XA9847823

PUTTING PSA TO WORK

R. GUBLER
R. Gubler Ingenieurbüro,
Zurich, Switzerland

A. GOMEZ-COBO
International Atomic Energy Agency,
Vienna

Abstract

The IAEA has, during the last three years, been working intensively on PSA applications. The draft TECDOC prepared during these activities, "PSA Applications" is summarized in this paper. Actual events at nuclear facilities provide an important basis to compare PSAs with reality. PSA based operational event analysis therefore can be used to evaluate the importance of operational events from a risk perspective but also can contribute to validating and enhancing PSAs and to continuously check whether or not the PSA models are adequate, appropriate and complete. The work of the IAEA in this area is therefore summarized as well. In a companion paper, titled "Towards a credible PSA fit for applications", two specific aspects regarding the quality of the PSA to be used are discussed in detail, namely the Living PSA concept, which ensures that the PSA reflects actual design and operational features and Quality Assurance for PSA.

1. INTRODUCTION

PSA analyzes the risk associated with operating the plant, either in terms of plant damage or radiation dose to the members of the public, using a logical and systematic approach that makes use of statistical data associated with performance of the equipment and plant personnel as a basis for the calculations. This in principle has the potential to produce an understanding of the inherent risk of operating the plant over a much wider range of conditions than the traditional deterministic methods which generally define what is considered to be a bounding set of fault conditions.

Therefore, PSA is considered a very powerful tool to support decision making, however PSA is not a panacea and it certainly cannot be used to answer everything or resolve every problem or issue that might appear at the plant. In addition, its weaknesses and limitations need to be acknowledged. An adequate understanding of the uncertainties associated with the PSA is necessary in order to support the PSA applications. This understanding is dependent on the sources of information used to develop the PSA model and the adequacy with which the information is documented. As the understanding of plant performance improves, and the weaknesses, limitations and technical difficulties associated with the PSA are progressively remedied the quality and usefulness of the PSA will increase.

The following sections present a discussion on current trends in PSA applications, followed by a summary of the work done at the IAEA in the area of PSA based evaluation of the significance of operational events. Actual events at nuclear facilities are an important base to compare PSAs with reality. Besides providing valuable insights regarding the implications of operational events, the approach contributes to validating and enhancing PSAs and to continuously check whether or not the PSA models are adequate, appropriate and complete.

2. PSA APPLICATIONS

2.1 Introduction

This Section presents a summary of the IAEA (draft) TECDOC on "PSA Applications".

PSA can be used to evaluate the risk significance of NPP design and operational features, to define a risk measure as the basis of prioritising the various items under review or for risk based ranking of plant components. Therefore, PSA can be used for the evaluation of possible changes in plant design and operational features and for the evaluation of NPP operational events. The necessity for having a tool able to address these evaluations in a comprehensive and systematic fashion is the rationale for establishing a PSA Applications Programme.

2.2 The use of risk monitors

A significant part of the PSA applications require the dynamic use of the PSA models, and near prompt knowledge of the actual risk caused by the actual situation at the plant. This requirement can be satisfied by using a special tool called Risk Monitor.

A Risk Monitor is "a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the risk monitor reflects the current plant configuration in terms of the known status of the various systems and/or components, e.g., whether there are any components out for maintenance or tests. The risk monitor model is based on, and is consistent with, the LPSA. It is updated[1] on the same frequency as the LPSA. The risk monitor is used by the plant operational staff in support of operational decisions."

The risk monitor is designed to show the current risk state based on the actual plant configuration and tests in progress at any given time. Its primary use therefore is to enable maintenance and test activities to be performed on a risk informed basis. This is done by either having a target, in some cases core damage probability (CDP) for any configuration in which the core damage frequency (CDF) is above a given threshold, or minimising the risk when such risk target or criteria does not exist.

2.3 Use of PSA to support NPP design

PSA has become an important tool in the nuclear power plant design process. The benefits from a plant-level engineering perspective and the quantitative insights from a comprehensive PSA are not available from consideration of only a limited set of design basis accidents and application of traditional deterministic design criteria for individual safety functions, systems, and components. Therefore, PSA is now being used to supplement deterministic criteria and analyses in the design process for new reactors.

