an important support and a part of probabilistic safety assessment. The objective of this paper is to integrate realistic deterministic safety analysis and probabilistic safety assessment to show how deterministic safety analysis impacts the human reliability analysis. The RELAP5/MOD3.3 Patch 03 computer code is used for realistic safety analysis. Parametric safety analysis studies represent a standpoint for determining the time parameters for human actions, which are used within calculation of human error probabilities. The method is demonstrated through selected representative human actions. The results show that realistic safety analysis represents an important standpoint for assessment of human error probabilities within human reliability analysis.

A2.2 Insights from the best estimate safe analyses for a precise PSA modelling, *S. Han*, Republic of Korea

As an effort to improve the current probabilistic safety assessment (PSA) model for OPR-1000, we found several areas that needed a re-estimation of the accident sequences by using a best-estimated thermal hydraulic code. As one of these areas, we identified that the LOCA sequences should be improved in the analysis model associated with the classification of the LOCA groups as well as the arrangement of the safety injection water source.

Firstly, we identified the classification problem of the LOCA groups in the current PSA for the OPR-1000, but they did not affect the result of the LOCA sequences because of the limitation of the current PSA approach. However, we expect that our reclassification could be useful if we try to apply a new approach to the estimation of the initiator frequency based on the mechanical characteristics, like a concept of the leak-before-break (LBB) applied to a pipe failure. Secondly, we estimated the effect from the chronological order between the recirculation operation of the safety injection system and the shutdown cooling operation. Especially, because it is necessary to supply small injection flow at a small break LOCA, the chronological order has a large effect on the core damage frequency.

Although a precise estimation was not achieved in this study, we showed that the chronological order between the re-circulation operation of the safety injection and the shutdown cooling operation had a large impact on the core damage frequency in the small break LOCA. We concluded that the present re-estimation has the potential of a realistic estimation and it is necessary to improve the current PSA model using the new information.

APPENDIX 3: EXAMPLES OF COMBINED PROBABILISTIC AND DETERMINISTIC ANALYSIS

A3.1 ATUCHA-2 (Argentina)

Probabilistic safety analysis plays a major role in nuclear installation licensing in Argentina. The nuclear regulatory authority of Argentina, ARN, has been established in its current configuration as an autonomous body by the Act 24,804, on April 25th of 1997.

In accordance with the above mentioned act, ARN is entitled to “establish regulations related to radiation and nuclear safety, physical protection and nuclear materials use control, the licensing and control of nuclear facilities, international safeguards and transport of nuclear materials”.

Extensive use of deterministic and probabilistic methods has been made at regulatory level for definition of boundary conditions and acceptance criteria for NPP accident analyses. While in most countries the backbone for accident analysis is performed by deterministic safety analysis (DSA) methods with probabilistic considerations to categorize the postulated initiating events (PIE), and the correspondent acceptance criteria , ARN prescribed in the regulatory standard AR 3.1.3, “Radiological criteria relating to accidents in nuclear power plants”, the use of probabilistic methods to perform safety analysis.

Plant acceptability is derived from the overall radiological consequences for the grouped events (into ten groups), by entering into the left lower triangle of Figure A3.1. The radiological consequences, in terms of effective dose, have to be evaluated for the so called “critical group”. Associated probabilities to each one of the ten event groups are determined following typical probabilistic methods to evaluate fault trees and event trees.
Despite the fact that the current trend in nuclear safety is moving towards a combined approach of both deterministic and probabilistic safety analyses methods, leading to the so-called “risk-informed” regulation, the Argentinean regulatory standard can be seen as an example of a more “risk-based” regulation.

Even though that the decision making process for the licensing of Atucha 2 NPP has to consider the probabilistic criterion of ARN standard, the current licensing process is following a combination of both DSA and PSA approaches.
Example – licensing of Atucha2 NPP in Argentina is carried out according to regulation AR 3.1.3 but at the same time, ARN is requiring a traditional Final Safety Analysis Report with a well established scope for a Deterministic Safety Analysis

Argentina was one of the first countries to move towards what is nowadays termed “risk-based regulation”. As explained above, accident analysis should deploy probabilistic methods to determine the frequency of the event, considering also availability of safety systems to determine the frequency of the event. Permissible consequences are established according to the frequency of the event.

