International Review of the Use and Development of PSA

J.-M. Lanore (IRSN, France)
P. Pyy (TVO, Finland)
N. Siu (NRC, USA)
A. Huerta (OECD)

To be presented at

ANS International Topical Meeting on
Probabilistic Safety Assessment and Analysis
(PSA 2008)

Knoxville, TN, USA
September 7-11, 2008

INTERNATIONAL REVIEW OF THE USE AND DEVELOPMENT OF PSA

Jeanne-Marie Lanore
Institute for Radiation Protection and Nuclear safety
BP17-92262-Fontenay-aux-Roses-Cedex-France
jeanne-marie.lanore@irsn.fr

Pekka Pyy
Teollisuuden Voima Oyj
Olkiluoto, 27160 Eurajoki, Finland
Pekka.Pyy@tvo.fi

Nathan Siu
US Nuclear Regulatory Commission
Washington, DC, 20555, USA
nos@nrc.gov

Alejandro Huerta
OECD NEA Nuclear Safety Division
Le Seine St-Germain, 12, Boulevard des Îles, 92130 Issy-les-Moulineaux
Alejandro Huerta@oecd.org

ABSTRACT

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 PSA understanding 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 a recent exchange have been compiled in a CSNI report entitled “The Use and Development of Probabilistic Safety Assessment.” Responses were received from 20 countries totalling several hundred pages of information.

The paper presents the main conclusions of the report, especially the common points as well as some outstanding specific points. The conclusions underline in particular the growing role of PSA worldwide for improving nuclear power plant safety in a risk-informed approach, the high level of work on-going for developing, up-dating and improving PSA, and some tendency towards harmonisation.

Key Words: International overview – OECD/NEA – Harmonisation – PSA developments

1 INTRODUCTION

1.1 Background

The CSNI WGRISK produced a report in July 2002 on "The Use and Development of Probabilistic Safety Assessment in NEA Member Countries" [1]. This provided a description of the nuclear power plant PSA programmes in the member countries at the time that the report was produced. In 2005 the decision was taken to set a new task for up-dating this report, and a new version of the report was issued in 2007 [2]. This paper is a summary of the main findings of this task.

1.2 Objective

The aim of the updating task was to produce an updated, stand alone version of the report that presents an analysis of the position on the use and development of PSA in the WGRISK member countries as of spring 2006. The task was carried out in cooperation with the IAEA. This has led to more information and thus provided a better overview on PSA worldwide.

1.3 Process

A detailed questionnaire was circulated to WGRISK members and to the IAEA to ascertain the state of the art in PSA use and development at the end of 2006. Detailed responses were prepared by 20 countries totalling several hundred pages of information. The collected information was analyzed and summarized to reach the conclusions presented in the NEA/CSNI Report in addition to the detailed information.

2 PSA SITUATION IN THE RESPONDING COUNTRIES

2.1 PSA Framework and Environment

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

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

It is important to note that for new plants, particularly those of advanced design, most countries are formally requiring that a PSA be performed. The place of PSA is increasing.

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

Although there are differences in the regulatory systems, there are strong similarities in the use of PSA. This is because PSAs are performed in all countries as a part of safety analysis (with or without regulatory requirements), and because PSA is never used as the only basis for making a decision.

2.2 Numerical Safety Criteria

2.2.1. Status of the Numerical Safety Criteria

There are differences in the status of the numerical safety criteria that have been defined in different countries, reflecting differences in regulatory systems. Some have been defined in law and are mandatory, some have been defined by the regulatory authority (which is the case in the majority of countries where numerical safety criteria have been defined), some have been defined by an authoritative body such as a President's Commission and some have been defined by plant operators or designers.

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

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

2.2.2. Framework for Defining the Numerical Safety Criteria

In most of the countries in which numerical safety criteria have been defined, these have been defined as “targets”, “objectives” or “goals” where the recommendation is that the risk should be lower than the prescribed value with no guidance given on what specific action needs to be taken if it is exceeded.

As an example of a more comprehensive framework for managing the risk arising from a nuclear power plant (or any industrial activity), the UK identifies three levels of risk: an unacceptably high level of risk where operation of the plant would not normally be allowed; a very low level of risk which is broadly acceptable and below which the regulatory authority would not seek further improvements to be made to reduce the risk; and an intermediate level where the risk would need to be reduced to a level that was as low as reasonably practicable (ALARP).

2.2.3. Metrics for Defining the Numerical Safety Criteria

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

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

2.2.4. Way Forward

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

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

The work carried out so far has not addressed the rationale for the way that the criteria have been defined and the reasons for the differences. This is being addressed by a specific WGRISK Task Group. The current status of this work is described in[4].

