IAEA-TECDOC-1200

Applications of probabilistic safety assessment (PSA) for nuclear power plants

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

February 2001

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

APPLICATIONS OF PROBABILISTIC SAFETY ASSESSMENT (PSA)
FOR NUCLEAR POWER PLANTS

IAEA, VIENNA, 2001
IAEA-TECDOC-1200
ISSN 1011–4289

Printed by the IAEA in Austria
February 2001

FOREWORD

Over the past years, many nuclear power plant (NPP) organizations have performed probabilistic safety assessments (PSAs) to identify and understand key plant vulnerabilities. As a result of the availability of these PSA studies, there is a desire to use them to enhance plant safety and to operate the plants in the most efficient manner practicable. PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit for plant safety can be obtained. However, any PSA which is to be used to support decision making at NPPs must have a credible and defensible basis. Therefore, it is very important that a 'Living PSA' be accepted by the plant and the regulator. Also, the establishment of an adequate and effective quality assurance framework is fundamental to any PSA project.

Recent IAEA activities on PSA have included the preparation of IAEA-TECDOC-1101, Framework for a Quality Assurance Programme for Probabilistic Safety Assessment; IAEA-TECDOC-1106, Living Probabilistic Safety Assessment (LPSA); and IAEA-TECDOC-1135 (jointly with OECD/NEA) on Regulatory Review of PSA Level 1. These publications are all aimed at improving the quality of the PSAs so that they can support decision making efficiently and reliably.

This report, which compiles information on a comprehensive set of PSA applications in the areas of NPP design, operation, and accident mitigation and management, is the culmination of an IAEA project on PSA Applications and Tools to Improve NPP Safety. In this regard, the Technical Committee meeting (TCM) held in Madrid in February 1998 allowed participants to review and provide very valuable comments for this report. Several important facts related to PSA and its applications were highlighted during this TCM:

- Living PSAs are the basis for the risk informed approach to decision making;
- Development and use of safety/risk monitors as tools for configuration management is spreading fast;
- The different uses of PSA to support NPP testing and maintenance planning and optimization are amongst the most widespread PSA applications;
- Plant specific PSAs are being used to support the safety upgrading programmes of plants built to earlier standards;
- Not all countries have a regulatory framework for the use of the probabilistic approach in decision making. Some countries are still far from '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.

The IAEA gratefully acknowledges the participation of all the experts who contributed to drafting and reviewing this report.

The IAEA officer responsible for this publication was A. Gómez Cobo of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

To date, probabilistic safety assessments (PSAs) have been performed for more than 200 nuclear power plants (NPPs) worldwide. Historically, PSAs have primarily been performed by regulatory bodies that have used them to gain generic risk insights (e.g. NUREG 1150 [1]), or by licensees, who have used them for a variety of purposes including compliance with regulatory requests to support a safety case, identification and understanding key plant vulnerabilities, and analysis of the impact of proposed design or operational changes. There have also been some instances where PSAs have been used to evaluate the design of new plants. Having invested considerable resources in developing PSAs, there is a desire on the part of both licensees and regulators to use the insights derived from them to enhance plant safety while operating the nuclear stations in the most efficient manner. PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit for plant safety can be obtained.

1.1. The role of PSA in NPP safety management

A nuclear power plant PSA analyses the risk associated with operating the plant, expressed in terms of various metrics related to the different levels of damage to the plant (e.g. core damage frequency), or its environment (e.g. societal or individual risk). The analysis is done using a logical and systematic approach that makes use of realistic assessments of the 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 assumed to be a bounding set of fault conditions. Furthermore, the adoption of conservative assumptions relating to plant and system performance is an accepted approach to addressing uncertainty when performing these deterministic analyses. The combination of considering a limited number of faults and a conservative approach to the analysis of each fault can produce inappropriate, or worse, misleading insights, and therefore decisions based on these types of analyses might not always be the most appropriate for reducing plant risk. By using PSA, which considers a much wider range of faults, takes an integrated look at the plant as a whole (system inter-dependencies), and uses realistic criteria for the performance of the plant and systems, more risk informed decisions can be made. The PSA, therefore, is a useful tool for safety management and its use can increase the level of safety by providing information not available from the evaluation of a limited set of design basis events.

However, while the PSA can be seen, in principle, to provide a broader perspective on safety issues than the deterministic approaches, the application of sound engineering principles has been demonstrably successful in achieving a high level of safety. Besides, while PSA is a very powerful tool to support decision making, its weaknesses and limitations need also to be acknowledged. Therefore, it is unlikely that PSA can be the sole decision making tool. Consequently, a consensus seems to be being reached that an integrated approach that uses deterministic engineering principles and probabilistic methods is the appropriate approach to decision making at nuclear power plants. For example, in its PRA Policy Statement, the US NRC stated "...PRA methods and data should be used in a manner that complements the US NRC's deterministic approach and supports the US NRC's traditional defence in depth philosophy". That is indicative of a trend towards a modern risk informed approach to safety regulation in which the PSA is used to provide one of the inputs to decisions concerning safety.

1.2. PSA in decision making

The extent to which PSA results can contribute to a decision depends on the level of detail of the PSA model, its quality, its completeness, and on whether the subject of the decision is amenable to analysis using a PSA. Therefore, when performing a PSA, it is very important to have an appreciation for what the PSA may be needed or intended for in order to define its requirements or to perform it in a way that allows it to be modified to support possible future applications. For certain specific and limited applications, a relatively simple PSA model may be adequate. However, for other applications, such as when a PSA is to be used as a day to day tool for decision making at NPPs, all aspects of the model are brought into play and a detailed, comprehensive model is necessary. 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.

Whatever the level of detail adopted, the model must reflect the current status of the plant. Therefore, if the PSA is to be of continuing use in the enhancement and understanding of plant safety, it must be updated or modified when necessary to reflect changes to the plant and its operating practices, and also to reflect improvements in methods. This has led to the concept of Living PSA (LPSA), [2]. Thus, a PSA used to support decision making must have a credible and defensible basis, and must reflect the design and operation of the plant. Also, it is very important that the PSA be accepted by the plant and the regulator. Therefore, all those facets of the PSA quality that are independent from the intended applications such as traceability, consistency, documentation, quality assurance, etc. are very important aspects that need to be considered when developing a PSA and afterwards when using it for different applications.

Although most of the applications discussed in this document can be performed before initiating changes at the plant, some applications require an on-line use. The appropriate tool for this application is called a safety/risk monitor. Section 2 presents a summary discussion on the LPSA and safety/risk monitor tools.

One criticism often levelled at PSAs which, for many people, limits their usefulness, is the uncertainty within the PSA community of how to address some of elements of the model. Typically, such uncertainties are addressed by making particular assumptions or adopting a specific model for an element of the PSA. The adoption of different assumptions and different models by different analysts leads to inconsistencies from PSA to PSA. A good example to illustrate this is the variety of approaches to human reliability analysis (HRA) and common cause failure (CCF) analysis. There are ongoing efforts to improve the accuracy and to standardize or at least harmonize PSA and PSA applications methods (e.g. Ref. [3]), however this is an issue not likely to be solved in the near future. However, rather than being an impediment to using PSA, this identification of uncertainties can be turned into a strength, by recognizing that an understanding of the impact of these uncertainties on the PSA results, obtained, for example, by performing sensitivity analyses, can lead to more robust decisions. This understanding is dependent on the sources of the information used to develop the PSA model and the adequacy with which the information is documented. Therefore, in order to achieve this goal, it is necessary that there exist a comprehensive documentation of the PSA, including an identification of the sources of uncertainty, and a specification of the underlying assumptions.

1.3. Outline of the report

This report is based on the premise that the use of PSA can provide useful information for the decision maker. This report is intended to provide an overview of current PSA applications.

Section 2 addresses the PSA application process, outlines the general requirements for PSA tools and provides a discussion on PSA aspects such as PSA level, scope and level of detail, which have to be considered when planning/performing PSA applications.

Section 3 discusses the technical aspects of individual applications and is divided into three parts. Section 3.1 is dedicated to the design related PSA applications. The second part of Section 3 considers the PSA applications that are related to the plant operations and the daily safety related activity of the plant personnel. Section 3.3 deals with PSA applications used to support the mitigation and management of incidents and accidental situations. Section 3 is not intended to be complete in its coverage of uses of PSA, but has focused on those applications that have been reported extensively in the literature. It is however, expected that future uses will probably be variants of the examples discussed in this part of the report.

Section 4 discusses the regulatory perspective on the use of PSA, and points out the main issues and regulatory concerns in the area of the PSA applications.

Section 5 discusses the establishment of numerical criteria for use in decision making using PSAs. Such criteria are likely to be different from country to country as they must relate to the regulatory framework adopted in each country. Therefore, the discussion concentrates on general issues, but gives specific examples to illustrate application of those principles.

2. THE BASIS FOR PSA APPLICATIONS

2.1. Introduction to PSA applications

PSA can be used to explore the risk significance of the various aspects of plant design or operation, to explore the risk impact of changes in plant design or operation, and for the evaluation of abnormal events that occur at the plant. In the following paragraphs the term *issue* is used to denote any plant design or operational feature, any proposed change of plant design or operational feature, and any plant events for which a PSA based evaluation is requested. The necessity for these evaluations is the rationale for establishing a PSA applications programme.

Any issue that is going to be evaluated needs to be explicitly defined together with the type of results required as input to the decision making. As already stated, as part of the evaluation, the PSA should be used in combination with other methods and sources of information. The PSA can be used to evaluate the risk significance of each issue, or to define a risk measure as the basis of prioritizing the various issues under review.

To use a PSA as part of the evaluation process, it is necessary to relate the issue to one or more specific elements of the PSA model [4]. If such a relationship cannot be found or the issue cannot be fully addressed by the existing PSA model, then it may be possible, in some cases, to modify the PSA or supplement it with new models or tasks. This, for instance, would

be the case when the PSA model needs to be expanded by including a new mode of operation, a new hazard event, etc. In all these cases, the relevant specific task procedures should be used in order to implement the necessary modifications, or, if necessary, new task procedures should be developed.

The evaluation of an issue may lead to changes in modelling assumptions, i.e. in the logic models and/or in the data. Changes in the logic models could result from one or more of the following:

- Change in assumptions leading to changes in the success criteria;
- Changes in system design;
- Changes in procedures;
- Changes in level of detail required in the fault trees, to incorporate a more detailed CCF model, for example;
- Changes in understanding of issues such as equipment qualification and their impact on component unavailabilities.

Changes in data will result from one of the following:

- New/modified generic data;
- New plant specific information;
- Changes in level of detail of the fault trees.

Once the PSA models and/or data have been modified as appropriate, the PSA model should be re-quantified and the results interpreted accordingly.

It may be that no changes to the model relating to the issue under consideration are identified. In this case the next step is to determine if it can be addressed by simply using the existing PSA results or by performing additional importance or sensitivity analyses.

Figure 1 outlines the PSA application process.

2.2. Tools

A Living PSA is the main tool required for performing PSA applications, ranging from simple applications, i.e. decisions based on the list of contributors to the plant risk, to applications requiring complex model and/or data manipulation. Some PSA applications require the on-line use of the PSA models, and near-prompt knowledge of the risk caused by the actual situation at the plant. This requirement can be satisfied by using a special tool called a safety/risk monitor. These two tools are discussed in the following sections.

2.2.1. Living PSA (LPSA)

This section presents a brief summary of the IAEA-TECDOC-1106 [2]. In addition to the topics discussed here, Ref. [2] also compiles information on the key aspects of the technical documentation for all the LPSA tasks and on state of the art and desirable features for the codes that support LPSA.

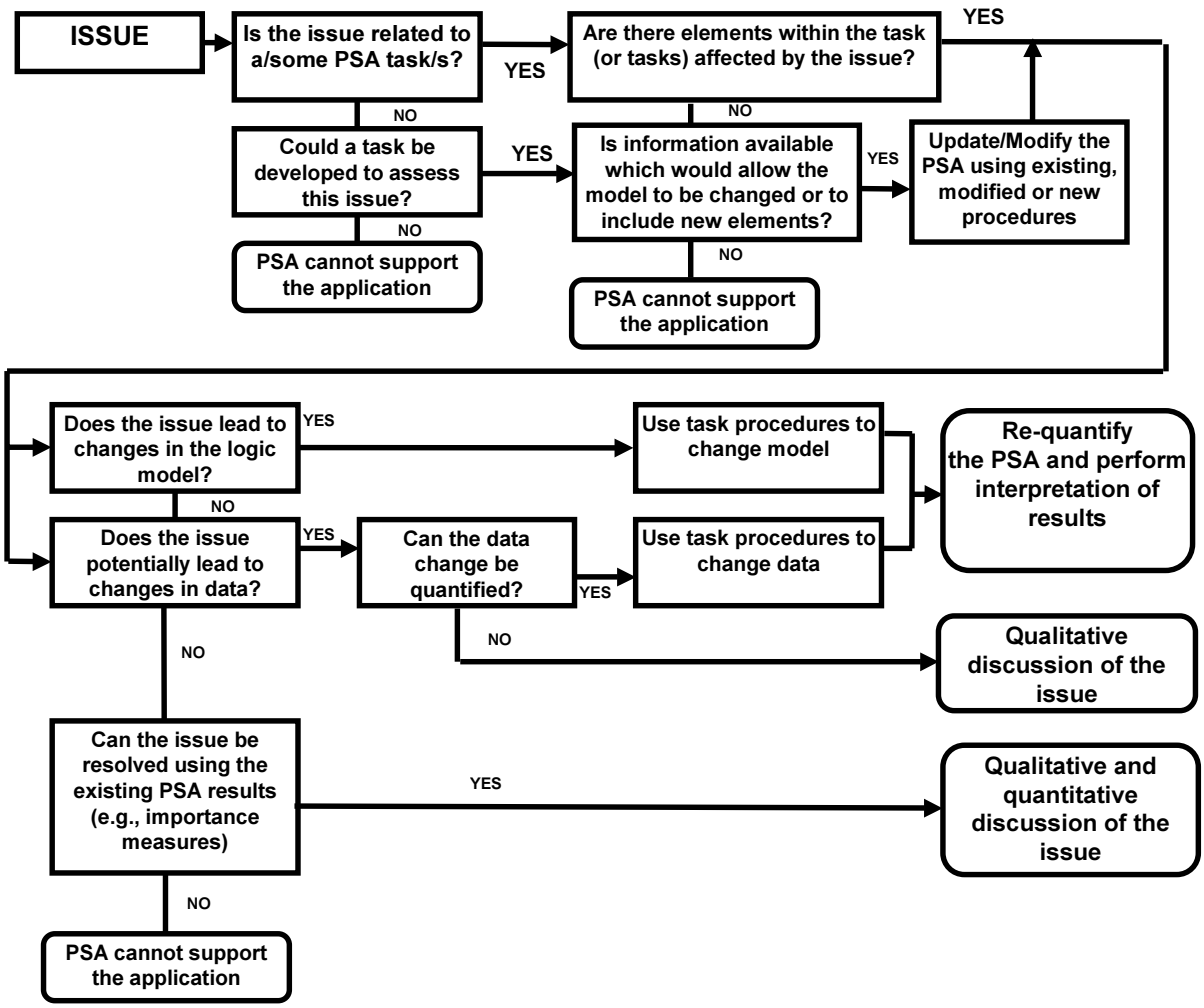

FIG. 1. PSA applications process.

Definition

A Living PSA (LPSA) can be defined as a PSA of the plant, which is updated as necessary to reflect the current design and operational features, and is documented in such a way that each aspect of the model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information. The LPSA would be used by designers, utility and regulatory personnel for a variety of purposes according to their needs, such as design verification, assessment of potential changes to the plant design or operation, design of training programmes and assessment of changes to the plant licensing basis.

General LPSA requirements

The above definition implies that, at the initiation of the LPSA project, the documentation associated with the work performed in each task and the project as a whole must be designed to meet two basic requirements:

- The basis for the LPSA model should be comprehensively documented so that each aspect of the model can be directly related to existing plant information or to the analysts' assumptions of how the plant and the operating staff behave.

- It must be possible to update the LPSA as changes are made to plant design and operation, feedback is obtained from internal and external operational experience, the understanding of thermal-hydraulic performance or accident progression is improved, and advances are made in modelling techniques.

Technical documentation

In order to meet the first requirement identified above, the LPSA should be accompanied by (i) a set of detailed individual Task Procedures (i.e. documents that give detailed guidance on how to perform the tasks, the techniques to be used and general assumptions to be made), (ii) Analysis Files for all PSA tasks, which compile reports, input data, relevant calculations, and model or database files containing task results, and (iii) a Document Data Base which cross references the input, output, and internal usage of the various documents used and produced during the development of the PSA.