Putting regulation AR 3.1.3 Atucha2 NPP chose to provide a PSA level 2 as “backbone” of its safety case. However, since the regulation AR 3.1.3 requires fulfilling acceptance criteria based on dose and not on releases, dispersion calculations have to be made. Atucha2 decided to roughly follow relevant USNRC regulatory guides to evaluate the dose rate to the critical group.

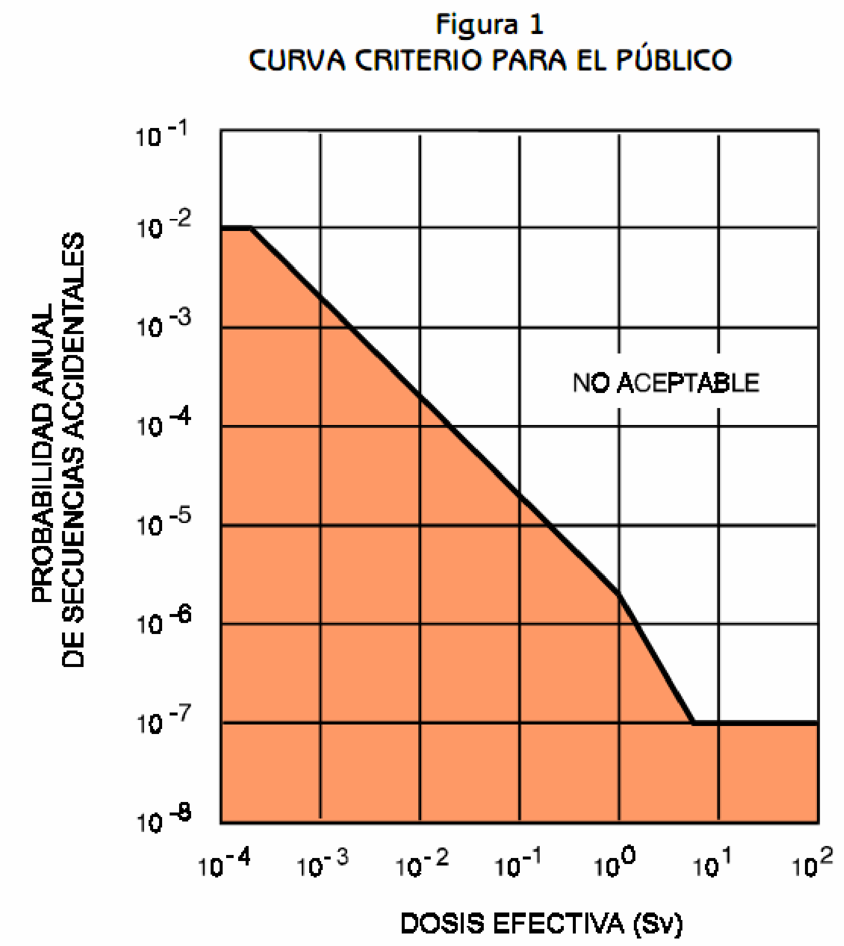

Figure A3.1, Permissible effective dose to a "critical group", depending on the probability of the group of postulated events (from regulatory standard AR 3.1.3, "Radiological criteria relating to accidents in nuclear power plants").

A3.2 Borssele (NL)

The single nuclear power plant in the Netherlands is Borssele (KCB, 480 MWe, started commercial operation 1973) has been active in PSA for many years.

PSA helped to execute and optimise the big modernisation effort of the years 1990 - 1997, when the plant, built to rules and regulations of the 1970s, was brought in line with the actual regulations. E.g., systems were refurbished to include appropriate redundancy on the system level, and to include better spatial separation of safety systems. Main coolant lines were upgraded for 'break preclusion', which reduced the break probability. Lines that could not be qualified were equipped with pipe whip restraint (secondary system lines outside containment only). Improvements included also emergency power and ultimate heat sinks during external events. Seismic resistance was also investigated. A fire risk PSA was also executed.

At present, applications of the PSA include on-line inspection / maintenance / testing (i.e. during power operation). It also includes a risk monitor, which is helpful for shutdown planning. PSA has been used to develop and implement SAMG and is used for SAMG drills / exercises.

A3.3 New Reactor Designs

This section on new reactor designs was provided by the Chairman of the meeting, Mr George Vayssier, based on his experience with the review of these designs. All information provided in this section is in the public domain.