Early in the design process, preliminary PSA models are used as an internal analysis tool. The PSA models and analyses are refined and become more complete as the design matures. The final PSA may be submitted to the regulatory body as part of the supporting documentation for the plant design and licensing criteria.

---

[1] To update the risk monitor means, in this context, to revise the models and database as changes are made to plant design and operational features, as the level of understanding of the thermal-hydraulic performance or accident progression increases, or as improvements are made in modelling techniques. This update needs to be done with the same frequency and in a manner consistent with the update of the LPSA. Updating does not include reconfiguration of the risk monitor , which may be performed on a daily basis or as often as necessary to monitor the operational risk of the plant.

Another very important and widely spread PSA application is to identify potential safety improvements and to support the selection, design, installation, and licensing of operating nuclear power plant upgrades. The PSA is an important framework for these analyses because it is the only available method to consistently account for all intersystem dependencies. The importance of these dependencies may be ignored or underestimated when decisions are based on only a deterministic safety approach.

2.4 Use of PSA to support NPP operation

PSA modelling techniques for assessing plant safety and measuring risk are effective tools for evaluating maintenance activities to assure that the risk significant systems and equipment are being maintained, and to assure that maintenance activities do not reduce plant safety and increase risk by, for example extensive maintenance resulting in increased equipment unavailability, or occurrence of high risk configurations during maintenance.

In this context the most significant PSA applications are the following:

- Use of PSA to support maintenance planning
- Use of PSA to support reliability centered maintenance programmes
- Risk-based in-service testing
- Risk-based in-service inspection
- Use of PSA in connection with NPP technical specifications: modifications to AOTs and STIs and exemptions to technical specifications
- Risk-based configuration control

Other PSA applications to support various aspects of NPP operation are:

- Risk-based safety indicators
- Use of PSA to evaluate safety issues
- Use of PSA to support NPP periodic safety review
- Graded QA
- PSA based evaluation and rating of operational events

Utilities and regulators world-wide acknowledge the benefit of using PSA for event evaluation. The reason is that PSA not only provides a sound basis for analyzing the significance of many operational events, but also the use of PSA for event evaluation allows for the PSA to be backfitted based on real plant occurrences, and systems and operator real response to events. This makes the PSA more realistic, more credible and therefore more suitable for further applications. A description of the process for PSA based event evaluation is presented in Section 3.

2.5 Use of PSA to support incident and accident mitigation and management

With the advent of improved understanding and increased characterization of severe accidents, accident management can be analyzed in an integrated process and the interrelationships of Emergency Operating procedures (EOPs), Severe Accident Management Guidelines (SAMG), and off-site actions can be planned and organized to minimize the possible consequences of severe accidents, considered over the whole spectrum of their possibilities and probabilities, within the limits of practicality.

The improved understanding comes from research and development activities in severe accident phenomenology and the application of the results of these to analysis of the realistic accident progressions. The increased characterization in modelling and probability comes from the plant-specific nature of modern PSAs, the inclusion of all internal and external events for various

operating and shutdown modes, and the comprehensive analyses of these accidents scenarios through PSA Levels 2 and 3. Deterministic calculations of the effects of system operations in accidents are enhanced by the augmented description of boundary conditions and integral plant responses that can be derived from PSA analyses.

In this context the most significant PSA applications are the following:

- Use of PSA to improve emergency operating procedures (EOPs)
- Use of PSA to support NPP accident management
- Use of PSA to support NPP emergency planning
- Use of PSA to improve operator training programmes

2.6 Use of PSA in the regulatory framework

The deterministic regulatory process does not explicitly account for the probability of an event occurring. Yet, probabilistic reasoning was always implicitly utilized. Therefore, a blend of deterministic and probabilistic philosophy has always guided the development of the nuclear regulatory process. However, as the knowledge-base matures, the overwhelming reliance on the deterministic regulatory process may not necessarily ensure the most suitable approach to obtain adequate protection of public health and safety. Using probabilistic techniques, it can be shown that some deterministic criteria do not lead to design and operational practices that are optimal. This has the ramification of seriously overlooking potentially significant safety measures, due to regulations that are exclusively based on deterministic criteria. Thus, PSA has become a tool also to be used in the regulatory framework leading to the concept of risk-informed regulation.