2.3 PSA standards and guidance

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

As an example in the USA, PSA standards and guidance have been or are being developed and this activity is being supported by professional societies, the industry and the Regulatory Authority. Notable PSA Standards and Guidance include the following:

- Standard for Level 1 PSA (for core damage frequency) and limited Level 2 PSA (for large early release frequency) for full power operation that covers internal initiating events and internal flood [American Society of Mechanical Engineers (ASME)].
- Peer review guidance for the same scope of PSA as the ASME standard [Nuclear Energy Institute (NEI)].

- Standards for: external hazards, low power and shutdown modes, internal fires, Level 2 PSA and Level 3 PSA [American Nuclear Society (ANS)].

Several other countries (e.g., Japan, Canada, Switzerland, Korea, Germany, Netherlands, and Finland) have developed their own Standards and guides. Many of these are very detailed and complete.

In other Member Countries, no specific PSA standards or guidance have been developed. The position in these countries is that the methods used for the PSAs that have been carried out have been defined within these projects. The way that this has been done has taken account of international practices as defined in documents published by IAEA, NEA and NRC.

Another example, in France, is that the PSAs are carried out by two independent teams (at IRSN and EDF). A detailed mutual external review has led to important improvements in the quality of the PSA.

2.4 Status and scope of PSA programs

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

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

Nearly all the countries indicate that they intend to up-date their studies (living PSA). Many countries are also extending the scope of the existing PSA studies to Level 2, external hazards or Shutdown Situations.

It appears that the future “standard PSA” will be a living PSA including both Level 1 and Level 2, both full power and shutdown situations, and both internal and external initiating events.

2.5 PSA methodology and data

2.5.1 General methodology

The overall methodology described by all the countries is very consistent for Level 1 PSA but less for Level 2.

All the responding countries use the event tree/fault tree approach for the Level 1 PSA and an event tree approach for the Level 2 PSA. The methodology generally follows the approaches described by NRC or the procedures for carrying out Level 1, 2 and 3 PSAs defined by IAEA in the Safety Series documents and associated TECDOCs. In addition, it is recognised that the approach used for the PSA and the level of detail of the model need to be consistent with the proposed PSA applications.

In the Level 2 PSA, there is a wide variation in the number of Plant Damage States (PDS) defined, the number of attributes used to define the PDSs, the number and type of nodes in the Containment (Accident Progression) Event Trees and the number of Source Term/ Release Categories defined. However, all respondents report the use of event trees (small or large) to model the consequences of a severe accident.

2.5.3 Specific points

The Human Reliability Analysis (HRA) carried out as part of the PSA typically addresses: human errors leading to the unavailability of a standby safety system, human errors that can lead to an initiating event, and human errors of omission in responding to an initiating event that has occurred.

There are a number of methods used for the identification and quantification of human errors. These include the traditional methods such as the Technique for Human Error Rate Prediction (THERP) which is still widely used. In addition, other methods such as MERMOS and the Human Error Assessment and Reduction Technique (HEART)/ Nuclear Action Reliability Assessment (NARA) have been developed and are used in particular countries. All of the PSAs have included human errors of omission. Some of them have also included errors of commission or, in some cases, a partial analysis has been carried out. This is seen as a difficulty or limitation of many of the PSAs that have been produced.

In order to improve the knowledge about HRA, the WGRisk carried out several tasks during the past years. Recently, a WGRisk task group has drafted a report on the use of training simulators for collection of HRA data. This report will be issued in the near future[3].

Functional and physical dependencies are included explicitly in the PSA model. In addition, there are a number of methods of taking account of the residual dependencies (Common Cause Failures) not taken into account explicitly. These include the Multiple Greek Letter (MGL) approach, the alpha-factor approach, and the beta-factor approach with a number of variants.

Concerning data in general, the overall trend is to use plant specific data whenever possible and systems for plant data collection have been set up in many countries. However, some current PSAs use generic data, or generic data that has been supplemented by plant specific data for the risk significant initiating events or component failures.

For rare events for which an international data collection could be helpful, CSNI has set up several projects of data collection: ICDE (common cause failures), COMPSIS (digital systems failure), OPDE (pipe failures), and OCDE/FIRE (fire events).

2.6 PSA applications

A large number of applications are given by all the countries and these applications are very similar.

2.6.1 Design evaluation:

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

It is often the case that, during the lifetime of the plant, the scope of the PSA that is carried out has increased – for example the PSA has been extended to include external hazards, cover low power and shutdown conditions, and extend the analysis to a level 2 PSA. This identifies additional weaknesses that need to be addressed.