A3.3.1 AP 1000

#	Topic	DiD	Ref. in AP1000 SAR
1	ROAAM applied, combines probabilities of loads to arrive at a final load probability distribution for a given fission product boundary, from which the failure probability of the boundary is calculated. Methodology is used to assess mitigative techniques. If a low prob. failure of the FP boundary is obtained, the strategy is then considered as a successful strategy.[13]	4	19.39.2
2	Cavity flooding is done before the SAMGs are entered (at the end of AFR.C1)[14]	4	19.39.9
3	Seismic Margin Assessment (SMA) for seismic loads ~ 1,67 SSE[15]; identifies SSC important to seismic risk plant survives 0,5 g	4	19.55. 19.59.6.3
4	PRA techniques have been used since the beginning in an iterative process to optimize the AP600/AP1000 with respect to public safety. Each of these iterations has included: • Development of a PRA model • Use of the model to identify weaknesses • Quantification of PRA benefits of alternate designs and operational strategies • Adoption of selected design and operational improvements.	All	19.59.2

[13] Risk Oriented Accident Analysis Methodology. Simplified interpretation; refer to work by Prof. Theofanous for proper interpretation.

[14] This is the equivalent of the FR.C1-procedure of 'classic' Westinghouse plants, which is an ultimate cooling procedure in the EOPs.

[15] SSE = safe shutdown earthquake

#	Topic	DiD	Ref. in AP1000 SAR
5	Use of PSA in design process, see list of items in this section, CDF ~ 2.4E-07, LERF ~ 1.95E-08 • high level of redundancy and diversity in passive systems • less dependent on non-safety systems • non-safety support systems have limited role in plant safety • less dependent on human actions, meets NRC safety goals even w/o human actions • more robust success criteria than current PSAs • no RCP seal leakage to be assumed due to canned RCPs • fully automatic depressurisation systems (but spurious actuation is large CDF contributor, sec. 19.59.3.1). Note: this systems replaces manual feed and bleed • LOOP less relevant due to passive systems • no RPV penetrations • no ex-vessel corium due to RPV external cooling, no MCCI • fully passive containment cooling, hence no risk for overpressure • low probability for spreading of fires and internal floods • automatic switch from injection to recirculation • various benefits during shutdown mode • fire protection devices	1-4	19.59.1 19.59.3. 19.59.5.3 19.59.6.2
6	Redefinition of break sizes (LBLOCA, MBLOCA, SBLOCA LBLOCA is >9 inch, incl. RPV rupture 9 < MBLOCA < 2 inch 2 < SBLOCA < 3/8 inch 3/8 < reactor leaks < 0 inch	3	19.59.3
7	Common cause failures from PSA: • software in the protection and safety monitoring system and plant control system, • logic board failures of the protection and safety monitoring system; • failures of transmitters used in the protection and safety monitoring system; • failures of reactor trip breakers; • plugging of containment sump recirculation screens; • failures of in-containment refuelling water storage tank • gravity injection line check valves and squib valves; • plugging of strainers in the in-containment refuelling water storage tank; • failures of fourth-stage automatic depressurization system squib • valves, and • failures of output cards for the protection and safety monitoring system.	1-4	19.59.3.5
8	HRA: 10 actions with importance > 1% no action results in decrease of CDF > 3% if assumed successful only 7 actions have importance 100 % (-> core damage) perfection of human actions not relevant for risk (most important: actions on SGTR)	3, 4	19.59.3.6

#	Topic	DiD	Ref. in AP1000 SAR
9	Check valve reliability is not relevant for risk	3,4	19.59.3.8
10	Overview of all PSA insights for AP1000	all	Table 19.59.18 (24 pages)
11	Consideration of Severe Accidents Mitigation Design Alternatives (SAMDA's)	4	