LPSA updating

The LPSA should be *updated as frequently as necessary* to ensure that the model remains an accurate representation of the safety of the plant. However, continuous updating of the LPSA appears not to be practicable due to reasons such as control of changes, control of documentation and resources required.

It is necessary to assess the impact of any modification (design, procedures, operating practices, licensing basis, etc.) on the PSA in order to check its continuing validity and thus to identify any need for updating. Whilst it is likely that each modification will be assessed on a case by case basis, *it would be good practice not to accumulate a backlog of such assessments for a period longer than one year.*

Modifications that impact the PSA results may require an immediate updating of the LPSA. However, even if this type of modification does not arise for a longer period, *it is still suggested that the updating process be audited every three years and the LPSA formally amended at that time.*

Organizational aspects

An LPSA can only be developed and maintained successfully by a team of qualified analysts with the full support of the plant management and the involvement of different plant departments. The LPSA team composition and its interaction with other technical departments of the NPP is therefore a fundamental part of the success of the project. The quality of an LPSA is ensured if it is performed by a qualified team which has adequate resources, plant support and involvement, and strictly adheres to an appropriate QA framework.

Quality assurance (QA) for LPSA

The quality of the LPSA depends on a well developed and maintained QA programme that is effectively applied during all PSA phases. The success of developing an LPSA directly depends on the initial QA measures taken. Inadequate QA measures employed in the early stages of a PSA may lead to loss of information and may severely limit the usefulness of the PSA.

Changes in PSA models, data, information and results, including changes to requirements, scope and objectives and input data, should be made in a controlled manner. The reason for a change has to be documented and consideration needs to be given to the impact and implications of the change. When carrying out a change, in principle, the modifications should be handled in the same way as for carrying out the complete PSA (information control; configuration control; documentation control; Verification and validation; Review). This is a key point for the periodic updating of an LPSA.

IAEA-TECDOC-1101 [5] provides guidance for the development of a QA programme for PSA.

2.2.2. Safety/risk monitors

A safety/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 safety 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 of service for maintenance or tests. The safety monitor model is based on, and is consistent with, the LPSA. It is updated[1] with the same frequency as the LPSA. The safety monitor is used by the plant staff in support of operational decisions, [2].

For a risk monitoring tool to be efficient, the target solution time following changes in plant configuration needs to be in the range of 2 to 5 minutes.

Since actual plant operation is dynamic, the average annual risk may not ever be representative of the risk associated with the plant at any particular time during the year. The safety/risk monitor provides risk based input for plant configuration management, including the evaluation of equipment outages and the combined impacts from the actual plant configuration. This information is useful for maintenance prioritization and for the development of contingency plans during unexpected equipment failures. The safety/risk monitor may provide rapid insights about the potential significance of operational events and precursors, provided that these events are within the scope and limitations of the safety/risk monitor models and assumptions.

It is worthwhile to highlight the main differences between the plant LPSA and the safety/risk monitor.

The LPSA is a comprehensive model which provides a considerable amount of information on many aspects of plant design and operation. In its complete form, and for its solution, assumptions are made about maintenance and test activities over the year as well as the random occurrence of initiating events. Its primary use is to predict the core damage

[1] To update the safety/safety/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 updating needs to be done with the same frequency and in a manner consistent with the updating of the LPSA.

Updating does not include reconfiguration of the safety/safety/risk monitor, which may be performed on a daily basis or as often as necessary to monitor the operational risk of the plant.

frequency (CDF) over the life of the plant and enable the utility to have a risk perspective in the long term planning of design and operational changes.

The safety/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 CDF is above a given threshold, or minimizing the risk when such risk target or criteria do not exist.

Another important difference is that the LPSA, being handled by experienced PSA experts, uses basic events and the related PSA terminology, whereas the safety/risk monitors use components, systems and the related plant terminology. This is because the risk monitors are used at the plant by plant personnel communicating with the plant terminology. This difference is reflected also in the plant model and the calculating options of the safety/risk monitors.

The plant risk can be represented in a number of ways depending on how the safety/risk monitor model is developed. The response time is extremely important for the successful application, and therefore, given current software and hardware limitations, nowadays it is still necessary that the plant model be represented differently from the LPSA model. The commonly used modelling techniques are the following:

- Integrated core damage, core boiling, large early release fault tree
- Integrated core damage fault tree
- Dependency matrices (system/train status)
- Fault trees for specific initiators
- Pre-solved cut set solutions.

Each of the above will potentially give a different solution for a given plant configuration.

The type of risk model used in the various monitors available is determined by balancing four factors, namely, the size of PSA, the hardware on which the model is installed, the speed of fault tree algorithm and the required solution time. Although very early risk monitors use simplified fault trees, or just the minimal cut sets originated from the plant LPSA, it is acknowledged that a more accurate solution will be achieved from a fault tree model which is a Boolean minimization of the LPSA. Such a model needs to contain all the information contained in the LPSA. In fact, the modern risk monitors use different modelling techniques to accelerate the calculation process, and at the same time the model is no longer simpler then the plant LPSA model. In fact, while the plant PSAs usually represent an average plant configuration, initiating event frequency and human error probabilities, some safety/risk monitor models may even be more complex to be able to represent the exact plant configuration at any time and the impact of test and maintenance activities on the initiating event frequencies and operator performance.

Some of the requirements for the safety/risk monitor software are different from those for the LPSA software. The safety/risk monitor is required to operate in real time and follow the plant operating profile, including the test activities which are taking place, and in addition, it has to be made so that it can be used by non-PSA specialists. Often, existing PSA computer programs were not designed to support these requirements.

Suggested operational specifications for a modern safety/risk monitor are the following:

- Capability to analyse all modes of operation
- Capability to perform batch solution of schedules
- Automated data interface with schedule and plant process computers
- Capability to calculate large early release frequency (extended to Level 2 PSA)
- Capability to perform evaluations for fuel in RCS or spent fuel pool
- Capability to track and store risk history
- Capability to apply rule based recovery actions
- Capability to store unavailability data for designed components.

The functions of the safety/risk monitors among others include the following:

- Understandable, user friendly output available to plant staff
- Calculation of the current core damage frequency (usually expressed as annual CDF) and cumulative CDF
- Storage and presentation of past core damage frequency
- Giving recommendation on the time in a given configuration once a predefined core damage frequency is exceeded
- Importance ranking of currently available components
- Restoration advice
- Calculation of time to boiling
- Calculation of large early release frequency.

The safety/risk monitor is used for evaluating the effects of changes in system configuration (by providing advice on the priority of restoration of components), changes in component status due to maintenance or component failure, the tests in progress, making long term or short term maintenance schedules or planning refuelling outages and changes in environment external to the plant which may cause an initiating event. Most of these applications belong to the PSA application called risk based configuration control (see also Section 3.2.3).

A safety/risk monitor can be also used to derive a range of potential figures of merit for risk informed evaluations. The following are examples to be used for risk informed decision making:

- Annual CDP
- Peak CDF during the year
- Length of time in various CDF bands
- Length of time above PSA CDF
- Safety system (component) unavailability

- Total maintenance time for safety related components
- Activities which lead to peak CDF
- Activities contributing to time above PSA CDF.

Typical examples of safety/risk monitors being used in plant operation can be found in Refs [6–8].

2.3. Discussion on PSA level, scope and level of detail to support applications

The applications for which a PSA can be used are, to some extent, determined by its scope. The scope of PSA is characterized by the following:

- radioactivity sources considered (reactor core, refuelling pool, spent fuel handling facilities, waste storage tanks)
- initiating events treated, (internal events, internal hazards, external hazards)
- plant operational modes analysed (full power, low power, shutdown, startup, refuelling)
- levels of PSA included (1, 2, 3).

Even if the PSA does not address all the above aspects, it may still be used if the insights and conclusions are supplemented by information from other sources. The range of potential applications and the significance of the results of the PSA, however, increase considerably with increasing PSA scope. For example, a Level 1 PSA may be adequate to support decision making in areas relating to core damage frequency, but a Level 2 PSA would provide a more sound basis for the decision making process as it considers both core damage and off-site release. Also, a Level 2 PSA will allow the treatment of issues related to the containment and containment safeguards.

Another example is the development of non-full-power modes PSA. The availability of a Shutdown PSA (SPSA) enables risk to be evaluated over the full range of plant operations, and, for example, will enable the PSA to be used for applications which require comparison of risk at power vs. risk during shutdown. Also, it should be borne in mind that the risk significance of a component can be considerably different during power or shutdown and that, therefore, this has to be taken into consideration for PSA applications such as those based on distributing components into high/low risk significance categories.

In addition, the inclusion of external initiators (hazards) in the scope will further widen the basis for the decision making process and enable the results to be compared against “all sources” probabilistic safety criteria. Reference [9] underlines the importance of the completeness of the PSA.

It is also important to understand the implications of the internal structure of the PSA and if possible ensure that the structure meets the requirements of future applications. One example might be the selection of a single configuration for modelling purposes, versus a more detailed representation of operational status. Such a situation can arise when modelling a three loop PWR plant for which it is common practice to model one out of the three steam generators as the faulted loop. Due to this assumption the frequency of steam generator tube rupture in the assumed faulted generator is a factor of three higher than it should be, while in the remaining two generators there is no corresponding frequency. This results in a distortion

of the ranking of the component importance. It is necessary to be aware of this potential difficulty when performing applications of the PSA: the initial choice of modelling approach for the PSA may even have to be reconsidered.

In the following sections, the minimum scope for the applications is discussed only briefly. It should be emphasized that in most cases, if the scope of the PSA used for the application is broader, the decisions based on the PSA results will be more risk informed.

3. PSA APPLICATIONS

3.1. Use of PSA in design

3.1.1. Use of PSA to support NPP design

PSA has become an important tool in the nuclear power plant design process.

Uses, benefits and advantages

The main benefits of the use of PSA during the design process are:

- Identification and resolution of plant vulnerabilities
- Identification of important intersystem dependencies and potential CCFs
- Examination of risk benefits from different design options
- Identification of accident scenarios and operator actions with a high sensitivity to human error
- Balance between preventive and mitigative measures
- Optimization of systems and components for safety and availability
- Qualitative knowledge and understanding of the contribution of components and systems to accident sequences.

A PSA provides a fully integrated model of the entire plant that can be used to examine the risk from a variety of possible initiating events (e.g. transients, LOCAs, support system failures, etc.). The PSA consistently accounts for both the event frequency and the potential consequences from equipment failures or human errors. The model combines front-line safety systems and support systems in a manner that allows designers to identify the risk significance of important intersystem dependencies. The PSA allows designers to quantify the likelihood of "passive" and "active" failure modes, to examine the significance of single failures and multiple failures, and to determine the risk importance of "safety", "safety related" and "non-safety" systems. Consideration of only a limited set of design basis accidents and application of traditional deterministic design criteria for individual safety functions, systems, and components does not provide the same benefits as the combination of traditional approaches and PSA.

Examples and experience

In the past, the design of nuclear power plants was mainly based on deterministic methods. Boundary conditions for safety analysis, safety factors with regard to prevention and control of design basis accidents, and requirements for each safety function have been derived

from deterministic criteria without explicit consideration of the reliability of accident prevention and mitigation functions.

PSA is nowadays used to supplement deterministic criteria and analyses in the design process for new reactor concepts in the United States (e.g. AP-600 [10–12], ABWR), for the joint French–German project EPR [13, 14], for the European EP1000 [15], etc.

PSAs to support new designs are often performed by the reactor vendor and are based on a prototype of the plant design. Preliminary PSA models are used early in the design process 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 (see for example Ref. [12]).

In The Netherlands the development of a Level 3 PSA is required as part of the siting procedures. Should the construction of a new nuclear power plant be contemplated, first, a generic PSA would support the early stages of the siting and licensing. Finally, a full scope Level 3 PSA would be necessary to demonstrate that the combination of site and plant design fulfils the Dutch probabilistic safety criteria for the Netherlands.

Other examples are the use of PSA for the design and licensing of Heysham 2 and Sizewell B NPPs in the UK and ABWR in Taiwan (China), and to support the design of the KNGR (Korean next generation reactor) [16] and of the advanced WWER reactors in the Russian Federation [17],

Technical and methodological aspects

There are no special requirements for PSA methods or models for new plant designs. These will depend on the requirements of the licensing or regulatory body and could include evaluation of off-site dose to individuals, frequency of large early release or frequency of core damage.

It is recommended that the scope of analysis should include at least a limited-scope Level 2 PSA. The PSA should determine the frequency of different plant damage states that may occur and it should identify all important physical and functional dependencies that affect containment or confinement systems. This is likely to reduce the amount of work necessary for future PSA development to the point of off-site dose calculations. It would also allow for the PSA to be used for the evaluation of design issues related to containment safeguards.

Particular effort should be made to identify unique initiating events, failure modes, event sequences and dependencies that may be introduced by new design features. Detailed dependency matrices should be developed to identify and document all physical and functional dependencies among support systems and front-line systems. All normally operating systems should be examined to identify possible initiating events that may be caused by loss of the entire system, of a single system train, or of combinations of trains. Event sequence diagrams may be used to develop the accident sequences and identify challenges to relief and safety systems in the period immediately following the initiating fault. This is particularly important in a realistic analysis where the identification of bounding faults is of concern.

Thermal-hydraulic analyses, bounding calculations, and engineering judgement may be required to determine realistic success criteria for certain systems and functions. Typical

examples include injection requirements for various LOCAs, flow requirements for cooling water systems, and ventilation or room cooling requirements. Lack of final detailed design analyses should not be used as a basis for postponement of a PSA evaluation or for omission of specific systems or functions from the PSA models.

The PSA analyses should be based on the best available data for the types of equipment and systems in the plant. In some cases, very limited data may be available for evolutionary designs or new equipment, especially in the case of passive systems. In these cases, data for similar components or documented expert judgement should be used to estimate failure rates, maintenance unavailabilities, CCF parameters, etc. The absence of documented component specific reliability data should not be used as a basis for postponement of a PSA evaluation or for omission of specific component failure modes from the PSA models. The models and analyses should be updated as more information, experience and data become available for the new equipment.

Precautions and limitations

Deterministic methods continue to be very effective to ensure safe plant designs. PSA should be used to complement, enhance, and validate conclusions that are based on well-established deterministic design principles. The most important benefits from PSA are the added perspectives that are provided by an integrated risk model for the entire plant and a consistent evaluation of both the frequency and consequences of possible accident scenarios. The PSA can actually be used to determine what events (from the frequency perspective) should fall within the Limiting Design Basis Faults for which thermal-hydraulic analysis is required.

Some PSAs for new plant designs have included only models for front-line safety systems that are supplied by the reactor vendor. Experience from PSAs of operating plants typically shows that support system failures and intersystem dependencies are extremely important contributors to overall plant risk. Therefore, it is recommended that PSAs should also include a detailed treatment of support systems and balance-of-plant systems that are designed and supplied by firms other than the reactor vendor. This effort requires early collaboration between the reactor vendor and other members of the design team. Substantial engineering judgement may also be required to develop models for systems that are in preliminary design. However, it is important that the PSA evaluate the entire plant design as it will be constructed and operated.

It is recommended that the PSA include failure modes of both “active” and “passive” components for all systems, particularly if it is found that testing does not demonstrate the successful operation of passive components. Considerable experience and engineering judgement are also required to determine which existing data are most applicable to the new systems or which generic databases or models provide the best information for a new design. Sensitivity analyses of the results will show the importance of such judgements for the assessed safety of the plant.

Advanced plant designs rely on increased use of software based systems for instrumentation and control, plant protection, and operator interfaces. There is currently very limited experience in the development and application of PSA methods to analyse complex software based logic. Therefore, current PSA methods have limited capability to estimate the actual reliability and risk contributions from these systems. However, in some cases, it is

possible to use bounding analyses and sensitivity studies to estimate the possible risk significance from postulated software errors.

The PSA for a new plant design may contain substantial uncertainties. These uncertainties stem from incomplete design information, preliminary thermal-hydraulic analyses, limited directly applicable data, reliance on preliminary procedures, engineering judgement, etc. In some cases, the uncertainties may contribute significantly to the preliminary PSA results. Additional supporting analyses or data may be required to reduce the uncertainty for certain cases. Either way, it is important that the sources of uncertainty in the analysis be identified and their potential impact on the results of the PSA understood. This understanding may be achieved using a variety of analytical tools, including the characterization and propagation of parameter value uncertainty, the use of bounding analyses, and the performance of well chosen sensitivity studies.