The PSA has also been used to compare the options for design changes to determine the relative reductions in risk that they would give. This is often done as part of a cost-benefit approach to determining what plant improvements should be made.

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

2.6.2 Accident management:

Often, a Level 2 PSA has been used to identify accident management measures that could be carried out to mitigate the effects of a severe accident. This has led to the incorporation of hardware in the plant (such as the catalytic hydrogen recombiners installed in the containment for all 7 nuclear power plants in Belgium) and the implementation of Severe Accident Management Guidelines to guide operators in the event of a severe accident. An example of this is the large programme of work carried out in Japan to produce Level 2 PSAs for each of the types of plant in the country and to incorporate plant specific hardware and guidelines in all the plants.

2.6.3 PSA-based event analysis:

The analysis of operating events using the PSA is carried out in many countries as part of the analysis of operating experience. The process usually involves a deterministic screening process to identify the significant events and the PSA is then used to determine the extent to which safety margins were reduced. This indicated the relative seriousness of the event.

2.6.4 Evaluation of Technical Specifications:

The Tech Specs define the Limiting Conditions for Operation (LCOs), the Allowed Outage Times (AOTs) and the Surveillance Test Intervals (STIs). In the past these have been based on deterministic considerations. In many countries the PSA has been used to justify and optimise the LCOs, AOTs and STIs.

PSAs that address both operation at power and low power and shutdown conditions have been used as part of the justification for moving some of the maintenance activities from being carried out during plant shutdown to being carried out during power operation.

PSAs have also been used to justify exemptions from Technical Specifications. An example of this arose at Borssele NPP when a reserve cooling water pump was found to be unavailable at a time when there was no spare at the plant. The PSA was used to show that the level of risk would be higher from shutting down the plant as was required by the Tech Specs than if the plant was allowed to continue operation at power.

2.6.5 Training of operators and plant staff:

The PSA is being used at a number of plants to provide input into the training programme of plant staff. The aim is to focus the training on risk significant systems/ structures/ components, accident scenarios, maintenance activities, etc.

2.6.6 Risk-Informed In-Service Inspection:

RI-ISI is being carried out for a number of plants. Both the Westinghouse and the EPRI methodologies are being applied.

2.6.7 Risk Monitors:

These are now in operation at a large number of plants and this is one of the widely accepted PSA applications. They are being used on a day to day basis in making decision on plant safety issues relating to maintenance activities

2.6.8 Risk informed treatment of structures, systems and components:

The PSA has been used, along with the deterministic insights, to identify the systems important to safety and these have been monitored using an enhanced surveillance programme. The same approach has also been used to identify the active components that need to be given special attention as part of the programme for the management of ageing.

2.6.9 Emergency planning:

The source terms and frequencies produced by the Level 2 PSA have been used as the basis for emergency planning. For example, the information from the Level 2 PSA for Borssele has been used to define the emergency planning zones for sheltering, the issue of stable iodine tablets and evacuation. In Switzerland, the results of the Level 2 PSA have been used to identify the reference scenarios for emergency planning.

2.6.10 Risk informed regulation:

The risk information provided by the PSA is increasingly being used by regulatory authorities in planning their activities. This includes: the prioritisation of inspection tasks so that they focus on risk significant issues, determining the significance of inspection findings, and developing the response to non-compliances. An example of this is in Mexico where plant specific Risk Inspection Guides have been developed.

A risk informed approach is used in a number of countries as an input to changing the regulations. In the USA, this approach has been used to change (or propose changes to) the regulations relating to: fire protection, combustible gas control, emergency core cooling system requirements and pressurised thermal shock.

2.7 Results and insights from the PSAs

2.7.1 Numerical results

Concerning the numerical values, the information given by the different countries is rather heterogeneous. In some cases a very complete presentation of results is provided, including relative contribution of the dominant initiating events. In several cases there is only a general indication about the fact that probabilistic objectives or orientations are met. Very often there also are some considerations about the fact that the risk is decreasing, due to safety improvements.

In fact the numerical results give only limited information and the problem with absolute values is well summarized in the USA contribution:

"It should be emphasized that comparisons of PSA results should be made with great caution. The PSA results are dependent on design- and operations-specific details, and on modeling approaches and assumptions. (Variations in modeling can be due to a number of reasons, including differences in the purpose of the PSA, associated differences in the PSA scope and level of detail, and differences in the level of maturity of the state-of-the-art for analyzing different accident classes and contributors.) It can be seen that this caution applies to comparisons of results for a single plant over time, as well as to comparisons of results between plants. Contextual information regarding the dominant contributors to risk and the reasons for their dominance (including modeling approaches and key assumptions as well as physical factors) will enable the reader to better compare and contrast study results."