A3.3.2 EPR

#	Topic	Reference SAR
1	By use of Probabilistic Safety Analyses (PSA) at the concept design phase to confirm the design approach and identify the multiple failure sequences that should be considered in the design basis, so as to prevent core meltdown accidents. Within this framework, an overall core meltdown frequency of 10-5 per annum per unit is set as a design objective, taking into account all types of failures and hazards.	Vol. II, subchapter C.1
2	The purpose of using probabilistic assessment is to give reasonable confidence that the design complies with the general safety objectives. To reach this overall safety level, probabilistic considerations are used: • to give assistance to plant designers for system comparison and optimisation, • to extend the deterministic design basis (RRC-A sequences) in order to achieve a balanced design, ensuring that there are no 'cliff edge' effects and to reduce risks to an acceptable level considering preventive and mitigation measures, • to justify the preventive maintenance schedule, • to verify the analysis of severe accidents, • to confirm the appropriateness of protection of the plant against certain internal and external hazards, • to assess the improvement in the safety level in comparison with existing reactors. • includes fire PSA (subchapter R.4)	Vol II, subchapter R.0, R.4

A3.3.3. ESBWR

	• Identify and address potential design and operational vulnerabilities. • Reduce or eliminate known weaknesses of existing operating plants that are applicable to the new design, by introducing appropriate features and requires. • Identify risk-informed safety insights based on systematic evaluations of the risks associated with the design. • Develop an in-depth understanding of the design's robustness and tolerance of severe accidents initiated by either internal or external events. • Develop an appreciation of the risk-significance of specific human errors associated with the design, and characterize the significant human errors in preparation for better training and more refined procedures. • Identify and support the development of design requirements, such as inspections, tests, analyses, and acceptance criteria (ITAACs), reliability assurance program (RAP), technical specifications (TS), and COL action items and interface requirements. • Support the process used to determine whether regulatory treatment of non-safety systems (RTNSS) is necessary, if applicable. • Determine whether the plant design, including the impact of site-specific characteristics, represents a reduction in risk compared to existing operating plant designs	Ch. 19, Part 1

<u>A3.3.4. ACR 1000</u>

The PSA will also be used to provide safety design assistance through engineering feedback to the process designers at an early stage so that changes can be made before construction. Ref. PSA-1 submission to UK HSE, sec. 1.4.1

A3.4 Laguna Verde NPP

The following is a deterministic + probabilistic change to the Technical Operation Specifications (TOS) of Laguna Verde that Mexican Regulatory Commission made to test the methodology to evaluate TOS changes.

The change was requested for the TOS 3/4.3.2 "Instrumentation Performance for Isolation". The government utility CFE proposes a change in the allowed time out of service (ATO) from one hour to seven days, of the differential temperature channels (ΔT) of the insulation instrumentation. This arguing that events in which ΔT failure is caused by the unavailability of the ventilation system of the reactor building "Heating, Ventilation and Air Conditioning" (HVAC), the time allowed out of 1 hour is insufficient for the recovery of HVAC and at the same time causes the insulation systems Reactor Core Isolation Cooling (RCIC), Reactor Water Clean-Up (RWCU) and also the Reactor Heat Removal (RHR), by action of the TOS by not restoring the availability of the instrument within the time allowed for 1 hour.

During the evaluation both aspects were analyzed deterministic and also performed a calculation of the increased risk. The plant operational experience indicates that the ATO of 1hr, has been insufficient to maintain the HVAC and leads to entry into the action of TOS

3/4.3.2, which has been identified that results in a sharp increase in risk, given the isolation of the systems RCIC / RWCU / RHR.

For its part, the change request proposes a change in the ATO of 1hr to 7days, which meets the proficiency required to provide timely maintenance to HVAC and meets the criteria for acceptance of increased risk of Guide. In addition, it also proposes new controls on the HVAC, which is expected result in better performance of it and in a decreased rate of entry to the TOS action at issue.

Therefore, based on a comprehensive making decisions ruled that the change would be acceptable in the ATO from 1 hour to 7 days, as long as they replace the action of the TOS indicating to put the unit in shutdown. This would meet the maintenance requirements, better control and performance of the HVAC plant and carry a lower risk settings without having to go first to a higher risk, in cases where HVAC return is not reached and therefore the ΔT, as exhaustion of the new off-duty time allowed. It should also be included as part of the change compensatory measures that have emerged from internal operational experience to ensure temperature control in the precincts affected by the unavailability of HVAC.

Nevertheless, this example was not put in practice in the LVNPP because several people from the Nuclear Safety Division request a complete change of the HVAC system instead of modification in TOS.