3.1.2. Use of PSA to support NPP upgrade and backfitting activities and plant modifications

One of the most important applications for PSAs of operating nuclear power plants is to identify potential safety improvements and to support the selection, design, installation, and licensing of plant upgrades (e.g. owing to changes in licensing criteria).

Uses, benefits and advantages

One of the major goals of PSA is to assess the level of safety of existing plants and to identify potential design weaknesses which may result in proposed plant improvements (backfits). If the frequency of core damage or severe off-site releases is largely dominated by a very limited number of accident sequences, effective backfits may be proposed to prevent or to mitigate these scenarios. Backfits may also be suggested if PSA results show that a plant does not meet recommended or established national or international probabilistic safety criteria.

Proposed backfits may involve changes to system designs and installation of new hardware. They may also involve changes to operational procedures, development of specific accident management procedures, or changes in operator training. The latter aspects are discussed in Section 3.3.

The results from a PSA often clearly identify specific functions, systems, and operator actions that should be improved to reduce overall plant risk. A plant specific PSA is an extremely valuable tool to examine each proposed measure, to assess benefits and weaknesses, and to provide inputs to cost-benefit analyses. The net safety benefits of several options can be evaluated individually and in combination to determine the most effective solution.

A complete evaluation that includes deterministic analyses and a PSA is necessary to evaluate proposed modifications that arise from a utility's desire to enhance plant safety and to achieve better cost efficiency and improved operating efficiency. System-level analyses and full-scope PSA evaluations can be used to demonstrate which modifications are acceptable and to compare or suggest possible alternatives. 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 only on a deterministic safety approach. PSA provides a common basis for understanding

the contributors to risk and qualitative and quantitative information to support discussions between the plant operator and regulatory authorities.

Examples and experience

PSA evaluations are usually performed by the utility and are reviewed by the regulators as part of the modification approval process. In many cases, comparative PSA evaluations are also used to prioritize proposed improvement options during working discussions between the plant operator and the regulatory authorities.

Some examples of these applications were presented at the IAEA Technical Committee Meeting in Madrid, Spain (1998) on PSA Applications and Tools to Improve NPP Safety [18, 19].

Some plants in Spain have used PSA as an input to the study of compliance with the Appendix R of 10CFR50 and the consequential plant upgrading related to fire safety. See, for example, Ref. [20] and papers by Morales et al. and Suarez included in IAEA-TECDOC-873 [7].

The PSA reference studies in Germany have triggered upgrading and backfitting activities to improve NPP safety design. Level 1+ PSAs are being performed for all nuclear power plants in operation in the framework of the periodic safety review (PSR). Regulatory guides have been developed to support this application. The primary objective is to check the adequate balance of the safety systems design. The second objective is to check the safety level of the plant; however, frequency values for plant hazard states are mainly used for orientation. Decisions on backfitting or upgrading take into account both deterministic and probabilistic evaluations. One additionally important area is to support the dialogue between licensee and regulator by providing quantitative safety insights [21–23].

Technical and methodological aspects

The minimum modelling requirements for this application include a detailed plant specific Level 1 PSA. To most effectively evaluate the importance of each proposed backfit on overall plant risk, the PSA should include both internal and external initiating events.

The analysts should be aware that the proposed changes may also affect the risk in other operating modes, and, as a minimum, a qualitative analysis of the impact of the proposed changes on the risk associated to other modes of operation should be performed.

Considerations on the containment vulnerabilities are also important for this application. Thus, it is useful that the scope of analysis should include at least a limited-scope Level 2 PSA. The PSA should determine the frequency of different plant damage states that may occur and it should identify all important physical and functional dependencies that affect containment or confinement systems. This is important in order to take into account the different benefits of each proposed modification both from the perspective of core damage or large early release frequency, e.g. proposed backfits that may not significantly contribute to CDF reduction may still be very effective to reduce the frequency of off-site releases.

The first step in the evaluation of the proposed backfit or upgrade is a qualitative assessment of its impact on risk. In many cases safety systems or systems which impact risk are

not involved, so it is not necessary to perform quantitative analyses. Comparative evaluation of proposed backfits requires that the PSA results should realistically account for actual plant operating experience. To the extent possible, the PSA should use plant specific data. However, the accumulated operating experience is often not sufficient to justify the use of only plant specific values for the majority of components and failure modes. The PSA should use a consistent method to combine plant specific experience and generic data. The PSA should not use screening values for equipment failure rates, maintenance unavailabilities, CCF parameters, or human error rates. Generic data and screening values may not fully account for plant specific factors that influence the relative benefits of different proposed options.

Precautions and limitations

Clearly, a PSA can only be used to identify which safety improvements are most effective to reduce overall plant risk within the limitations of the PSA models and scope of analysis. This information provides an important basis for informed discussions between the plant operator and the regulatory authorities. However, final selection of the backfits must also take into consideration deterministic design criteria, cost-benefit evaluations, and other factors that are beyond the scope of many PSA models and analyses.

Modified procedures and training are often suggested as alternatives to plant hardware modifications. The assessment of the reduction in risk from such improvements will depend on the level of detail in the modelling of operator actions in the PSA. In these cases, the decision making process needs to take into account the possible increased burden on the plant operating staff from more complex procedures, training requirements, difficult decision criteria, and stress that may be introduced by higher reliance on operator actions to mitigate severe accidents. In these evaluations, it is fundamental to perform a thorough analysis of human dependencies that may appear when new operator actions are introduced. These dependencies may significantly reduce the efficiency of the proposed changes.

Decisions about proposed plant improvement options should be based on a thorough review of the PSA event sequences and examination of different measures of importance. Care should be taken to ensure that any negative impact arising from the interaction of the modification with existing equipment or addition of potential initiating events is taken into account.

Proposed plant improvement options should consider all contributions to plant risk. Options should not be based on limited examination of a single issue unless that issue completely dominates the total plant risk profile. In many cases, identification of the most effective improvement options requires an integrated understanding of all contributors to risk. These contributions often depend on specific plant design and operational features. Therefore, the most effective solution for one plant may be different from the most effective solution for another.

Recommended improvement options should consider the inherent uncertainties in the PSA methods, models, and results. In some cases, additional analyses are necessary to refine the PSA results and, if possible, to reduce important sources of uncertainty before specific plant modifications are recommended.

Selection of practical backfits to achieve full compliance with national or international probabilistic safety criteria may be rather difficult for some plants if the PSA does not identify

any dominant contributors to risk. In this case, a large number of improvements may be required to achieve a significant reduction in the total plant risk.

3.2. Use of PSA in connection with NPP operation

3.2.1. Use of PSA in NPP maintenance

3.2.1.1. Use of PSA to support maintenance planning.

The establishment of an effective safety related maintenance programme at the nuclear power plants ensures that the level of reliability and effectiveness of all plant systems and equipment having a safety function is maintained in accordance with design and assumptions, and that the safety status of the plant is not adversely affected during operation. The purposes of monitoring, testing and other preventive maintenance actions are therefore to detect the degradation and to prevent the failure of the safety function of systems and equipment and to assure the prompt correction and restoration of these safety functions.

The following sections discuss the use of PSA in connection with NPP maintenance planning.

Uses, benefits and advantages

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.

PSA can be used to prioritize the system maintenance related activities which can have the greatest impact on risk and plant safety. Maintenance can be planned and scheduled accordingly. The results of maintenance activities and the performance of the equipment can be compared against the modelling performance assumptions used for the reliability and availability of the equipment. Decisions can then be reached on the adequacy of the performance of the system, the need for revised maintenance activities, or the need for system redesign or modifications. This process of identifying risk significant systems and equipment can also be used to plan and schedule all maintenance activities on a risk informed basis.

PSA can be used to identify systems for which detailed study of maintenance activities is appropriate. This detailed study can then be carried out using other techniques.

PSA can subsequently be used to monitor the risk impact of changes in maintenance and testing strategies, provided adequate data on the change in system or component reliability is available.

If there is a risk monitor model, the PSA can also be used to examine the risk impacts over the set of activities from the proposed maintenance schedule. This will include the specific combinations of equipment that are removed from service, the frequency and duration of planned maintenance, and the plant operating mode for each activity. This will provide a risk

profile for the duration of the schedule, the mean risk over the duration, and the integrated core damage probability for the complete set of activities.

The use of PSA should help maintenance staff to optimize the maintenance programme, i.e. (a) to identify equipment requiring somewhat upgraded preventive maintenance, (as an increase in its reliability results in a substantial gain in safety), (b) to identify equipment requiring sustained or slightly reduced preventive maintenance (as a decrease in its reliability does not affect the level of safety) and (c) to identify equipment requiring only corrective maintenance (as its unavailability does not result in a major increase in risk).

Furthermore, some items in the maintenance programme or maintenance requirements set up by engineering judgement may not lead to an increment in the safety level. PSA based methods provide tools to balance the safety, operational/technical and economical requirements. The development and management of an effective maintenance programme involves complex and multidimensional cost-benefit analyses. PSA provides quantitative information about the potential risk benefits from improved equipment availability and the risk consequences when equipment is removed from service for maintenance. This information can be compared with other costs and benefits to ensure that resources are used most efficiently to support a high level of plant safety and availability.

Examples and experience

The use of PSA to support maintenance planning is very much connected to other PSA applications that this document deals with separately for practical reasons. For example, the use of PSA to support in-service testing and in-service inspection activities, the use of PSA in connection with the technical specifications of the NPP (surveillance test intervals and allowed outage times) and risk based configuration control are different aspects of NPP maintenance.

Operating experience with emergency diesel generators (EDG) has raised questions about their testing and maintenance to achieve the EDG reliability levels and about the total EDG unavailability experienced (fraction of time EDG is out of service due to testing, maintenance, and failures). Reference [24] uses operating experience to assess EDG unavailability due to testing, maintenance, and failures during reactor power operation and during plant shutdown. The collected data showed improvement in EDG reliability together with an increase in EDG unavailability due to maintenance, a significant portion of which was due to routinely scheduled maintenance. PSAs of selected nuclear power plants were used to assess the risk impact of EDG unavailability due to maintenance and failure during power operation, and during different stages of plant shutdown. The results of these risk analyses have led to qualitative insights for scheduling EDG maintenance in such a way that the impact on risk of operating nuclear power plants is minimal.

Reference [25] presents a study performed in order to optimize the frequency of on-line maintenance of the emergency diesel generators at Hope Creek. This study was aimed at identifying, analysing and modifying maintenance planning and scheduling practices to assure the high availability of emergency diesel generators. Input from the application of a recently developed reliability model, from PSA considerations, plant specific experience, insights from personnel involved in EDG maintenance and other practical issues were used to define a maintenance schedule that balances beneficial and adverse impacts. The conclusions resulted

in feasible recommendations to optimize and reduce the frequency of diesel on-line maintenance, thereby freeing resources to better maintain other equipment important to safety.

The San Onofre Safety Monitor is a real-time risk monitor which is used on a daily basis by the operation, maintenance and safety organizations to evaluate the risk of proposed and actual plant configurations. Following an US NRC recommendation, switchyard maintenance impacts were added to the Safety Monitor during its initial use in an attempt to more fully address the potential for site induced loss of off-site power events [26]. Use of this tool identified unexpected risk impacts from concurrent "high impact" switchyard maintenance and in-plant maintenance on some plant components. As a result of those risk impacts, the utility placed additional controls on the co-ordination of in-plant and switchyard maintenance at San Onofre and became more sensitive to the impact of switchyard maintenance on plant risk.

A relevant example of the role of PSA in maintenance optimization approaches is the US NRC Maintenance Rule. The Maintenance Rule is a performance based rule that calls for risk based considerations for its implementation. The principal activity required by the rule is the monitoring of the performance or condition of structures, systems, and components (SSCs) within its scope. Additional activities and remedial actions are only required when the performance of SSCs drops below the level of utility specific performance criteria. The Maintenance Rule brings in the concept of risk by requiring that the goals for measuring the performance of SSCs shall be established commensurate with safety. In NUMARC 93-01 [27], the Nuclear Energy Institute described an approach to using a PSA to categorize SSCs according to their risk significance to help determine the scope of the maintenance rule, and also gives guidance on the establishment of performance goals and monitoring. The PSA is also a tool that can be used to address the following statement: "In performing monitoring and preventive maintenance activities, an assessment of the total plant equipment that is out of service should be taken into account to determine the overall effect on performance of safety functions". Reference [28] provides an overview of ComEd's PSA support of Maintenance Rule implementation.

During an IAEA Technical Committee meeting on PSA applications held in Madrid in February 1998, a session was held on Use of PSA to support Test and Maintenance. References [29–33] present interesting examples of this type of PSA application.

Examples of the use of PSA to support on-line maintenance programmes at nuclear power plants can be found in Refs [34, 35].

Further information on this application can be found in IAEA-TECDOC-1138 [6]. In particular, Section 4 of IAEA-TECDOC-1138 discusses the use of PSA in maintenance related decision making and provides additional information on issues associated with PSA applications in maintenance such as PSA quality, scope, level of detail, human reliability and other specific modelling features that are desirable to support these applications. This publication also presents an extensive discussion on deterministic/engineering considerations and their interfaces with probabilistic evaluations. Finally, this publication also includes some papers related to this PSA application presented during an IAEA Technical Committee Meeting on Advances in Safety Related Maintenance, held in Vienna, Austria, in September 1997.

The minimum modelling requirements include a detailed plant specific Level 1 PSA. To most effectively evaluate the importance of each component and each planned maintenance activity on overall plant risk, the PSA should include both internal and external initiating events.

In general, proposed maintenance plans will include containment or confinement systems and their support systems. Therefore, the analyses should also include at least a limited-scope Level 2 PSA. Also, it should be recognized that maintenance induced failures of the containment systems can introduce containment by-pass situations which may go undetected for some time.

An important purpose for this application at many plants is to optimize the combinations of planned maintenance that are performed during plant power operation and during shutdown. To most effectively determine the net risk impact from each proposal, the scope of analysis should include PSA models for shutdown conditions. These models are necessary for a detailed comparison of the risk from performing each activity during shutdown and during power operation. Shutdown PSA models are required to evaluate trade-offs and to minimize total plant risk during all operating modes.

Many plants schedule planned maintenance for co-ordinated groups of equipment at the same time (e.g. one complete train of safety systems, electrical inspections, etc.). The relative risk from this type of maintenance, compared with individual component outages, depends on the specific plant design and its normal operating configuration. If this type of correlated maintenance is proposed, the PSA models must include appropriate logic to account for the fact that all affected components are out of service simultaneously. The PSA must also account for changes to the plant operating configuration when this type of maintenance is performed. For example, it is necessary to revise assumptions and models for normally running and stand-by equipment when each train is out of service. This may require substantial changes to the original PSA models if they are based on a specific assumed plant configuration.

For some maintenance related applications it could be beneficial to have separate models for unavailabilities due to preventive maintenance, corrective maintenance and surveillance tests. This would show explicitly the different contributions from regularly scheduled preventive maintenance or surveillance testing tasks (with a relatively fixed frequency and duration) and from corrective maintenance (with less certain frequency andduration). However, in practice, at the nuclear power plants the limits between preventive and corrective maintenance tasks are not always clear cut, and therefore, depending on how unavailabilities due to maintenance are recorded, it seems that this separation might not always be possible or simple. In addition, the use of separate models for unavailabilities due to preventive maintenance, corrective maintenance and surveillance tests increases the size of the model, the number of cut sets and may mask the importance of the (total) component unavailability due to maintenance and testing activities. This is not a problem if the PSA software used is able to handle calculations of importance measures of groups of events that have been assigned a common characteristic.

The use of single unavailability events, rather that separate events as discussed above, is, in principle, not an impediment in order to carry out PSA based maintenance planning applications, but it implies that more off-line analysis of the results may be necessary to evaluate the importance of the different contributions to the unavailabilities due to maintenance. If it is intended to look closely into such items it is necessary that the reporting of the reliability data

derived for the components contain information on what assumptions were made about the performance of preventative maintenance, its frequency and content, as well as the test intervals for the specific components.

Ideally the facility should exist in the PSA model to replace individual and multiple basic events with a substitution event representing the unavailability due to the maintenance activity associated with one or more components.

Proposed maintenance plans may have different impacts on possible CCF, human error probabilities and initiating event frequencies. Therefore, it is necessary to re-examine the CCF, human reliability and initiating event analyses in order to study the impact that the proposed strategies and changes to maintenance might have on these types of events.