Risk-informed regulation involves the whole area from implicit probabilistic considerations in the traditional deterministic requirements to an intensive use of probabilistic safety and risk analysis results in optimisation of regulatory attention, enforcement of regulatory requirements, and for more efficient utilisation of resources to enhance safety improvements by licensees. This might involve the formalised use of quantitative Probabilistic Safety Criteria (PSCs), or informal, qualitative measures.

The objectives of risk-informed regulations dictate that the regulatory attention be commensurate with the risk significance. Therefore, providing risk-based regulatory criteria are appropriately developed, a systematic and efficient expenditure of resources are to be expected, while, simultaneously, a balance in overall safety of nuclear power plant can be achieved.

However, in order to achieve an efficient risk-informed approach to regulation an adequate framework is required. This means that a formal process for decision-making needs to be implemented and procedures need to be established for changing already existing regulatory requirements based on new proposals that use probabilistic inputs. In addition, the regulatory authorities need to have dedicated staff with sufficient understanding of the PSA methodological framework. Therefore, the regulatory authorities are responsible for providing an adequate degree of training to their non-PSA staff members responsible for decision-making in order to have a common basis for communication, and understanding of the vulnerabilities and strengths of the probabilistic approach.

To fully implement and integrate the PSA process into the existing licensing and regulatory framework, the regulatory authorities are responsible for adequate proliferation of PSA technology, including exchange of experience and communication between the PSA specialists, the non-PSA engineers, and regulatory staff responsible for inspection and enforcement. This will reduce the potential for misunderstanding and resistance to change, and will focus attention more towards safety enhancement and efficient use of safety resources.

3. PSA BASED EVALUATION OF THE SIGNIFICANCE OF OPERATIONAL EVENTS

3.1 Introduction

During the seventies it was realized that the information contained in a PSA can be used for the analysis of operational events. The probabilistic models of the PSA constitute the information base to derive the scenarios for considering potential ways events could develop and implications of operational events. A special method was developed, widely named "precursor analysis" which is profitably applied in many member states to enhance plant safety and to improve PSAs. This section presents a summary of an appendix on "the use of PSA to evaluate the significance of operational events", which is part of the draft safety report on "Plant Review of Operational Safety Performance" (in preparation).

The use of PSA for the analysis of operational events serves two purposes:

1. it increases the understanding of the plant vulnerabilities given the event occurrence and provides the basis for effective experience feedback, and

2. the PSA model is continuously checked for appropriateness and completeness with respect to its ability to depict the operational events.

Actual events at nuclear facilities provide an important base to compare PSAs with reality. PSA based operational event analysis therefore can contribute to validating and enhancing PSAs and to continuously check whether or not the PSA models are adequate, appropriate and complete. The best basis for PSA based operational event analysis is a plant (or at least plant type) specific PSA which is maintained as a living PSA.

3.2 Purpose of PSA Based Operational Event Evaluation

The purpose of PSA based operational event evaluation is to characterize the relative risk importance of operational events for optimizing feedback of operating experience, to derive insights and to support the evaluation of plant specific design and operational problems as the events occur. Starting from an event at the plant, which could be an event which may initiate a plant trip or degrade or disable safety systems, or both simultaneously, the method gives an estimate, in terms of a conditional probability, of the margin which still separates the plant from an accident with unacceptable consequences.

Thus, the basic purpose of PSA based operational event analysis is to find answers to the following questions:

- How could an operational event have degenerated into an accident with more serious consequences?

- Can we determine a measure for what separates an operational event from a potential accident with more serious consequences?

Special weight is given to experience feedback: by extrapolating operational events to accident scenarios with serious consequences, valuable insights can be gained on accidents on the basis of minor incidents, without suffering their real consequences. The method thus makes it possible to learn from minor events before we must learn from real accidents.

3.3 Overall Approach

The overall approach of evaluating operational events involves the following steps:

- Initial screening of the operational event, whether or not the event is risk significant;
- understanding the operational event and its safety implications;
- Pre-selection of the operational event for further investigation;
- Relating the operational event to the reference PSA models and finding out whether or not the event can be adequately analyzed with the PSA models;
- Operational event analysis, mapping of the events on the PSA models, qualitative and quantitative evaluation, interpretation of results and derivation of insights.