A3.5 Cernavoda NPP

i) Outage interval extension: was done based on the fact that the results of PSA identified large safety margins coming from the deterministic analysis and the sensitivity case performed on the PSA model concluded that the risk increase is not unacceptably high. In order to comply also with the deterministic analysis and with the requirements on special safety systems reliability, some of the preventive maintenance and tests where moved from the outage to on-line operation. The result was that the outage, previously approx. 27 days each year, at the present is approx. 44 days each two years.
Outage planning: it is done base on the design documentation and the designer specifications and the plan is then verified with EOOS risk monitor to obtain the risk profile and to demonstrate that the risk will not exceed the acceptable limits. If the risk profile shows areas of unacceptable risk the outage plane is modified by rearranging the maintenance and testing activities in a way that maintains the risk at acceptable level in all plant configurations.

ii) Plant safety related modifications: in each case when the plant applies for approval of a modification on a safety significant system the application shall contain the deterministic and probabilistic evaluation of the impact it produces on the plant safety.

iii) Temporary changes of plant configuration: temporary deviation of plant configurations from provisions in OLC has been accepted provided that the operational risk of the plant did not exceed the acceptable limits.

LIST OF PARTICIPANTS AT THE TECHNICAL MEETING

1	**IAEA**	Mr Milorad Dusic IAEA, Department of Nuclear Safety and Security Division of Nuclear Installation Safety - Safety Assessment Section Wagramer strasse 5 P.O. Box 100 1400 Vienna, AUSTRIA Tel.: 0043 1 2600 22522 Fax: 0043 1 26007 EMail: m.dusic@iaea.org Internet: http://www.iaea.org
2	**Canada**	Mr Vali Tavasoli Directorate of Assessment and Analysis Canadian Nuclear Safety Commission 280 Slater Street PO Box 1046, Station B Ottawa, ON Canada, K1P 5S9 Tel.: +1 613 996 0192 Fax: 1 613 995 5086 Email: Vali.Tavasoli@cnsc-ccsn.gc.ca
3	**China**	Mr Xuija Wang Shanghai Nuclear Engineering Research and Design Institute 29 Hongcao Road, Shanghai, CHINA Tel.: +86 021 64850220 20204 Fax: +86 021 64851074 Email: wangxj@snerdi.com.cn
4	**Croatia**	Mr Tomislav Bajs ENCONET d. o. o. Miramarska 20 10000 Zagreb, CROATIA Tel.: +385 1 6312399 Fax: +385 1 6312380 EMail: tomislav.bajs@enconet.hr
5	**Croatia**	Ms Ilijana Iveković ENCONET d. o. o. Miramarska 20 10000 Zagreb, CROATIA Tel.: +385 1 6312399 Fax: +385 1 6312380 EMail: ilijana.ivekovic@enconet.hr
6	**Czech Republic**	Mr Jaromir Machacek CEZ a. s. Jaderna elektrarna Temelin Utvar JB a HP – 500210 37305 Temelin, CZECH REPUBLIC Tel.: +420 381 10 3992 Fax: +420 381 10 2794 EMail: jaromir.machacek@cez.cz

7	**European Commission**	Mr Andrea Bucalossi Institute for energy, SPNR Unit Westerduinweg 3 PO box 2, 1755 ZG Petten THE NETHERLANDS Tel.: +31 224 56 5052 Fax: +31 224 56 5637 EMail: andrea.bucalossi@ec.europa.eu
8	**Italy**	Mr Carlo Parisi University of Pisa/San Piero a Grado Nuclear Research Group (GRNSPG) via Diotisalvi, 2 - c/o prof. D'Auria 56122 - Pisa - ITALY www.grnspg.ing.unipi.it Tel.: +39 050 2210 378 Fax: +39 050 2210 384 EMail: c.parisi@ ing.unipi.it
9	**Italy**	Mr Nikolaus Muellner University of Pisa/San Piero a Grado Nuclear Research Group (GRNSPG) via Diotisalvi, 2 - c/o prof. D'Auria 56122 - Pisa - ITALY www.grnspg.ing.unipi.it University of Natural Resources and Applied Life Sciences, Institute for Safety and Risk Research, Vienna Tel.: +39 050 2210 373 Fax: +39 050 2210 384 EMail: Nikolaus.muellner@univie.ac.at
10	**Korea, Republic of**	Mr Seok-jung Han Korea Atomic Energy Research Institute Daeduck-daero 1045 Yuseong, DAEJON REPUBLIC OF KOREA Tel.: +82 42 868 8714 Fax: +82 42 868 8256 EMail: hanseok@kaeri.re.kr
11	**Lithuania**	Mr Virginijus Vileiniskis Lithuanian Energy Institute Breslaujos 3 LT-44403 Kaunas LITHUANIA Tel.: +370 37 401928 Fax: +370 37 351271 EMail: virgis@mail.lei.lt
12	**India**	Mr Mahendra Prasad Atomic Energy Regulatory Board Room No. 670 Niyamak Bhavan-B Anushaktinagar Mumbai 400094