2.7.2 Dominant risk contributors:

Much more interesting insights are given by the relative contributions.
One fact is particularly outstanding: the high contribution of internal and external hazards. Some of the key contributors noted by respondents are as follows:

- Fire (e.g., USA, Finland, Hungary)
- Earthquake (e.g., Hungary, Switzerland)
- Flooding (Netherlands.)
- Harsh weather (Finland)
- Typhoon (Korea)

One reason for these high contributions is perhaps that several hazards were not covered by the first PSA versions, and safety improvements were implemented for the dominant internal initiators, while the introduction of hazards in the PSA led to identify new problems. This is illustrated by some examples of plant modifications due to the treatment of external hazards and leading to a lower contribution to the results. WGRisk has established a task group to examine non-seismic external events; the group's work is reported in a separate paper at this conference.

It has also to be noted that Low Power and Shutdown situations contribute significantly in several results. WGRisk has also established a task group in this area; the group is expected to complete its technical work in 2008.

2.8 Future development and research

2.8.1 Development for future PSA applications:

Several countries describe their activities aiming to improve risk-informed regulation and risk-informed decision making (USA, Canada, The Netherlands).

Other countries indicate more specific applications:

- Optimization of testing and maintenance (Hungary, Czech Republic, Taïwan),
- Precursor analysis (Germany, Czech Republic),
- Risk Monitors (Slovakia, Czech Republic).

In fact, many PSA developments are linked to PSA applications reported in section 2.6.

2.8.2 Research activities:

An interesting point is that an important number of research activities are in progress, relating to many different PSA aspects. The most commonly identified topics are as follows:

- HRA (USA, UK, Switzerland, Korea, Japan, Hungary, France, Czech Republic)
- Digital I&C (USA, Korea, Japan)
- Fire (USA, Mexico, Japan, Finland, Canada, Sweden)
- Earthquakes (Japan, Hungary)
- External Hazards (Mexico, Japan, Finland, Canada, Belgium)
- Level 2 PSA and severe accidents (UK; Slovakia, Korea, Japan, Hungary, France, Canada, Belgium, Sweden)
- Data and CCF (UK, Switzerland, Sweden, Japan, Hungary, Canada)
- Uncertainties (Korea, Canada)

Other development topics appear in country replies less frequently. Some examples are as follows:

- Ageing (Italy, France, Czech Republic, Canada)
- Level 3 (Japan)
- Dynamic PSA (Switzerland)
- Reliability of passive systems (Japan, Italy)
- PSA for Non-Reactor Facilities (Italy) and more specifically PSA for Spent Fuel Pools (Slovakia, France)
- Advanced Methods (USA, Korea)

Furthermore, work aimed at better presentation and communication of PSA contents and results has been (or is being) carried out in USA, Korea and Spain.

It is useful to note that recent WGRisk activities, completed or ongoing, address many of these areas. Regarding current work, in addition to the previously mentioned task groups on HRA and non-seismic external events, WGRisk has a task group working on digital I&C PSA. In addition, WGRisk will be initiating a new task group working on advanced reactor PSA and will be co-organizing a workshop on severe accident mitigation measures with the CSNI working group on the analysis and management of accidents (WGAMA).

In summary, it can be noted that although PSA methods and applications have made real progress during these last years a significant level of development is still in progress. This amount of research activity indicates that PSA results sufficiently useful to justify this amount of work.

3 CONCLUSIONS

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

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

- The role of PSA for safety analysis and safety improvement is increasing. In particular PSA is generally required and applied for all new nuclear power plants.

- Although differences are still identified, a general trend towards harmonisation appears, regarding methods and scope, as well as applications.

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

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

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

4 ACKNOWLEDGMENTS

The paper is based on the report of the NEA /WGRISK. The contribution of all participants in the task, especially Mr. J. Murphy and Dr. C. Shepherd for their important contribution to the synthesis of the responses are gratefully acknowledged.

5 REFERENCES

1. The Use and Development of Probabilistic Safety Assessment in NEA Member Countries, NEA/CSNI/R(2002)18
2. Use and Development of Probabilistic Safety Assessment, NEA/CSNI/R(2007)12
3. HRA Data and Recommended Actions to Support the Collection and Exchange of HRA Data, to be issued as NEA/CSNI report.
4. P. Hessel, “WGRisk Task on Safety Criteria” *PSAM 9*, Hong Kong, 18-23 May 2008.