In operational event analysis a re-analysis of the PSA needs be performed under the condition that the operational event has occurred. On this basis new conditional probabilities of accident sequences are calculated. If the calculated conditional probability of accident sequences leading to unacceptable consequences is larger than a given threshold value, then the operational event will be selected as an event which merits further consideration. A widely accepted threshold or cut-off value is 1E-6 for the conditional probability.

The PSA model used for operational event analysis should be sufficiently complete in scope to include the plant response to the operational event. It should include all relevant initiating events and all relevant operating conditions of the plant. Sometimes it is necessary to adapt or extend the models of the reference PSA due to the following reasons:

- Most reference PSAs only retain events and accident sequences that contribute in a non-negligible manner to the core damage frequency or other defined unacceptable consequences. Sometimes it is necessary to restore accident sequences that were eliminated or truncated out in the reference PSA.

- The level of detail of the PSA events and models is insufficient for directly depicting the operational event in the PSA. in this case additional considerations establishing the connection between the operational event and the PSA events and models are necessary.

- The PSA is incomplete or inadequate. This would also mean that the reference PSA should be revised.

Mapping of the operational event on the PSA is the most crucial step regarding the ability of the reference PSA. In order to relate the event to the PSA, the analyst determines which accident sequences are involved or could be involved, what fault tree models, basic events or operator actions are affected, and what recovery actions could be applied or are made impossible. In the mapping process the relation between the observed operational events with the events described in the PSA models is established. Basically there are the two following types of operational events:

- The event represents a transient which interrupts normal operation of the plant, thus there is a obvious effect on plant operation. In this case the event can be directly related to an initiating event of the PSA (if modelled) and the accident scenarios affected by the event are those developing from this initiating event.

- The event involves the unavailability or a degradation of equipment or systems without an immediate impact on plant operation. If the event is related to one (or several) safety functions, a systematic survey of the principal scenarios on which the event impacts needs to be done. First, all the initiators which require the affected safety function(s) need to be identified. In the event scenarios or sequences developing from these initiating events only the scenarios which entail the operational event are retained.

As part of the procedure of PSA based evaluation of operational events the scope of the evaluation can be extended by "what if" questions. What would happen if the event occurs under different conditions and context? This step allows to make maximum use of the information from the operational event. Again, the framework of the reference PSA can significantly support this type of question. An operational event occurs within a specific context and situation. The objective of this task is to ask the question what would happen if the event would occur under different conditions or in a different way. Typical parameters for which this question could be raised are the following:

- plant type
- initial condition of the plant
- chronology of events in the incident
- environment for common mode failures
- different human behaviour
- different context for human interactions.

Some operational events are not amenable to analysis or very difficult to model within the PSA framework. This involves such items as organizational problems, quality assurance programme deficiencies or degradation in design margins. Those operational events which cannot be analyzed reasonably should be identified and documented as potentially significant events which are impractical to analyze.

4. CURRENT TRENDS IN PSA APPLICATIONS

In order to compile state-of-the-art information on developments in PSA applications and tools, the IAEA convened a Technical Committee Meeting on PSA Applications to Improve NPP Safety in Madrid, Spain, from 23 to 27 February 1998. This meeting was organized by the IAEA in co-operation with the Spanish Nuclear Safety Council (CSN) and the Union of Spanish Electrical Utilities (UNESA).

Presentations and discussion during this TCM displayed the current trends in PSA and PSA applications. For example:

- It is generally accepted that Living PSAs are to be the basis for the risk based approach to decision making.
- The development and use of risk monitors as tools for configuration management is spreading fast.
- The use of PSA to support NPP test and maintenance is one of the most popular PSA applications. The idea of focusing maintenance efforts on the most safety significant components, systems and structures is very appealing to the nuclear community.
- Several organizations have established frameworks and procedures to use PSA to evaluate the importance of operational events from a risk perspective.
- Plant specific PSAs are being used to support the WWER safety upgrading programmes.
- Not all countries have a regulatory framework for the use of the probabilistic approach in decision making. Some countries are still far from the "risk-informed" regulation, and this means that there is still considerable work ahead, both for regulators and utilities to clarify approaches, to establish a framework and to reach a common understanding in relation to the use of PSA in decision making.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the participation of all the experts that contributed towards drafting and reviewing these two reports.

NEXT PAGE(S) left BLANK