		INDIA Tel.: +91 022 25990470 Fax.: +91 022 2590494 EMail: mprasad@aerb.gov.in
13	**Mexico**	Mr Angel Bernardo Paz Garcia National Commission on Nuclear Safety and Safeguards (CNSNS) Col. Barragan 779 col. Narvarte Delegacion Benito Juarez MEXICO Tel.: +50 9532 00 ext 471 Fax: +50 9532 00 EMail: abpaz@cnsns.gob.mx
14	**Romania**	Mr Radian Marius Sanda CNCAN 4, Libertatii Bulevard P.O. Box 42-4 050706 Bucharest Sector 5 ROMANIA Tel.: +40741551152 Fax: +40213162754 EMail: radian.sanda@cncan.ro
15	**Slovakia**	Mr Michal.Vlčko Slovenske elektrarne, a.s. Mlynske nivy 47 82109 Bratislava Tel: +421 (2) 5866 3923 Fax: +421 (2) 32 408 099 EMail: michalvlcko@enel.com
16	**Slovenia**	Mr Andrej Prošek Jozef Stefan Institute Jamova cesta 39 1000 Ljubljana SLOVENIA Tel.: +386 1 5885358 Fax: +386 1 5885377 Email: andrej.prosek@ijs.si
17	**Slovenia**	Mr Marko Čepin Faculty of Electricl Engineering Tržaška 25 1000 Ljubljana SLOVENIA Tel.: +386 1 476 82 43 Fax: +386 1 476 82 89 Email: marko.cepin@fe.uni-lj.si
18	**Slovenia**	Mr Jože Špiler GEN energija Cesta 4. julija 42 8270 Krško SLOVENIA

		Tel.: +386 7 4901117 Fax: + 386 7 4901118 Email: Joze.spiler@gen-energija.si
	Slovenia	Ms Andreja Peršič Slovenian Nuclear Safety Administration Zelezna cesta 16 P.O. Box 5759, SI-1001 Ljubljana SLOVENIA Tel: +386 1 472 11 26 Fax: +386 1 472 11 99 Email: andreja.persic@gov.si
	Slovenia	Mr Leopold Vrankar Slovenian Nuclear Safety Administration Zelezna cesta 16 P.O. Box 5759, SI-1001 Ljubljana SLOVENIA Tel: +386 1 472 11 43 Fax: +386 1 472 11 99 Email: Leopold.vrankar@gov.si

Meeting Agenda

Monday, 7 June 2010

9.00-10.00
- Registration
- Opening of the Meeting (IAEA, NEA & EU)
- SNSA Organizational Matters
- IAEA Objectives of the Meeting
- Selection of the Chairman Adoption of the Agenda Introduction of the Participants

10.30 - 12.00 - National Presentations and Discussions
- Combining Probabilistic and Deterministic Safety Analyses in Option 4 from the IAEA Specific Safety Guide SSG-2 on Deterministic Safety Analysis for NPPs M. Dusic, IAEA
- Design assessment of a CAREM-like isolation condenser considering uncertainties M. Gimenez & F. Mezio, ARGENTINA

12.00 – 14.00 - Lunch Break

14.00 – 15.30 - National Presentations and Discussions (cont.)
- Best estimate analysis for LOCA X. Wang, P.R. of CHINA
- Precursor based PTS screening methodology of the EOP operator actions for PWR Plant, T. Bajs & I. Ivekovic, CROATIA