Precautions and limitations

While the PSA can be used to evaluate changes to maintenance programmes at the high level, there are limitations in the detailed understanding of the causes and nature of component failures. Thus, it is difficult to relate specific aspects of surveillance testing and maintenance to component reliability. For example, it is not within the capabilities of the current state of knowledge to determine the impact on the reliability of a component of changing a surveillance test from a functional test to a test designed to measure degradation due to ageing. Similarly, the negative impact of testing in causing wear-out, or indeed the positive impact in preventing the drying out of seals or building up of deposits, are not easily accounted for. Thus, the use of models that purport to address the relationship between testing, maintenance and reliability must be characterized carefully, and used with caution.

3.2.1.2. Use of PSA to support reliability centered (RCM) maintenance programmes

Effective maintenance of equipment systems and structures at NPPs is essential for their safe and reliable operation. Although maintenance is a routine activity, a number of methods and approaches have been developed to optimize maintenance both from the safety and the economic standpoints.

Reliability centered maintenance (RCM) analysis is a systematic evaluation approach for developing and optimizing a maintenance programme.

The RCM methodology involves a systematic and logical consideration of the systems, subsystems or component functions, the failure modes for each function, the importance associated with the function and its failure. For safety related systems, the PSA model is the only tool to identify the relative importance of the system components (through a range of importance measures). Therefore, PSA can be used in connection with the RCM process in order to focus the analysis on the key components.

Uses, benefits and advantages

Using PSA in connection with RCM offers some very clear advantages for safety related systems and non-safety systems the performance of which has an effect on some initiating event frequencies. PSA is uniquely capable of identifying the safety significance of components and maintenance activities (planned or unplanned) and therefore can be used for identifying areas of emphasis for the RCM process. The reliability database established for the

PSA can provide one of the inputs to the decision making process when performing RCM. The risk impact of the revised maintenance strategy arising from the performance of RCM can be assessed by modifying relevant PSA data, i.e. by changing the equipment/system unavailabilities according to the new strategies and by tentatively modifying the relevant failure rates based on engineering judgement. Following the introduction of the revisions and when real plant data is available (after the programme has been implemented long enough), the PSA database should be updated and the actual risk impact reassessed.

Examples and experience

A paper on Use of risk importance measures in maintenance prioritization by A. Dubreil Chambardel, F. Ardorino and P. Maugerm, included in IAEA-TECDOC-960 [36], (see also Ref. [37]), presents an RCM method developed by EDF in France since 1990 to optimize maintenance through a prioritization of resources for equipment that are important in terms of safety, availability and maintenance costs. In 1994 it was decided that this method be applied to most of the *important* systems in the French PWRs. About 50 systems are in the scope of this RCM programme. The safety related systems were ranked according to their risk contribution provided by PSA.

In this RCM programme, PSA importance measures are also used to help defining equipment and failure modes critical to safety. It is foreseen that this PSA based information can be used, together with other information on equipment reliability and maintenance cost and efficiency, to determine trends regarding upgrading or downgrading of maintenance, check and inspection tasks.

Technical and methodological aspects

In order to support the RCM process effectively, the PSA model needs to be at least a Level 1 PSA that includes internal and external initiating events.

Following the basic RCM steps, the PSA can contribute as follows:

- plant partitioning/system selection/data and information collection — the PSA model includes information that is already structured in a way that can meet some of the RCM needs;

- functional failure mode criticality ranking/identification of critical components. The PSA can be used to rank the components/failure modes according to their impact on the overall plant risk. In order to obtain a list of components/failure modes to be considered which is as complete as possible in the RCM process, the results obtained from the PSA will need to be supplemented by the addition of other components/failure modes based on engineering judgement, cost considerations or other qualitative factors;

- initial maintenance task selection — before the programme is implemented, the PSA can be used to assess the effect of the revised programme on the overall plant risk;

- maintenance task implementation — using the PSA as a living tool, the ongoing effects of applying RCM can be assessed to help determine whether or not further changes to the maintenance programme are necessary.

Precautions and limitations

In the RCM process, PSA can be used both as an informational source and as an assessment tool. In using the data relating to maintenance activities and component performance in the PSA, attention should be paid to the completeness (components and failure modes) and extent of the data models in the PSA. The use of PSA to identify components needs to be combined with results from other approaches.

If the PSA is used to assess the impact of new or proposed maintenance practices in the plant risk, caution is necessary when making assumptions related to the expected behaviour of components following such changes in maintenance. Decisions should not be made based solely on the results of these evaluations. It is expected that the effect that modifications of the maintenance activities may have in the component reliability parameters will not be observed at once but, rather, once the programme has been in place long enough to provide meaningful feedback.

3.2.1.3. Risk informed in-service testing (IST)

Current in-service testing programmes are performed in compliance with the requirements of the ASME code (Section XI) or equivalent codes.

Traditionally, the test strategy is deterministically based with an intuitive or quasi quantitative assessment of plant safety. The PSA can be used to support the IST programme, taking into account the relative risk significance of the components. The relative risk significance is assessed using a blend of probabilistic and deterministic methods before any test interval is changed and the aggregate impact of the changes is evaluated.

Uses, benefits and advantages

The use of risk information in the optimization of the in-service testing programme will help to better focus and allocate limited resources. Also, one of the outcomes of the process may be a reduction in overall operational and maintenance costs while maintaining a high level of safety. The PSA, together with deterministic methods and expert judgement, can be used to assess the risk significance of components, categorize them and accordingly formulate a new test strategy. Before the proposed strategy is implemented, it is verified by evaluation of cumulative effects. After the implementation of the modified test strategy, a continuous performance monitoring needs to be implemented and corrective actions may have to be taken if needed. A target risk level against which to assess plant risk is an advantage in implementing such a programme.

Examples and experience

IAEA-TECDOC-1138 [6] includes a paper on Risk Based Maintenance to Increase Safety and Decrease Cost, presented by J. Phillips at the IAEA Technical Committee Meeting on Advances in Safety Related Maintenance held in Vienna in September 1997. This paper outlines

the process proposed by ASME for applying risk based methods to in-service testing of active components in nuclear plant systems.

Reference [38] issued by ASME presents a specific application of the risk based in-service testing process for light water reactor NPP components. The recommended process for applying risk based methods to the IST pumps and valves in NPP systems is centered on three major areas, i.e. ranking of component importance in two IST groups using PSA together with deterministic and engineering insights, development of the risk informed IST programmes for the two groups, and implementation of the IST risk based programme. See also Ref. [39].

References [33] and [40] present an outline of the Cofrentes NPP risk informed in-service testing project and its results. References [41–43] provide additional examples. Recent publications can be found in Ref. [44].

Technical and methodological aspects

RG 1.175 [45] indicates that although a full PSA covering all modes of operation and initiating events is preferred for this application, a lesser scope PSA can be used to provide useful risk information. However, in this case, it needs to be supplemented with additional considerations.

The first step of this application is the determination of the safety significance of the components. This is normally done by an expert panel blending the results of the PSA and other engineering considerations. The components are categorized into two groups: low safety significant components (LSSC) and high safety significant components (HSSC). Initially the components can be ranked using the results of the PSA (i.e. importance ranking). The list is then finalized taking into account qualitative insights and engineering judgements to compensate for the limitations of the PSA.

Components in the LSSC group are the candidates for less rigorous testing compared with those in the HSSC group [45].

The PSA is used to analyse whether or not the extensions of test intervals for LSSC affect the risk in an unacceptable manner, i.e. if there are risk increment limits in place, these should not be exceeded. The impact of changing the testing strategy is evaluated by increasing the unavailability of the affected components and calculating the changes in CDF and release frequency. The performance history of the component needs to be evaluated as part of the justification for the proposed extension, i.e. this evaluation will help to support the conclusion that no significant degradation is to be expected as a result of the extended test interval.

As part of the process to evaluate the test strategies for HSSC, expert panels use operational experience and techniques such as failure mode and effect analysis (FMEA) and perform an assessment the effectiveness of the tests. It is necessary to bear in mind that while increasing the frequency of HSSC tests may be one way of reducing the risk calculated by the PSA, this approach can have detrimental effects on the component. This has to be considered when defining new test strategies. It may be that enhanced testing activities are more desirable than increased test frequencies.

When the IST plan has been developed, the plant-specific PSA can help to evaluate the effect of the planned programme changes on the overall plant risk. In this process, it is

important to consider the potential for test related initiating events, the effects of taking equipment out of service, and the potential impact of the modified programme in the CCF events and human failure events modelled in the PSA.

As part of the implementation process, performance monitoring, periodic reassessment and corrective action programmes need to be established to ensure that the assumptions upon which the modified testing strategies are based remain valid and that no unexpected degradation in the performance of the HSSC and LSSC occurs as a result of the implemented changes.

Precautions and limitations

The PSA should be used in conjunction with deterministic methods and expert judgements in order to improve confidence in the results. The proposed changes need to be carefully examined from the point of view of their effects, before the changes are implemented. Also, periodic re-assessments need to be performed and corrective actions need to be taken if necessary. There is an interaction between testing and preventative maintenance activities, so the impact of changes in one programme must be fed into the other.

3.2.1.4. Risk informed in-service inspection (ISI)

ISI programmes are intended to address all piping locations that are subject to degradation. The incorporation of risk insights in the programmes can help focus inspections on the more important locations. The risk informed in-service inspection methodology broadly consists of ranking the elements for inspection according to their risk significance and developing the inspection strategy (frequency, method, sample size, etc.) commensurate with their risk significance. It provides a framework for allocating inspection resources in a cost effective manner and helps focus the inspection activities where they are most needed.

Uses, benefits and advantages

PSA findings and risk insights can be used to support decisions on changes proposed to a plant inspection programme. All the methodological steps of the process can benefit from using the PSA in addition to the other sources of information. For example, PSA can be used to identify the appropriate scope of components for inspection (i.e. piping segments) to be included in the programme. If the subject for analysis is modelled in the PSA, the probabilistic model is the best way to assess its risk significance. If not, it is still possible to establish the risk significance of the components for inspection by mapping the failures of such components to elements of the PSA model and to the results of PSA calculations. In addition, the PSA can provide a framework for determining target probabilities for the components subject to inspection and for assessing the risk impact of changes to ISI programmes.

Examples and experience

Reference [46] provides specific applications of a general method for risk based inspection proposed by ASME and is directed at the inspection of light water reactor nuclear components. This publication also discusses pilot studies carried out at some nuclear power plants in the USA. See also Ref. [39].

IAEA-TECDOC-1138 [6] includes a paper on Risk Based Maintenance to Increase Safety and Decrease Cost, presented by J. Phillips at the IAEA Technical Committee Meeting on Advances in Safety Related Maintenance, held in Vienna in September 1997. This paper outlines the risk based in-service inspection approach and discusses its benefits and the pilot project carried out at the Millstone-3 NPP.

Reference [32] briefly discusses the pilot projects carried out at the Arkansas, Vermont Yankee and Fitzpatrick NPPs to optimize the required maintenance programmes by applying a risk informed approach. It presents an overview of the WOG (Westinghouse Owners Group) risk informed in-service inspection methodology and discusses in some detail the Surry pilot project.

Ref. [47] indicates that the Nuclear Energy Institute (NEI) has developed guidelines on risk based ISI and submitted two methods, one developed by EPRI and the other developed by the ASME research and the Westinghouse Owners Groups for staff review and approval.

In July 1998, the US NRC released RG 1.178 [47] on An Approach for Plant Specific Risk Informed Decision Making: Inservice Inspection of Piping. This guide provides guidance on acceptable approaches to meeting the existing Section XI of the ASME Boiler and Pressure Vessel Code requirements for the scope and frequency of in-service inspection of piping systems. It focuses on the use of PSA and risk insights to support decisions on changes proposed to plant inspection programmes for piping.

Recent publications can be found in Ref. [44].

Technical and methodological aspects

In the process of identifying and selecting elements to be in the scope of the ISI programme, risk assessment is used to address the severity of consequences and the likelihood of failure. The severity of consequences is used to classify the component failures in different categories of risk significance. The likelihood of failure allows to focus the inspection on the most critical parts (terminal ends of piping runs, dissimilar metal welds, etc.). The combination of these two parameters allows the determination of the safety significance of the different elements to be considered for the inspection programme (e.g. pipe segments). The safety significance of the component will help determine the adequate level of inspection.

The selection and risk prioritization of components for inspection is performed by combining information from PSA with probabilities of pressure boundary and structural failures calculated using evaluation techniques such as structural mechanics analysis. Due to small probabilities of component ruptures, such failures make only a small contribution to the total CDF and, usually, they are not included in the models; if they are, they probably do not appear in the dominant minimal cut sets. Generally, only some pipe breaks are included globally in initiating events such as LOCAs, or flooding. Therefore, additional analysis of fault trees and cut sets is required to determine the effect of component rupture on the overall CDF. A way to address this limitation of the PSA models is to identify initiating events, basic events or groups of events already modelled in the PSA, whose failures capture the effects of the failure of the element analysed (surrogate approach) [47]. When assessing the consequences of a failure, it is necessary to also consider its indirect effects, i.e. effects on other components or systems caused by pipe whip, jet impingement, etc., or flooding.

Once the modified ISI programme has been defined, the PSA can help to demonstrate that the effect of the planned programme changes on the overall plant risk is not unacceptable.

As for risk informed IST, risk informed ISI should be considered a living programme and, therefore, as part of its implementation process, performance monitoring, periodic update and corrective action programmes need to be established.

Precautions and limitations

The PSA is an important input to the decision making process to develop the inspection strategy but, as discussed above, not the only one. The PSA should be used with care because structural failures are only small contributors to core damage frequency, and thus they are often not explicitly included in the models. It is important to fully understand the potential impacts of the failures under consideration in order to correctly identify all the aspects of the PSA models that may be affected and thus need to be taken into account for the estimation of the consequences of the failures.

3.2.2. Use of PSA in connection with NPP technical specifications (TS)

3.2.2.1. Use of PSA to support modifications to AOTs and STIs

Technical specifications (TS) are safety rules for NPPs that are approved by the regulatory authority. The technical specifications define limits and conditions for operations, testing, and maintenance activities as a way to assure that the plant is operated safely in a manner that is consistent with the assumptions made in the plant safety analyses. The TS define limiting conditions for operation (LCOs) and surveillance requirements (SRs).

LCOs define equipment operability requirements and allowed outage times (AOTs). The AOT for a particular system or component specifies the time period during power operation within which any repair or maintenance should be completed. AOTs are increasingly being defined for shutdown. If the AOT when at power is exceeded, the plant operating mode must change, or the plant must be shut down. The frequency and type of maintenance are not controlled by the LCOs, but the duration of maintenance and the combinations of components that may be simultaneously unavailable are controlled.

Surveillance requirements define the safety system (and safety related/supporting) testing requirements and the surveillance test intervals (STIs). The STIs control the frequency of testing. In some cases, the surveillance requirements also define the scheduling of tests and specific testing strategies. If the STI is exceeded, the affected equipment must be considered inoperable and, according to the AOTs, the plant operating mode must change, or the plant must be shut down.

PSAs are used in several Member States to develop quantitative bases for optimized limits on equipment AOTs, STIs, and testing strategies.

Uses, benefits and advantages

Technical specifications have been developed, applied, and improved in most countries over the years. LCOs and surveillance requirements have been traditionally based on deterministic analyses and engineering judgement. The technical specifications are one of the

most important criteria that affect daily plant operations, testing, and maintenance activities. They are strictly followed during all modes of plant operation, and they are an important interface between the plant operator and the regulatory authorities. Therefore, it is important that these requirements be stated clearly and be consistent with the actual contributions to plant risk.

The AOTs were originally defined for corrective maintenance. There is now increased agreement among plant owners and regulatory authorities that performance of planned preventive maintenance during power operation introduces potential benefits for improved equipment reliability, improved operational flexibility and outage work planning, and reduced risk during plant outages. Therefore, AOTs are now also used to control times for preventive maintenance.

PSAs can be used to modify AOTs and STIs based on a quantitative analysis of specific contributors to overall plant risk. The benefits from these risk based analyses include:

- Consistent basis for AOTs that account for the installed level of redundancy, operating configuration, equipment reliability, and risk importance of each system.
- Justification for planned preventive maintenance schedules during power operation and during shutdown conditions.
- Specification of STIs that minimize total unavailability from undetected incipient failures and from test induced failures.
- More effective surveillance requirements and functional testing strategies to identify incipient failures and to minimize CCF mechanisms.
- Improved communication between plant operators and regulatory authorities through a common basis for understanding and quantitative measurement of the risk impact from new or revised technical specifications.
- Reduction of requests for regulatory relief from excessively restrictive LCOs.

Examples and experience

Regulatory authorities in some Member States now accept PSA as a valid basis for review and revision of existing technical specifications and for development of specifications for new plants. However, PSA is not currently used as exclusive justification for licensing decisions. Regulatory authorities typically encourage the use of PSA to provide quantitative support for requests that are also justified by deterministic analyses and criteria. The use of PSA to support optimized technical specifications is an important element in evolutionary programmes for risk based/informed regulations that have been adopted by several Member States.