15.30 – 16.00 - Coffee Break

16.00 – 17.00 - National Presentations and Discussions (cont.)
- Application of advanced safety assessment methods in Romania R. Sanda, ROMANIA
- Application of the safety margins concept in the Russian regulatory practice A. Sinitsov, RUSSIAN FEDERATION
- Best estimate plus uncertainty applications in Ignalina NPP licensing process V. Vileiniskis, LITHUANIA

Tuesday, 8 June 2010

09.00 – 10.30 - National Presentations and Discussions (cont.)
- Integration of probabilistic safety assessment and deterministic safety analysis for improvement of human reliability analysis A. Prosek & M. Cepin, SLOVENIA
- Insights from best estimate safe analyses for a precise PSA modelling S. Han, REPUBLIC OF KOREA
- Analyses by 3D neutron kinetics coupled thermahydraulic code for the licensing process of Atucha-2 NPP, C. Parisi & F. D'Auria, ITALY

10.30 - 11.00 Coffee Break

11.00 - 12.00 National Presentations and Discussions (cont.)
- Application of Best Estimate plus Uncertainty Analysis in the Atucha-2 NPP Licensing Process A. Muellner, AUSTRIA
- EC-JRC- IE Activities in the area of Safety Analyses A. Bucalossi, EC

12.00 - 14.00 - Lunch Break

14.00 - 15.00 National Presentations and Discussions (cont.)

- Methodology for the assessment of confidence in safety margin for large break loss of coolant accident sequences M. Prasad, INDIA
- Analyses by 3D neutron kinetics coupled thermahydraulic code for the licensing process of Atucha-2 NPP, C. Parisi & F. D'Auria, ITALY

15.00 – 15.30 -Coffee Break

15.30 – 17.00 - Presentation of the Background Material M. Dusic, IAEA

- General Discussion on the draft Working Material Establishment for Working Groups (WGs) Discussion on Topics to be addressed by the WGs Proposal:
    - WG1 WG2 WG3
    - Application of Deterministic Safety Analyses (DSA)
    - Advanced Computational Tools
    - Integrated Approach - Relation of PSA and DSA

Wednesday, 9 June 2010

09.00 – 17.00 Work in Working Groups

Thursday, 10 June 2010

09.00 – 12.00 - Work in WGs

12.00 – 14.00 - Lunch Break

14.00 – 15.00 - Presentation of Results by WG Chairmen (plenary session)

- Discussion

15.00 – 17.00 - Continuation of work on WG reports for presentation in the plenary session

Friday, 11 June 2010

09.00 – 10.00 - Finalization of WG Reports for presentation in the plenary session

10.00 – 10.15 - Coffee break

10.15 – 12.00 - Presentation of the Final Report by WG Chairmen (plenary session)

- Final Report Consolidation Future Actions
- Conclusions and Recommendations Closure of the Meeting

European Commission

EUR 24648 EN – Joint Research Centre – Institute for Energy
Title: Application of Advanced Safety Methods - Conclusions of the IAEA OECD JRC joint Technical Meeting
Author(s): A. Bucalossi
Luxembourg: Publications Office of the European Union
2010– 37 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-18792-6
doi:10.2790/29775

Abstract

This publication presents the main results of the Technical Meeting on Application of Advanced Safety Methods (for licensing of Nuclear Power Plants) held on 7-11 June 2010 in Bled, Slovenia. It was organized with the cooperation of the International Atomic Energy Agency (IAEA) and with the Organization for Economic Co-operation and Development - Nuclear Energy Agency (OECD/NEA).

This meeting is part of a series organized by the three organizations and has the objective to provide a forum to exchange information regarding activity in the use of Advanced Safety Methods more specifically focussiong on deterministic Best Estimate plus Uncertainty (BEPU) methods both in the domains of research and relative to licensing and on Probabilistic Safety Analysis

The use of BEPU methods is possible today due to the increased knowledge in Thermal-hydraulic phenomena and high performance computational tools and allows a much clearer understanding of the available safety margin during Design Base Accidents. The results shows that the industry is in fact moving in this direction in order to be able to demonstrate compliance to safety limits after power uprates as the older conservative methods were shown to be too pessimistic.

The use of probabilistic and deterministic methods is today starting to be used for defence in depth concept and also more often in combination with Deterministic Safety Analysis.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

LD-NA-24648-EN-C

EUROPEAN COMMISSION

Publications Office

ISBN 978-92-79-18792-6

9 789279 187926