IAEA-TECDOC-729 [48] discusses the basic objectives and reasons for seeking PSA based applications for improving technical specifications, describes how PSA can be used to modify AOTs and STIs, presents an overview of methods and data requirements and provides examples of some applications.

NUREG/CR-6141 [49] presents different approaches for risk based analyses of AOTs and STIs. It includes information on data needs, outlines the insights to be gained and provides additional references and examples of evaluations.

NUREG/CR-6172 [50] presents an approach for reviewing PSA based submittals for changes to technical specifications. It also provides an example of a review by the US NRC of a PSA based submittal to modify the TS at the South Texas Project (STP) Electric Generating Station Plants.

US NRC RG 1.177 [51] presents an approach for plant specific, risk informed decision making regarding NPP technical specifications and provides extensive information on modelling requirements for a PSA used to support TS modifications.

Reference [31] presents an overview of the research work on PSA based analysis of the technical specifications and preventive maintenance (PM) carried out at the University of Valencia (Spain). This paper includes discussions on risk measures to be adopted for this evaluation, risk level variation over different plant states, risk associated with the TS requirements and on how to use PSA to determine risk contributions. Finally, it proposes strategies for TS and PM planning.

IAEA-TECDOC-1138 [6] includes several papers that discuss the use of PSA for technical specifications. The "Study on risk based operation and maintenance using the LPSA system", by K. Kurisaka, discusses the optimization of surveillance test intervals and limiting conditions for operation using PSA. It also presents a case study on risk based evaluation of surveillance test intervals for some safety related valves performed at a liquid metal cooled fast breeder reactor. The paper PSA and Methods to Optimize the Maintenance of Safety Related Equipment at Laguna Verde NPP, by A. Rodriguez and R. Camargo, presents the risk based approach selected for the optimization of STIs and AOTs at the Laguna Verde NPP and some results obtained. Risk Based Definition of TS requirements for NPPs with WWER Type Reactors, by V. Morozov and G. Tokmachev, presents a summary of studies that used PSA as an input tool, of modifications to technical specifications requirements carried out at some WWER plants. This paper proposes an approach to TS optimization based on a nine-state Markov model which uses PSA results as some of the required input data. Finally, On Test and Maintenance — Optimization of Allowed Outage Time, by B. Mavko and M. Čepin, proposes an approach for AOT optimization based on the comparison of risk at power and risk during shutdown.

Reference [52] presents examples of modifications to AOTs for the safety injection tank, low pressure safety injection system and emergency diesel generator performed by the CEOG (Combustion Engineering Owners Group) and explains how the proposals for AOT modifications where reached.

Further examples can be found in IAEA-TECDOC-873 [7].

Technical and methodological aspects

The regulatory authorities and the plant operator should clearly define the scope, purpose, and acceptance criteria for all risk based changes to the technical specifications. This scope is important to ensure that consistent criteria are used for approval of proposed changes and for the supporting PSA analyses. For example, different conclusions regarding AOTs and

STIs may apply if the scope is focused on core damage (e.g. Level 1 PSA) or if the scope is focused on off-site releases (e.g. Level 2 PSA). For example, the results from many PSAs for pressurized water reactors (PWRs) conclude that steam generator tube rupture (SGTR) events are relatively insignificant contributors to the total frequency of core damage. However, SGTR events are often the most important contributors to severe off-site releases. Therefore, different conclusions may apply about the most appropriate AOTs and STIs for systems that affect SGTR event response, depending on the Level 1 PSA and Level 2 PSA risk impacts from these systems.

Proposed revisions to the technical specifications may include changes that permit certain preventive maintenance and testing activities to be performed during plant power operation, rather than during shutdown. In this case, it is desirable that the scope of analysis also include PSA models for shutdown conditions. These models would facilitate a comparison of the risk from performing each activity during shutdown and during power operation. In addition, for changes to TS requirements for systems needed for decay heat removal (e.g. auxiliary feedwater system, residual heat removal system, emergency diesel generator and essential service) an appropriate assessment of shutdown risk needs to be considered [51].

Operational experience collected can be used to confirm the adequacy of the defined AOTs and STIs. The reliability data used for components should be documented in such a way that the assumptions relating to test intervals and component reliability are clearly stated.

The assumptions relating to the modelling of maintenance unavailabilities (planned or unplanned) should specify the relationship (if any) between the unavailabilities actually occurring (plant specific data) and the AOT for the component or system.

Additional special requirements for methods, models, and data depend on the specific PSA application. The following sections summarize different requirements for analyses that are performed for changes to AOTs and to STIs.

Allowed outage times (AOTs)

The performance of preventive maintenance and necessary corrective maintenance during normal power operation (or during shutdown) should be controlled to allow sufficient time for proper completion of the work and to minimize the risk from equipment unavailability while maintenance is in progress. For a risk based evaluation, the primary quantitative assessment focuses on the risk impact due to the AOT period. This requires assessment of three types of risks.

- Instantaneous (conditional) risk while the component is in maintenance.
- Cumulative (integrated) risk over the AOT period.
- Average risk over a long period (e.g. yearly), taking into account the frequency of maintenance performed on the component.

In some cases, the optimum AOT may involve trade-offs between extended equipment unavailability during power operation and unavailability of the same equipment during shutdown conditions. For example, if an AOT is exceeded, most technical specifications require that the plant must be shut down. The affected equipment then remains out of service during the shutdown. The risk of shutting down the plant and subsequent operation in hot stand-by with

some equipment unavailable may be comparable to the risk from an extended equipment outage during power operation. Examination of these cases requires a low power and shutdown PSA.

The results from these PSA evaluations should present a quantitative assessment of the impact of the proposed AOT on each level of risk. For example, the results should summarize the conditional risk during a component outage and the average annual risk as a function of different proposed values for the AOT. Qualitative assessments and justifications need to be presented for important considerations that are not quantified in the PSA models (e.g. operational flexibility, personnel factors, consistency in regulatory compliance, etc.)

Surveillance test intervals (STIs)

The frequency and strategy for equipment testing should be controlled to confirm equipment functional operability, to minimize the risk from unavailability due to undetected failures, and to minimize the risk from unavailability due to tests and test induced failures.

The PSA models should be sufficiently detailed to include events that represent all the components and failure modes that are verified by each proposed testing strategy. In general, different models are required to account for the impacts of staggered testing and sequential testing.

In order to support modifications to STIs, the PSA based analyses need to address the following issues:

- Unavailability of stand-by components that are revealed only upon the performance of a test that includes functional verification of the respective failure mode. These failures on demand are sometimes modelled using a constant probability of failure on demand model (often interpreted as implying that the failure results from the shock caused by the demand), sometimes using a constant stand-by failure rate model (where the failure is envisioned as resulting from a randomly occurring event while the component is in stand-by), or sometimes as a mixture of the two. These test-revealed failures require that the component must be removed from service for repairs, and they are a source of unscheduled maintenance unavailability.

- Unavailability of equipment during the test due to realignment of valves, installation of jumpers or lifted leads in actuation or control circuits, opening of AC or DC circuit breakers, etc.

- Unavailability of equipment due to human errors to properly restore normal alignments after testing is completed.

- If it is known that a test leads to a higher probability of an initiating event (initiating event frequency is related to test frequency) then this relationship must be taken into account if the test frequency is changed.

Risk based optimization of STIs requires establishing a relationship between the frequency of tests and unavailability on demand. This is usually done using the stand-by failure rate model, since that model provides an explicit relationship between the test interval

and the unavailability. Since crediting all the probability of failure on demand to the stand-by failure rate process maximizes the impact of changing the test interval (subject to the assumption that the failure rate itself remains constant), attempts have been made to separate out the contributions due to the constant probability of failure. However, substantial expert judgement is usually required to allocate failures between these two categories. Sensitivity calculations can help to determine whether conclusions about the most effective STIs are significantly different for a range of postulated failure fractions.

Proposed testing strategies (e.g. staggered vs. sequential tests) may have different impacts on possible CCF mechanisms. Therefore, it may be necessary to re-examine the applicable CCF event data and the corresponding failure rate parameters if the analysis includes a comparison of different strategies, in addition to evaluating the proposed STIs.

The results from these PSA evaluations should present a quantitative assessment of the impact of each STI and testing strategy on overall plant risk. For example, the results should summarize the average annual risk as a function of different proposed values for the STIs. It is especially important to document all assumptions that are made regarding the impacts from "stand-by" and "shock/demand" failures and to provide sensitivity calculations that support the PSA conclusions. Qualitative assessments and justifications should be presented for important considerations that are not quantified in the PSA models (e.g. regular scheduling for periodic tests, personnel factors, consistency in regulatory compliance, etc.).

Precautions and limitations

Some PSA evaluations for AOTs use the assigned AOT as the mean duration for all preventive and corrective maintenance. This practice avoids the difficult task of estimating how the actual duration of maintenance may be affected by changes in the AOT. It provides an upper-bound estimate for the risk contribution from maintenance. However, for some equipment, this estimate may be substantially higher than the actual contribution, based on observed experience. This process also overestimates the risk sensitivity from variations in the AOT. The amount of conservatism from these effects generally increases as the AOT duration is increased. For example, if the AOT is relatively short, a large fraction of all maintenance activities may require nearly the entire AOT for completion. However, as the AOT duration increases, the fraction of activities that require the entire AOT typically decreases. Therefore, the total unavailability does not scale directly with the AOT. Use of the AOT for the estimated duration of maintenance simplifies sensitivity calculations that show how risk may be affected by changes in the AOT, but it overestimates the actual impacts from these changes. The plant operator and regulatory authorities should agree on the method that will be used to estimate the duration of maintenance before the supporting PSA analyses are performed.

If the approach selected for optimizing AOTs consists of comparing the risk of continuing to operate at power with the risk of shutting down the plant with the equipment unavailable in both cases, it has to be borne in mind that, because of the perhaps larger uncertainties in a shutdown PSA, particularly during the transient process of shutting down, there may be a tendency for this calculation to be done conservatively and thus to bias the equation in favour of longer AOTs.

Some PSAs use a stand-by failure rate model to quantify the unavailability of stand-by components to operate on demand. According to this model, the unavailability of a stand-by component depends only on the stand-by failure rate and the STI. The stand-by failure rate

model is a simplified approximation of a more detailed model that separately accounts for the impacts from incipient ("stand-by") failures that occur over time while a component is idle and demand ("shock") failures that occur when the component is required to change state. This model is adequate for quantification of average unavailability for most PSA applications. However, if the stand-by failure rate model is used for STI evaluations, it is recommended that sensitivity studies be performed to confirm that the risk impacts from the proposed STIs are not significantly different for reasonable ranges of possible "stand-by" and "shock" failure rates.

Some PSAs use a demand failure rate model to quantify the unavailability of stand-by components to operate on demand. The equipment failure rates in this model account for the combined effects from "stand-by" and "shock" failures, but the model does not quantify each cause separately. This model is also adequate for quantification of average unavailability for most PSA applications. However, it cannot be used for STI evaluations because it does not explicitly quantify different STI effects on equipment unavailability due to incipient failures.

The plant operator and regulatory authorities need to define numerical criteria for the maximum acceptable increase in risk from any change to existing AOTs or STIs. These criteria should be based on a total measure of overall plant risk, according to the defined scope of the PSA analyses (e.g. Level 1 PSA, Level 2 PSA, power operation, shutdown conditions, internal events, external events, etc.). The criteria should consider both relative and absolute measures of the change in risk. Specific numerical acceptance criteria may vary from one country to another. This is discussed further in Section 5.

Assessments should evaluate the risk impacts from each AOT and STI individually and the combined impacts from all proposed changes. Decisions should be based on the cumulative impacts from all proposed changes, considered collectively. Trade-offs may be necessary to optimize the AOTs and STIs for specific systems and to maintain an acceptable level of overall risk.

3.2.2.2. Use of PSA to support exemptions to technical specifications

As stated in the previous section, the technical specifications (TS) define limits and conditions for operation, testing, and maintenance activities as a way to assure that the plant is operated safely.

From time to time, the plant operator may need a TS exemption due to operational burdens and constraints.

Uses, benefits and advantages

As a comprehensive tool describing the risk associated with a particular plant configuration, the PSA can provide useful support to TS exemption justifications and/or to proposals for mitigation or compensatory measures, or to justify the relevance of these measures.

Examples and experience

It is expected that plants that have a plant specific PSA available may use its results and insights in order to help in the justification of exemptions to the plant technical specifications. In

these cases, the PSA can provide a risk based evaluation and justification for temporary modification of TS requirements. It helps to clarify arguments and rank priorities. It helps also to reduce the burden of regulatory requirements without compromising safety.

Technical and methodological aspects

As a minimum a plant specific Level 1 PSA is required. Models for fall-back states required by TS such as cold shutdown are desirable if justifications to TS exemptions are going to be based on comparisons between risk at power and risk during shutdown. In order to evaluate exemptions related to containment and associated functions, as a minimum a Level 1+ PSA would be necessary. The level of modelling detail should be enough to include all components and functions concerned.

The results of the application and the conclusions may be based on specific quantitative analysis or on insights obtained from the PSA results (cut sets and lists of importance measures). The justification for the TS exemption should include the estimated effect of the compensatory or mitigation measures.

The assumptions made in the model to quantify the impact of the exemption must be presented. Sensitivity analysis would reinforce the justification for the requested exemption. Qualitative assessment and justifications have to be developed in order to complete non-quantified aspects or aspects not taken into account in the model.

Precautions and limitations

Some aspects that need to be considered to justify a TS exemption cannot be addressed by the PSA based analysis. Therefore, the PSA remains a complementary tool to present and justify a TS exemption.

Some of these exemptions may need to be justified in a very narrow time frame. Therefore, the performance of a specific, detailed, comprehensive analysis and PSA re-quantification may not always be possible. However, PSA methods and results can still be used as one of the tools that can help the operator to justify an exemption to a TS requirement. In such cases a bounding analysis is likely to be the most appropriate.

3.2.3. Risk based configuration control

A comprehensive configuration control programme implies a sophisticated set of risk related measures to manage and control concurrent unavailabilities of components, the possibility of functional alternative components, the outage times of the unavailable components and the frequency of the critical configurations. These measures are implemented through operational and maintenance activities such as maintenance and test scheduling and scheduling of operational realignments.

An appropriate risk based configuration control programme would enable plant personnel to maintain the risk level of the nuclear power plant within an acceptable range during all the operational regimes.

Uses, benefits and advantages

The use of the plant specific PSA to support configuration control makes it risk based. The PSA can help to identify the measures needed, according to the situation, to reduce the risk to the acceptable level.

During the operation of a nuclear power plant, the availability of equipment changes due to equipment failures and maintenance activities. Also, the operating modes of the available equipment can change due to operational considerations. Plant configuration at a point in time can be characterized by the status of the equipment, e.g. out of service, open, closed, running, on stand-by, etc. For safety significant equipment, the equipment status can directly influence the risk. Even the configuration of non-safety related equipment can also have an important impact on the risk. For example, some testing activities could increase the probability of the occurrence of initiating events. Therefore, different combinations of equipment configuration, tests and maintenance activities will result in different levels of risk. The programme established to manage configuration related risk changes is called risk based configuration control.

The main benefit of establishing a risk based configuration control programme is the reduction of risk peaks and the control of the cumulative, or average risk. It helps to ensure that, as far as possible, the plant does not enter the critical, high risk situations and that other risk significant configurations are avoided.

There are two main tasks in the risk based configuration control, *risk planning* and *risk follow-up*. Risk planning is a forward looking application of PSA and it consists of supporting the preparation, planning and scheduling of plant activities and configurations. This application can be performed with an on-line or off-line PSA model. Risk follow-up involves the online use of the PSA by plant personnel in order to keep the risk due to actual configurations, plant activities and unanticipated events, at an acceptable level.

It is necessary to control the risk due to plant configurations during power operation as well as during shutdown states (both planned and unplanned). In fact, it should be borne in mind that during the planned shutdown periods the plant configuration changes much more dynamically than during power operation and, thus, it is to be expected that risk follow-up become more challenging. Therefore, risk based configuration control activities are bound to play a very important role during the shutdown states.

Examples and experience

It is worthwhile mentioning that most of the existing risk monitors were developed with the intention of using them for on-line configuration control. See Section 2.2.2.

The first application of such a tool was the ESSM at Heysham 2 in the late 1980s. This was followed by the Safety Monitor and the EOOS risk monitor, both used by utilities in the USA and Europe. Some organizations are developing their own risk configuration tools. See for example Refs [6–8], [29], [53] and [54].

The ORAM-SENTINEL is another example of a tool designed to be used for configuration control. This tool is widely used in utilities in the USA [55–58].

For the purposes of configuration control, some utilities have developed risk matrices which include the combination of systems out of service that are allowed, not allowed or not recommended. (e.g. Refs [29] and [59]).

Technical and methodological aspects

Section 2.2.2 provides technical details for the safety/risk monitors.

In a nuclear power plant, the organizations that can be most affected by and involved in the configuration control activities are maintenance and operation. The maintenance department can use the configuration control tool (i.e. safety/risk monitor) to plan the maintenance schedule. Operations personnel may use it daily to check the acceptability of the plant schedule. In some plants, the shift technical advisor uses it once every shift to evaluate the current risk level. The risk monitor it is also used by the operations personnel to get information on the recommended AOT, i.e. to establish limits more restricted than the technical specifications.

During a refuelling outage, the risk/safety monitor can be used up front, i.e. to identify risk evolutions and to programme the outage schedule accordingly. The configuration control tool can also be used by the outage personnel to modify the schedule according to needs that may arise during the outage.

The use of configuration control tools should be controlled by procedures. These procedures need to clearly specify who uses the tool and when the tool has to be used. Also, they need to stress the fact that this tool is only intended to support decision making, but never to override other rules such as the plant technical specifications.

The plant staff needs to be trained in the used of the risk based configuration tool. Some plants provide a short training course that focuses mainly on how to operate the tool and its limitations. Other plants provide longer training which includes basic PSA training.

The risk monitor models have to be updated at the same time as the LPSA models.

Precautions and limitations

Risk based configuration control is but one of the aspects of NPP configuration management. There are several other factors to be taken into account, such as the minimum required configuration during the shutdown period or the restrictions imposed by the technical specifications. Risk based configuration control supplements other configuration management activities at a plant, but it does not replace them and is not expected to do so in the near future.

3.2.4. Risk based safety indicators

In recent years, improvements in hardware and PSA related software have reduced the time necessary to re-quantify a PSA. This much increased capability, as discussed in the previous section, has opened new opportunities for the use of PSA models to recalculate the risk associated with varying plant configurations, thus providing a quantitative assessment of the impact of planned activities (i.e. maintenance, tests, changes) and unplanned events.

Given the value of the available PSA models and the significant information that can be extracted from them to evaluate, monitor and communicate plant safety related information, it is important to identify the type of indicators that can be extracted from the PSA which are most appropriate for the different uses and needs of plant management and staff.

Uses, benefits and advantages

Indicators to monitor the safety performance of nuclear power plants can be developed for a number of reasons, i.e. to present the plant safety status or to display changes in the operational conditions and plant response.

Presentation of plant safety status is valuable for management and for regulatory use. Displaying the changes due to operational conditions supports decision making for a goal directed safety management.

PSA contains a large amount of safety related information and is capable of quantitatively addressing the above mentioned issues. The risk based indicator system is a safety information tool, which can generally be used to monitor safety performance and to alert the user if parameters exceed certain levels or follow undesired trends.

Different types of information can be derived from PSA when it is used as a safety indicator tool for *long term* or *short term* applications. The *long term* risk based indicators focus on monitoring plant behaviour in order to get insights on the past history of NPP safety and to update the calculated average CDF. *Long term* use includes analysis of past plant behaviour integrating the events occurred, failures and unavailabilities. This information (including CDF trends, comparison between expected and calculated CDF, etc.) is of interest to regulators and high level plant management. *Long term risk based indicators* can also help to pinpoint ageing effects on components and systems. This information is important for the plant staff and can initiate design changes or modifications to testing and maintenance strategies, etc. Similarly, *long term risk indicators* can be drawn up for planning purposes. For long term planning, the assumptions regarding planned design changes, expected component behaviour, etc. can be introduced in the PSA models and data and can be analysed to obtain the expected average CDF for the next period.

Risk based indicators for *short term* use require instantaneous evaluation of risk. This type of application provides information on changes in CDF due to plant events and risk associated with planned activities.

Another two perspectives in the use of risk based indicators are the *backward looking* and the *forward looking* applications. *Backward looking* applications involve the reporting and analysis of events occurred such as initiating events, precursors including their development from an initial event, component failures, CCF, human errors, unavailabilities, recorded etc., and their integration in the PSA to obtain the indicators of past risk. These indicators will help to identify plant vulnerabilities, deficiencies in human performance, needs for design modifications or backfittings, needs for modification of maintenance strategies, need for modification of technical specification requirements, etc. *Forward looking* applications involve the integration in the PSA models of planned measures, configuration changes, planned maintenance activities, etc., and the PSA calculations to obtain the *indicators of the expected risk.* These indicators will help to prevent high risk configurations,

to assess possible changes to operating procedures, to assess proposed design changes, to plan maintenance strategies and outages, etc.

Examples and experience

An example of such a PSA application was presented by M. Bonaca at the Executive Meeting on Risk Based Regulations and Inspections that was held in Stockholm in August 1996 [60], the so-called *integrated safety performance indicator* implemented at the Northeast Utilities' Plants in the USA. At these plants, the following indicators are monitored and tracked: *actual daily risk profile*, *planned daily risk profile*, *annual rolling average of risk profile* and *initiating event frequencies*. The purpose of these indicators is to demonstrate the trends in overall nuclear safety by tracking the daily fluctuations in accident initiating potential and mitigating system availabilities.

IAEA-TECDOC-1141 [61] presents in its Annex 2 a description of the risk based indicators in the framework of the indicators to monitor NPP operational safety performance.

Technical and methodological aspects

PSA models are based on a large quantity of parameters and basic information. It would be neither possible, nor practical to use all these parameter as safety indicators. Besides there are different levels of importance for the parameters and not every piece of information included in the PSA is significant to safe plant operation. Therefore, PSA based safety indicators need to be selected at different levels of the PSA analysis, based on their importance and on the safety insights they provide to both NPP management and operator.

"Plant risk" is the global indicator. This indicator considers the overall risk resulting from plant operation. Depending on the scope of the PSA, this attribute can be measured in terms of individual risk, population risk, frequency of release categories or CDF. If the objective of the PSA is to assess and periodically monitor plant safety, the attribute most commonly used to perform this function is CDF (per year of operation).

Main contributors to CDF, therefore individually important and deserving to be individually monitored are "*frequency of initiating events (IEs)",* the indicators of the plant ability to respond to events: "*probability of core damage"* (upon occurrence of each initiating event) and "*probability of radioactive release"* (upon occurrence of core damage). These are second level indicators.

"*Safety function unavailabilities"* might be intermediate level indicators. As mentioned, PSA can provide indicators for many different levels; according to the behaviour and the sensitivity of the indicators used, the proposed framework can be modified and other intermediate indicators selected.

Lower level indicators are the *"system unavailability indicators".* These indicators can help to explain the behaviour of higher level indicators.

Depending on the information details needed to explain the higher level behaviour, lower level indicators such as *"train unavailability indicators"* or even *"component unavailability indicators"* can be selected. However, in order to build up a good and efficient

risk based indicator system, the developer of the indicator programme has to be aware of the usefulness and benefit of the different indicator levels.

Risk based indicators can be used for different purposes; depending on the purpose, short term or long term evaluations have to be performed.

Living PSA is the necessary tool for the risk indicator calculation. For the calculation of instantaneous risk, or risk associated with a specific plant configuration for short term evaluations, it is useful to have a risk monitoring tool capable of providing a fast answer for the issue evaluated.

The PSA used to produce risk based indicators should include all the internal and external initiating events relevant to the plant. For the calculation of the "*probability of radioactive release indicator"*, it would be necessary to have a Level 2 PSA.

There are methods and approaches to support estimations of changes in the expected *"initiating event frequencies"*, such as FMEA, fault tree analysis, probabilistic fracture mechanics analysis, or engineering judgement.

Precautions and limitations

Although PSA is a powerful tool to produce safety indicators of the risk associated to a plant, it must be borne in mind that there are significant contributors to plant safety for which PSA cannot give information. These are the attitude of the staff of the NPP towards safety and NPP management and organizational aspects. Thus, the use of PSA to support a safety indicator programme is limited.

The use of relative indicator trends rather than absolute values is suggested in order to avoid misinterpretation of indicator meanings.

3.2.5. PSA based evaluation and rating of operational events

The main purpose of the operational events analysis is to evaluate the safety significance of the events and to establish an event importance ranking.

The criteria for the declaration of "safety significant events" are currently not the same in all countries and, in general, these criteria are not specific enough to allow the evaluation of the seriousness of an event. The INES scale offers more objective criteria for this evaluation but its purpose is clearly communication with the media and not an in-depth technical evaluation of the safety significance of events.

Uses, benefits and advantages

The probabilistic models of the PSA serve to derive the scenarios of the possible ways in which events can develop and to analyse the implications of operational events.

The use of PSA for the analysis of operational events increases the understanding of the plant vulnerabilities given the event occurrence, and provides the basis for effective experience feedback. 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.

PSA can be used to analyse plant events which may initiate a plant trip, degrade or disable safety systems, or both simultaneously. The application can then provide an estimate, in terms of a conditional probability, of the margin for an accident with unacceptable consequences.

Thus, the basic purpose of PSA based operational event analysis is to determine how an operational event could have degenerated into an accident with more serious consequences and to derive the conditional probability of core damage due to such event.

Of special importance are the benefits from this application in terms of 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.

In addition, PSA based evaluation of events allows for the PSA model to be continuously checked for appropriateness and completeness with respect to its ability to depict the operational events. Actual events at nuclear facilities provide an important basis to compare PSAs with reality. Therefore, PSA based operational event analysis can contribute to validating and enhancing PSAs and to continuously check whether or not the PSA models are adequate, appropriate and complete.

Finally, the qualitative results of the evaluation of the event may give additional insights with the potential of modifying the ranking assigned based just on deterministic/engineering considerations.

Examples and experience

In the USA, following the review of the WASH-1400, and even more so after the Three Mile Island accident in 1979, several commissions investigating the possible enhancement of operational safety proposed the initiation of the analysis of precursors using probabilistic models. Such an approach was initiated in the early 1980s and was known as the US NRC ASP (Accident Sequence Precursor). ASP is still an ongoing programme, and precursor reports are prepared every year. See Refs [62–65].

Several national projects have developed since the mid-1980s, e.g. the German Precursor Study was initiated in 1984. Its primary objective was to determine if the accident sequence frequencies estimated by the German Risk Study could be confirmed by the operational experience of the Biblis NPP. (See paper on Precursor Studies by Kafka and Hoertner in IAEA-TECDOC-387 [66]). The accident precursor analysis for German nuclear power plants is an ongoing project performed by GRS [67].

In 1989 the IAEA initiated a pilot study on the use of plant specific PSA for event analysis (IAEA-TECDOC-611 [68]).

In 1993, EDF launched a programme for probabilistic analysis of incidents, referred to as the “precursor” programme. It involved identifying and analysing all the significant incidents that occurred in French NPPs which could have degenerated into more serious scenarios. (See

Ref. [69]). At the same time, the technical support organization of the French safety authorities began the same kind of evaluation (see Ref. [70]).

Further examples can be found in Refs [71–76].

The paper by R. Gubler entitled Putting PSA to Work included in IAEA-TECDOC-1031 [77] presents the most recent IAEA work on this topic. This paper describes a method for using PSA to evaluate operational events.

Technical and methodological aspects

PSA based event evaluation requires a very good knowledge of plant operation, especially of the event to be analysed, and a good knowledge of the contents of the plant PSA.

Operational events can only be evaluated in those plant states for which the plant PSA models are available. Also, it is recommended to use plant specific (or at least plant type specific) models. In general, this application is more realistic and credible with plant specific reliability data and is thus recommended. Nevertheless, if generic reliability data are available and relevant for plant, the insights of the study can still be drawn using generic data.

Three types of events can be analysed with PSA. The first are the sometimes called precursors to an initiating event, i.e. occurrences which are not in themselves initiating events, but given additional failures would have lead to an initiating event. If the event results in a reactor trip or shutdown, the event is then considered to be an initiating event (of the second type). The third type of events to be analysed are the so-called conditions, i.e. events which affect the plant's ability to respond to an initiator.

In all cases, the existing models and/or input data are modified to take into account the effect of the event on the degradation of safety functions. The analysis is performed up to the point of assessment of the conditional probability of core damage (or off-site release if this is the figure of merit of concern).

The general method for event evaluation consists in selecting fault trees and event trees from the base case PSA, which can be adapted to represent the paths to core damage or off-site release which are relevant to the actual event.

The approach involves the following:

- Clear and precise understanding of the incident (initiating event, equipment involved, operator performance).
- Mapping the event to the relevant sections of the PSA models (event trees).
- Modifying the fault and event tree models and maybe the data, including common cause failure and human reliability data, to reflect the incident. It is necessary to point out that a consistent method must be used for adjusting the human failure event probabilities, CCF probabilities and initiating event frequencies for the evaluation of operational events.
- Recognition of significant recovery actions performed during the incident or possible in response to it but not modelled in the PSA.
- Validating the "new" model with the plant operators.
- Calculating the results and analysing them with plant operators.

The most frequent way of presenting the results of the analysis is to calculate the *probability of core damage conditional to the occurrence of the event.* However, the relative significance of an event might be different depending on the "risk index" used, i.e. measures related to core damage vs. measures related to large release.

The plant state in which the event occurs is important. The results can be strongly affected if the event occurs in a particular plant configuration. For example, LOCA events may be much more onerous if they occur during intermediate or cold shutdown modes during which part of the automatic protection system may no longer be activated. Afterwards "what if" analyses can be performed to evaluate the event as if it had occurred in a different operating state or in a different plant configuration.

Plant specific initiating event frequencies should be used in all evaluations where the event under evaluation is a "condition event". For example, a failure of an emergency diesel generator does not have the same impact if the plant is situated in a region with a very stable grid (low frequency of loss of off-site power, LOOP) compared with a plant situated in a region where the frequency of LOOP is high.

Whatever risk based method, existing or newly developed, is used for event rating:

- The measures developed should be comparable for all events analysed.
- The measures should be calculated on a consistent basis.
- The rating scale should be understood by the analysts who perform the analyses and by the organizations who might receive rating reports and possibly base their decisions on them.

Precautions and limitations

The PSA based approach to rate events will not be useful for all the events that happen at the plant (i.e. radiation exposure, waste production). Care must be taken when comparing the safety significance of all NPP events that have safety implications.

It is recommended, when performing such evaluations, to take particular care in the modelling of the human interactions and CCFs. There are different modelling approaches to CCF and HRA and it may not be straightforward to modify, for the purpose of the analysis, the CCFs and human interactions involved in the operational event.

3.2.6. Use of PSA to evaluate safety issues

Technical problems at the plant might appear at any stage from the design and construction to later during plant operation. If these issues have a safety impact, they need to be addressed quickly so that a decision on how to proceed is taken without delay. Some safety issues may require a period of time to clearly identify the associated risk and the adequate measures. Sometimes these situations can lead to the need for extended cold shutdown, without additional value for the safety. PSA can provide a valuable input to the analysis and resolution of many technical problems or safety issues that might appear at the plants.

The safety issues can be identified by the regulatory body or the utility, they can be plant specific or generic.

The identification of the issue presents two aspects, characterization of the technical problem and description of the associated safety impact in terms of risk evaluation.

Uses, benefits and advantages

Safety issues can be identified with a variety of engineering and analysis techniques, including the use of PSA. The development of the PSA models may uncover areas of safety concern. Thus, PSA provides tools, information and indicators which are useful for identifying safety issues.

Very often issues that are technically difficult cannot be addressed in the short term, and a too conservative response may lead to undesirable situations such as performance of maintenance activities with insufficient preparation and undue radiation exposure to the workers, unnecessary loss of production, keeping the plant in a non-optimal, fall-back state, according to unavailabilities observed, or loss of public confidence in the nuclear industry.

In order to address adequately such issues, it is necessary to clearly identify the risk associated with them. The plant operator must have a consistent basis to determine which issues are most important to the safety of the facility in order to prioritize their resolution. PSA provides a powerful tool for this process.

PSA evaluations can also help in the selection of the mitigating measures and to justify continued plant operation.

Examples and experience

Appendix V of Ref. [78] describes the role of PSA as one of the tools in the overall safety review process. It specifically addresses the identification of safety issues, the evaluation of the relative safety significance of issues, the comparison with safety goals, the determination of issue improvement priorities and the evaluation of priorities for corrective measures.

The consequences of high energy line breaks (i.e. steam line, feedwater line) are a safety issue for WWER-440 reactors. This issue has been analysed with PSA and found to be an important risk contributor [79].

For BWR plants a generic safety issue is the blockage of the ECCS suction strainers when the system is in the recirculation mode. PSA is used to evaluate the risk impact of this issue (see Ref. [80] and Section 7.6.4 of Ref. [81]).

Technical and methodological aspects

As for other PSA applications, the PSA based evaluation of safety issues requires a plant specific or at least plant-type specific PSA. It should include all the internal and external initiating events. Ideally, it should cover all relevant operating conditions including low power and shutdown. In order to examine issues from the core damage, containment failure and off-site consequence perspectives, it is recommended that the PSA also include an analysis of physical and functional dependencies that affect the response of containment and containment safeguards.

When using PSA to evaluate safety issues, the first step of the process is to identify the affected accident sequences, evaluate their contribution to core damage frequency and the impact of the issue.

In order to evaluate whether the risk contribution of the safety issue is acceptable or not, the risk associated with the safety issue has to be compared against probabilistic criteria. If the residual risk remains acceptable for a limited condition of operation, the utility and the safety authorities can agree on a limited period of operation, with adequate restrictions or complementary/periodic tests, during which a definitive solution has to be found.

If the identified contribution to risk is unacceptable, an immediate solution may be required. It may be necessary or relevant to consider various alternatives to arrive at an acceptable solution; PSA can help to choose the measures that provide a better solution in terms of decrease of risk.

The cost effectiveness aspect may also be taken into account in the final choice of the acceptable solution.

Precautions and limitations

PSA provides a powerful tool for the evaluation of safety issues. However, depending on the characteristics of the issue and on the PSA models, evaluation of safety issues is not always straightforward, and not all the safety issues can be evaluated using PSA analyses.

Limited scope studies and extrapolations from generic PSAs should be used with caution.

3.2.7. Graded QA

Some plant components are classified as being safety related. Because of the importance of safety related components to protect public health and safety, a quality assurance programme is established to be applied to all activities affecting the safety related functions of that equipment. The overall purpose of the QA programme is to establish a set of systematic and planned actions to provide adequate confidence that safety related equipment will perform satisfactorily in service. The QA programme should be applied in a manner consistent with the importance to safety of the plant equipment [82].

Uses, benefits and advantages

PSA provides new insights that may be used to determine the relative safety significance of plant equipment. The probabilistic insights could be utilized to help identify low safety significant structures, systems, and components (SSCs) that are candidates for reductions in QA treatment.

Examples and experience

An approach to implementation of graded QA programmes is given in US NRC RG 1.176 [82]. This guide provides guidance for identification of the safety significance of SSCs, modification of QA controls according to safety categorization, monitoring the effectiveness of the graded QA programme, etc.

A typical application of implementation of the Graded QA programme has been carried out at the South Texas Project plants [83].

Technical and methodological aspects

US NRC RG 1.176 [82] indicates that all operational modes and internal and external events should be included in the evaluation of the safety significance of systems, functions and components. As a minimum, PSA models and results for core damage and large early release frequency for internal initiating events at full power are needed. In this case, qualitative studies of other initiating events and operational modes also have to be used as an input to the categorization process.

The definition of the proposed QA change includes the identification of all the functions a system must perform both during normal operation and those related to the prevention and mitigation of accidents. Then, it is necessary to categorize the identified system functions according to their safety significance. Generally, a minimum two level categorization is used (low and high significance).

The PSA model provides an adequate framework to characterize the importance of the system and system function. The quantitative importance measures from the risk studies provide valuable insights on the relative ranking of safety significance of well defined model elements in the PSA such as basic events, components, human actions, functions, trains, or systems. However, it has to be borne in mind that the safety significance of systems and system functions is more difficult to identify than the importance of PSA elements such as basic events. If the PSA software cannot support the evaluation of importances at system and system function level and for groups of components, the use of additional considerations, such as surrogate importance measures for categorizing the safety significance of functions will be necessary. For example it may be assumed that the system is as important as its more important component. However, this is not a sufficient justification to assume that the system function is low safety significant, and, thus, it requires further analysis.

The final categorization is determined during integrated decision making by an expert panel using, as for other PSA applications, PSA results in conjunction with traditional engineering judgement.

Once the high safety significant functions are identified, the list of components required to support the functions need to be identified. It must be pointed out that the definition/boundary of the components to which QA controls are applied and the definition/boundary of the basic events in the PSA are often different and that not all the components subject to QA are included in the PSA. The safety significance categorization for components is based on the safety significance of the function the component supports. Components which support only low safety significant functions are classified as low safety significant. The safety significance of components supporting high safety significant functions is not necessarily high. However, the classification as low safety significant of a component that supports a high safety significant function needs to be justified.

Once the low safety significance candidates have been identified, and before relaxing the level of QA controls applied to such components, it is necessary to demonstrate that the proposed changes to the QA requirements do not violate the safety principles. In addition, for

non-safety related components which have been categorized as high safety significant, it will be necessary to evaluate whether enhanced quality controls are necessary.

As for the other applications described above, performance monitoring, operational feedback and corrective action programmes need to be established as part of the graded QA implementation process.

Precautions and limitations

The categorization of the safety significance of components for application of graded QA should be accomplished through the use of traditional engineering evaluations in combination with quantitative risk importance measures and qualitative risk insights.

The PSA must demonstrate sufficient quality to support a decision on the acceptability of the proposed QA programme changes. If it is intended to fully implement a graded QA programme, all operational modes and internal and external events should be considered for the evaluation of the safety significance of systems, functions and components. If quantitative risk analyses for shutdown conditions and external events are not available, a qualitative assessment should be used as a minimum to ensure that the categorization of the safety significance of functions fully considers all relevant operational demands.

3.2.8. Use of PSA to support NPP periodic safety review

A safety assessment process consists in identifying safety issues, determining their safety significance and making decisions on the need for corrective measures. This has to be done continuously during the life of the plant. In practice however, a major safety review is normally performed periodically, e.g. every 10 years.

Uses, benefits and advantages

PSA provide useful insights into the safety of a nuclear power plant and is consequently a useful contributor to a periodic safety review. Although a periodic safety review can be carried out without a PSA, it is recommended that a PSA be undertaken for every plant and used in subsequent periodic safety reviews [84].

A major benefit of including PSA in periodic reviews is the creation of an up-to-date overview of the whole plant. If an older plant cannot be shown to comply with modern deterministic standards, PSA results can sometimes be used to help justify continued operation. The PSA review may well lead to the identification of real cost-effective improvements to safety. Frequently, the incorporation of data resulting from operating experience into the PSA to replace conservative design assumptions will lead to a relaxation of operating constraints, thus permitting more economic operation as well as maintaining adequate safety margins.

Examples and experience

In the UK, safety reviews of the plants and their safety cases are performed every 10 years. The development of a Level 2 PSA is part of the periodic safety review process. The development of these PSAs has lead to the identification of modifications which, once implemented, provide safety benefits [85].

In the Netherlands the PSA is required to be part of the 10-year periodic safety review. In the first periodic safety reviews of the Borssele and Dodewaard NPPs that were carried out in the early 1990s, the plant specific PSAs, that were under development at that time, were used to modify the proposed backfittings requested as a consequence of the new "licensing basis" for both plants [86].

Technical and methodological aspects

The role which PSA can play in the process of safety review will depend on its quality and the efforts at the plant to maintain it. Two important aspects are the current validity of the underlying modelling assumptions and the data used to quantify the models. Plant specific reliability data for key systems enhances the usefulness of the PSA results.

The usefulness of the PSA for safety review will depend on the extent to which the PSA meets the following criteria:

- It needs to be plant specific, or at least representative of the design. In addition, it must be regularly updated to account for plant modifications and should cover all plant configurations including cold shutdown.

- It should be complete enough in scope to include plant response to all relevant internal and external initiating events, support systems, and common cause initiating events. It must include human interactions, testing and maintenance activities and as much as possible all possible recovery factors (human and technical).

- The data must be plant specific as far as possible. The need for plant specific data is particularly strong for initiating events and for the operating profile of the plant (including the detailed planning of the refuelling outages). A plant specific reliability database is recommended.

- To examine issues from the different perspectives of core damage, containment failure and off-site consequences, the PSA should also include an analysis of physical and functional dependencies of the containment systems and barriers. As a minimum, an appropriate limited scope Level 2 PSA would enable these perspectives to be addressed.

Precautions and limitations

There are no specific codes or standards against which to judge the exactitude of the PSA results; for this reason, the comparison of the results with other PSAs or absolute risk criteria for the various PSA figures of merit have to be performed with extreme caution.

The results are particularly dependent on the degree of detail in the model, the assumptions on CCF and human factors, the inclusion of recoveries (human or component repair actions not covered by procedures), the degree of conservatism (in data and models), the range of plant configurations models and the basis for the physical models (design basis or realistic thermal-hydraulic analysis).

If no severe accident analysis (beyond the onset of core damage) is performed, then it is not possible to make any assessment and comparison against targets for off-site release or risk to the individual.

The most valuable information from PSA is a constant, interpreted basis for identification of the most important contributors to plant risks and the evaluation of the most effective safety improvements. With PSA, probabilistic safety goals can be used to best advantage for prioritization and for the scheduling of corrective measures.

3.3. Use of PSA in the area of incident and accident mitigation and management

With the advent of improved understanding and increased characterization of severe accidents, accident management can be analysed as an integrated process. The interrelationship of emergency operating procedures (EOPs), severe accident management guidelines (SAMG), and off-site actions can be planned and organized to minimize the consequences of severe accidents, considered over the whole spectrum of their possibilities and probabilities, within the limits of practicality. PSA plays a role in the development of these strategies. However, it must be said that PSA (whether plant specific or generic) never was and probably never will be, the sole source for information.

3.3.1. Use of PSA to improve emergency operating procedures (EOPs)

EOPs are predefined and documented procedures that operators follow when activating plant protective features. These documents are used to verify the automatic action of safety systems, to diagnose the situation by following a predefined logical process for selecting the appropriate procedure, and to take action as prescribed by this specific procedure. EOPs in some form are required and are in use as far as is known in almost any nuclear power plant in the world.

More and more EOPs are being based on a symptomatic (or safety system, function or state) approach, where the actions taken are determined by the actual situation as indicated to the personnel in the control room, rather than the chronology of past events and actions, as discussed for example in IAEA Ref. [87]. The TMI-2 accident, experience with plant operations, and the increasing sophistication of PSA have shown the need to take into account complex situations where it is difficult or impossible to diagnose the initiating event or even the effects of prior mitigative actions.

Uses, benefits and advantages

The improved understanding of nuclear accidents is a result of the gains from research and development activities in severe accident phenomenology and in the application to the analysis of realistic accident progressions. For its part, the increased characterization of nuclear accidents as to modelling and probability stems 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. 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.

Examples and experience

At the Palo Verde plant of Arizona Public Service, the plant PSA, in particular the Level 2 analysis and methodology, was used in support of relaxing conservatisms on such things as peak containment and pressure constraints on EOP decisions [88]. The EOP decision points had been based on limited deterministic calculations that were considered very uncertain. To improve this situation, the PSA spectrum of breaks were analysed with the MAAP code and a table of probabilities for pressure and temperature was generated using the PSA frequencies. The result was increased margin in the EOP decision making points as applied to instrument uncertainties that contributed to the regulatory decision to approve simplification of the EOPs. This then resulted in efficiencies in procedure maintenance and training.

The PSAs for the Rovno and Zaporizhye NPPs are being used in the development of the symptom based EOPs for these plants.

Technical and methodological aspects

The EOPs contain decision points and criteria for taking various actions. The uncertainties and margins associated with these parameters can be assessed through the use of PSA to identify bounding sequences for which realistic thermal-hydraulic analysis are performed and potential operator actions and timing are identified. The codes used for these analysis can be design or severe accident based (CATHARE, RELAP, NOTRUMP, MELCOR, STCP, MAAP, etc.)

The human reliability analyses for operator failure probabilities utilized in PSA modelling of the plant response to accidents are based on the operator actions prescribed in the EOPs. The analysis of failure probabilities provides insights into the validity and variability to be expected in the application of the EOPs. Data on operator reliability is continually being gathered to improve the analyses — PSA can provide some framework for assessing this data. This can lead to the development of improvements in existing procedures and to the evaluation of the safety consequences of proposed changes to EOPs.

The systematic assessment of plant vulnerabilities and the insights derived by the PSA process can contribute to the improvement of the EOPs by providing some assurance that a wider scope of vulnerabilities is addressed in a realistic, appropriately detailed and consistent manner. The integral view of the accident progressions provides information on the benefits and drawbacks of various operations in various abnormal plant states. It also can provide a basis for specifying the decision points for when the transition into the SAMG phase should occur at specific plants.

Precautions and limitations

Complete dependence on PSAs and PSA methodology to evaluate existing EOPs or to develop new EOPs cannot be justified. The existing EOPs are the product of long experience and are generally proven products. PSA can contribute to an understanding of the dominant accident sequences and the role of the operator in preventing core damage. Provided the human reliability modelling is related directly to the various steps in a procedure (or potential new procedure), this understanding can be used for the derivation of bounding conditions for the thermal-hydraulic calculations and simulator validation of new or revised EOPs. It is very

important to understand that the value of this aspect of the PSA is very dependent on the performance of plant specific task analysis for the derivation of the human error probabilities.

3.3.2. Use of PSA to support NPP accident management

When the EOP directed operation of the plant protective systems has failed to be effective in arresting an accident, the realm of severe accident management (SAM) is entered where any other possible means, internal or external, of mitigating the accident and its consequences may be utilized. The necessity of increasing plant safety by adopting measures of this type on a planned basis is recognized in Member States. In most Member States, the consensus of adopting SAM measures is reached between the regulators and the utilities on a more or less voluntary basis because such measures are not deemed to be legal requirements. Unlike EOPs, SAM procedures and programmes are currently fully implemented at only a relatively small number of plants. There are, however, widespread activities in progress to develop and adopt such arrangements at many more plants.

In the development of generic SAMG, plant specific PSAs of one or more representative plants within a particular group are used as well as bounding deterministic calculations to cover the whole group. A further description of accident management programmes in nuclear power plants is presented in Ref. [87].

The development of SAMG focuses on the decision making process for responding to and recovering from a severe accident condition. The overall framework of SAM includes the definition of objectives and goals which define the endpoint of the SAM process. The framework defines the use of challenges and parameters to indicate a controlled stable state as the means of diagnosing the severe accident status and defining the appropriate set of SAM strategies which can be implemented to respond to the severe accident conditions.

Because of the large uncertainty in our understanding of severe accident progression, SAM as a practical matter will probably be symptom based, as opposed to event based. In other words, it is more important to understand the challenges to the goals and objectives of SAM than it is to understand the accident progression (e.g. the degree of core damage, the location of various fission product species, etc.). This is not to say that the future accident progression at any point in time is not important; rather, the exact condition of the plant at any given time is less important than the challenges.

Uses, benefits and advantages

The first step in the development of SAM is to use the results of the plant specific PSA, given that such an analysis is available. It is the best source available to identify accident sequences, to categorize them into functional groups, and to provide descriptions of plant responses and vulnerabilities. PSA can support the development of strategies to deal with the identified vulnerabilities and of calculational aids that would be used to assist in the selection and application of the strategies. The integral view of plant response utilized in PSA methodology will be helpful in discerning the potential for negative effects of certain strategies.

In the SAM area, the applications of PSA are aimed not only at identifying accident sequences but also at developing accident chronologies, identifying success paths (strategies),

prioritizing safety features to reduce risks and forming the basis for operator training and for the development of procedures. In particular, lessons learned and insights developed from the PSA will be incorporated into plant specific SAMG.

Once the SAMG are developed and in place, the applicability of PSA is diminished. It would be periodically referred to in the "living sense" to assure that the SAM processes are still valid, both in terms of plant operation and phenomenological processes. The PSA is unlikely to be consulted during a real accident.

The applications of PSA in SAM training would parallel those for EOP training (see Section 3.3.4). It is likely that the degree, amount and frequency of training for SAM will be significantly less than for the EOPs and the unifying view that could be presented through the PSA results and models will be useful in maximizing the utility of the training provided. PSA can also be used to reduce the burden on licensed operator training programmes. For example, most SAM procedures call for the establishment of an emergency response organization (ERO) to provide additional support resources including personnel for emergencies.

Examples and experience

The Level 3 PSA for the Borssele NPP in The Netherlands was used in 1997 to develop a SAM procedure to keep the faulted steam generator filled in case of SGTR. Containment by-pass via a faulted dry steam generator was found to be a major contributor to the calculated societal risk. Subsequently, the approach adopted for the Borssele plant was based on adopting the generic SAMGs of the Westinghouse Owners Group (WOG). The next step is to modify these generic guidelines by taking into account the differences in design between the Borssele plant (SIEMENS/KWU-PWR) and the plant that formed the basis for the WOG SAMG, and by performing plant specific bounding deterministic calculations. The plant specific full scope Level 3 PSA will only be used for fine tuning [89].

The nuclear industry in the United States prepared an initiative to develop and install accident management programmes at all nuclear power plants by the end of 1998. The programme was designed to satisfy the US NRC performance objectives. Generic SAMGs were developed by each of the four owner groups (GE, W, B&W, and CE) that are applicable in a bounding sense to each plant in the group. These SAMGs include vulnerabilities, strategies, and guidance on production of plant specific procedures and calculational aids. This material was developed in large part by reference to the PSAs for each of the component plants of the group and calculations carried out that bounded all the plants. It was intended that the plant specific material be produced without the need for further extensive calculations on the part of the individual plant. The first or basic level training package was developed by the Institute for Nuclear Plant Operation (INPO) and the general programme direction by NEI (formerly NUMARC) and EPRI. The role of the US NRC was to co-operatively reach agreement with the NEI and EPRI programmes and to review the Owners Group material.

Reference [90] discusses how accident management strategies in Japan are based on the results of the PSA based individual plant examination programmes.

Reference [91] discusses how the Level 3 PSA developed for the Sizewell B NPP POSR was used in the assessment of the feasibility and effectiveness of two specific severe accident management options, i.e. the use of existing containment fire sprinkler (for containment protection) and filtered containment venting.

Reference [92] reviews and contrasts the key features of several models developed to address severe accident issues, i.e. containment event tree approaches (commonly used for evaluation of SAM measures), phenomenological fault trees, the ROAAM approach (also based on a probabilistic framework), and influence diagrams (network model with three types of nodes — decision, chance and value — connected by directed arcs that represent the dependence between the variables).

Technical and methodological aspects

In the past it was assumed that containment failure was inevitable if the core melted. The present understanding is that once the core has started to melt, the progression of the melt is avoidable, and it may be possible to restore core cooling, and, furthermore, core melt does not necessarily cause vessel or containment failure.

The objectives of accident management are to prevent or minimize core damage (restoration of core cooling and control of reactivity), to maintain the integrity or delay the failure of the RCS, to maintain the integrity or delay the failure of the confinement/containment and to mitigate the release of radioactive material.

According to Ref. [87], the process for the development of accident management strategies involves: (a) assessment of vulnerabilities and capacities (evaluation of the status of core cooling, reactivity, RCS and containment integrity under different plant conditions); (b) development of accident management strategies focused towards maintaining the safety functions; (c) structured process to match strategies and vulnerabilities; (d) definition of procedures and guidance taking also into account the available instrumentation, time for human actuation (diagnosis, actuation, evaluation of consequences), potential for confusing signals, etc.; and (e) validation of severe accident management procedures. A Level 2 PSA based on a full scope Level 1 plant specific or plant-type specific PSA can be used to support accident management in NPPs in the following ways:

- Identification of significant severe accident sequences. Note that the criteria for selection need to be based on the frequencies and consequences of the sequences.
- Categorization of the important accident sequences into groups with similar accident progression characteristics.
- Identification of weak points and critical features (containment and containment functions).
- Evaluation of consequences of failed systems, operator errors, inoperative equipment, potential use of non-safety related equipment to restore safety functions, etc.
- Development of accident chronologies.
- Identification of success paths.
- Prioritization of actions to reduce risk.

Precautions and limitations

Although a large number of severe accident studies have been completed (e.g. IPEs and PSAs) which define the most likely severe accident sequences, the knowledge of severe accidents with respect to accident progression leading to core damage is still very uncertain. This is due, in part, to the nature of the severe accident studies where: a) all equipment

failures are assumed to occur at the initiation of the event, b) limited recovery or repair of faulted equipment is modelled, and c) only those operator actions prescribed in the plant specific emergency operating procedures (EOPs) may be assumed to be implemented. The binning and grouping of cut sets and containment event sequences contributes to a loss of specific information through this averaging process. There are also uncertainties in phenomenological processes, in their modelling and a certain degree of randomness in the occurrence of events. Thus, while severe accident studies may imply that accident progression is well understood, the truth may be more uncertain. For this reason, development of SAM material must make use of all available safety and operational data that is available, without the PSA being the sole source.

The PSA itself is unlikely to be consulted in the case of an emergency. With the accident in progress, the probabilistic nature of the PSA is not readily applicable and the data and methods are not in a rapidly accessible format. The understanding of the range of outcomes from various events and actions will already have been codified in the SAM material.

In using PSA to support accident management, a wide range of possibilities need to be investigated with special attention to the possible drawbacks of the proposed measures by introducing other challenges to the plant. For example, if only a small amount of water becomes available in the late phase of the core degradation process, it might be more worthwhile to use this amount of water for other mitigative measures. The amount of water might not be enough to cool the degrading core adequately, but in reverse might introduce a sudden large amount of hydrogen after injection in the reactor pressure vessel.

3.3.3. Use of PSA to support NPP emergency planning

Emergency planning consists of the development of strategies to protect the public in situations of severe reactor accident. The reason for developing these strategies is that during the first hours of an accident at an NPP, critical decisions may be necessary for actions to protect the public; moreover, balanced protective actions will be required in the long term.

During the first few hours of an accident at a nuclear power plant, plant conditions are major determining factors in developing early protective action recommendations. The plant operator is responsible for mitigating the consequences of an accident and for recommending to off-site officials protective actions that are commensurate with the severity of the accident. These public officials are responsible for making decisions on the actions necessary to protect the public and for transmitting these decisions to the public.

The regulatory body responsible for the plant will monitor the actions of the plant operations staff and may provide guidance, recommendations and advice concerning the protective actions to both the operators and public officials. The plant operator and public officials would use such guidance in developing their emergency plans and implementing procedures.

The basic premise in emergency planning, and this is supported by PSA results, is that in the unlikely event of a severe core damage accident, plant operators cannot predict with certainty the occurrence of a radiological release, the magnitude and duration of any such release, or the radiological consequences of the release. The protective actions must be taken in light of these uncertainties, i.e. knowing the possible range of risks. Most emergency plans

in Member States were originally developed on the basis of release and dispersal calculations for a selected set of postulated accidents.

Uses, benefits and advantages

Level 3 PSAs can be used to assess the effectiveness of various protective actions such as sheltering and evacuation and the timing of their initiation. This assessment can assist in the preparation of the emergency plans.

Emergency plans and emergency preparedness need to be fully related to the actual understanding of the severe accident effects. Therefore, a good quality PSA can provide a very important contribution to the development of such plans.

Examples and experience

The US NRC and the US Federal Emergency Management Agency (FEMA) have revised their recommendations for initial protective actions [93], based on improved understanding of severe accident developed from various studies, including especially the PSAs reported in NUREG-1150 [1]. The US NRC and FEMA concluded that it would be better to evacuate promptly near the plant as a precautionary measure, rather than to shelter the nearby population while waiting for additional information that may become available only after a release occurs (as previously recommended). They recognized that sheltering people in most structures close to a plant would not prevent early adverse health effects during a major release.

The RODOS software system, developed under the Commission of European Communities (CEC) 4th framework programme, is an integrated tool for real or postulated nuclear emergencies in Europe. This system comprises a series of integrated software modules from initial source term prediction, through short range and long range dispersion and consequence modelling, to the evaluation of proposed countermeasures. A proposed source term module (RODOS-STM) for this system uses a Bayesian belief network to calculate the conditional probability of a source term category given a number of supporting observations. The information generated by the Level 1 and Level 2 PSA studies is the main source of data for the conditional probability assignments which link the nodes in the network. Information about the proposed RODOS-STM can be found in Ref. [94].

Reference [95] presents an overview of the use of risk assessment techniques to formulate the technical basis for the Koeberg NPP emergency plan.

Technical and methodological aspects

A plant specific Level 3 PSA based on the results of a full scope plant specific Level 2 PSA is necessary in order to adequately support NPP emergency planning.

The primary information needed for the Level 3 PSA stems from the Level 2 PSA. This is the radio-nuclide release (source term), including its *magnitude*, *frequency, energy content, height and timing of release.*

Additionally, it is necessary to collect a significant amount of meteorological data and data regarding the population, agricultural production, land and food distribution around the

plant. Other economic data might be relevant for the analysis of accident consequences and thus useful for the organization of emergency strategies.

In addition, the Level 3 PSA will require that the different possible countermeasures are factored into the analysis (i.e. *short term: sheltering, evacuation, iodine prophylaxis; long term: relocation, land decontamination, food bans, etc.*). With all this information, the Level 3 codes (e.g. MACCS, COSYMA) are able to calculate the risk associated with the plant generally in terms of early and latent fatality risk.

These codes allow to specify a wide range of emergency actions and criteria for imposing and withdrawing the actions, so that information can be obtained on how the consequences of an accident change according to the countermeasures considered. Therefore a Level 3 PSA is a valuable source for the development of emergency plans.

Precautions and limitations

Although there are ongoing developments of systems to help support decision making in emergency situations and some of these tools may use data obtained from the PSA, it is expected that the PSA itself would not be consulted to support the emergency response during an accident. With the accident in progress, the probabilistic nature of the PSA is not readily applicable and the data and methods are not in a rapidly accessible format. For efficiency and usefulness, the understanding of the range of outcomes from various events and actions and the impact of the different countermeasures should already have been taken into consideration in the development of the pre-established NPP emergency plan.

3.3.4. Use of PSA to improve operator training programmes

Operator training is extensive and continuous. Training is a combination of classroom and simulator exercises and in-plant actions, to the extent possible and appropriate. The procedures and training are designed to reduce the chance of operator error by increasing the familiarity of the operators with the prescribed actions and reducing the amount of memorization required and distraction by matters of lesser importance. The operators are tested for satisfactory performance both individually and as teams. This training includes training in EOPs.

Uses, benefits and advantages

PSA can support EOP training because it provides information on the accident processes, the relative likelihood of the dominant accident sequences and the associated operator actions required to prevent core damage. Thus, PSA can be used to help in the selection of accident scenarios for training. Absolute sequence frequency and risk significance in terms of relative contribution to the core damage frequency can be used as selection guides. Similarly, the relative consequences of various operator errors and the PSA predicted chance of failure can be used to select those actions that would benefit from emphasized training.

It is evident that with the introduction of SAMG there is also a need to make operators understand severe accident scenarios. A Level 2 PSA can be used in training to provide an understanding of the complexities and uncertainties of severe accident processes, the expected

plant specific responses and the limitations of the instrumentation and protective systems in such circumstances. The timing and necessity of transition to SAM procedures and organization can be presented in terms of the structured results of the PSA.

Examples and experience

It is presumed that those plants that have plant specific PSAs utilize them in the EOP training in a limited fashion to provide an overall understanding of the processes, environmental conditions and action outcomes that may be encountered in an emergency. For example, the paper by M.D. Morales et al. in IAEA-TECDOC-873 [7] indicates that several insights obtained from the results of the PSA of the Almaraz NPP, such as the human actions with short available time, have been transmitted to the different operator crews through their training.

Technical and methodological aspects

PSA results highlight the significant contributors to core damage. It is not unusual to find that many of these contributors are human errors. Sometimes, the high probabilities for these human type events arise from deficiencies in training. The impact of training in the human failure probability can be analysed if "operator training" is one of the performance shaping factors considered in the analysis of the human failure events. By performing sensitivity analyses, PSA analysts can determine how enhanced training can contribute towards reducing risk.

PSA can be used to improve operator training for emergency conditions because it can help to select and rank the accident scenarios based on established criteria: accident sequence contribution to core damage, fractional contribution of human errors in the sequence, sequence consequence, etc.

Precautions and limitations

The selection of scenarios for operator training should not be solely based on PSA results.

Care must be taken to ensure that both high frequency-low consequence and low frequency-high consequence sequences are selected to be included in the operator training programmes. For this reason, a Level 2 PSA can be of great advantage because it provides information on consequences as well as on frequency.

The impact of enhanced training programmes cannot be directly evaluated with PSA if the analysis of operator errors does not include the impact of training as one of the performance shaping factors considered in the quantification of human error probabilities.

4. REGULATORY PERSPECTIVE ON THE USE OF PSA

4.1. Increasing use of PSA in the regulatory process

4.1.1. Historical perspectives

Historically, the nuclear reactor licensing process has been based on deterministic regulatory requirements for the design and operation of nuclear power plants. Plants are designed with an implementation of the defence in depth philosophy, manifested by, for example, the use of multiple barriers to fission product release (i.e. fuel, reactor coolant system boundaries, and the containment system), and the establishment of safety margins. Conservatisms have been built into the analysis tools and the deterministic regulatory criteria to account for the uncertainties associated with the design, operation, and phenomenological processes impacting the plant performance. Plant design requirements have been derived through the analysis of design basis accidents (DBAs), supplemented by the single failure criterion in an attempt to ensure an adequate level of safety. DBAs are a combination of challenges resulting from postulated initiating events (PIEs) [96], and failure events against which plants are designed to ensure adequate and safe plant response. They are selected to envelope credible accident conditions, and to ensure that these accidents can be accommodated within the design envelope.

The deterministic regulatory process does not explicitly account for the probability of an event occurring. However, probabilistic reasoning was always implicitly utilized by not requiring analyses for multiple failure events, which are considered to be of low probability. DBA analyses often combine the initiating event with an additional single active failure to demonstrate design acceptability. Even though the design has to meet various criteria, meeting these criteria with multiple independent active failures is not a design requirement. Nor is the consideration of multiple simultaneous independent initiating events. Subjectively, such multiple simultaneous failures were intuitively judged to be too improbable and were therefore not included as part of the deterministic regulatory requirements [97].

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 provide the most suitable approach to achieving adequate protection of public health and safety. In fact, contrary to what had been assumed in the establishment of DBAs, the results of PSA studies have demonstrated that the risks of nuclear reactor accidents result from events that occur outside of the design basis domain, and are due to multiple failures, human errors, and external events. This observation has been dramatically supported by several of the serious historical incidents, such as the Three Mile Island Unit 2 (TMI 2) and Brown's Ferry incidents. The re-examination of some design basis events has, in fact, shown them to be extremely unlikely, to have limited off-site consequences, or both. Thus, reliance on regulations that are exclusively based on deterministic criteria may lead to overlooking potentially significant safety issues.

From the very beginning of the development of risk assessment methods, the use of PSA based results in regulatory analyses and licensing actions has been regarded with some scepticism. This perhaps reflected a concern about the uncertainties inherently associated with PSA results, and that the analysis has a significant degree of subjectivity, since many of the inputs are based on judgement. However, the realization that PSA provides an ideal

framework for addressing uncertainties and for highlighting the areas of subjectivity while providing significant insights into contributors to risk has led to an increased acceptance of PSA as a regulatory tool. The post accident investigation of the 1979 accident at TMI 2 in the USA provided the impetus for increased use of PSA techniques and risk based information for operational safety decisions in the nuclear industry and at the Nuclear Regulatory Commission. Simultaneously, an enormous shift was already taking place in many other countries towards the performance of plant specific PSAs to systematically examine the plant/containment performance, and to identify plant specific vulnerabilities to severe accidents. The use of the PSA is now an integral part of the safety analysis report (SAR) in a number of countries. In the UK this requirement was included for the licensing of Sizewell B and is a requirement for the SAR in the Ukraine. The US NRC has also fully recognized that PSA has a role in the licensing and regulatory process with the issuance of its PRA Policy Statement, and more recently the Regulatory Guide 1.174 [98] and its associated Standard Review Plan Chapter.

The point has now been reached where a large number of PSAs have been completed in many countries for plants of varying designs and vintages. As risk assessment methods have been developed and applied, their strengths and weaknesses have become relatively well appreciated. In addition, applications of PSA have spread to include the most important areas of reactor safety encompassing the design, operation, and regulatory oversights. The continuous advancement in development of realistic risk assessment methods and increased experience based on plant specific PSAs provide impetus for a systematic approach to integrating risk concepts into regulatory evaluation, operational safety assessment, and decision making. Risk concepts are being incorporated into regulations being promulgated in various countries for various industrial activities.

However, for a number of reasons, including a recognition of the lack of completeness in scope of coverage and a lack of standardization of PSA methods, PSAs are still primarily seen as an element for decision making, rather than the primary tool for decision making.

4.1.2. Risk informed regulation

The process of regulation of nuclear power plants differs considerably from country to country. It encompasses the establishment of legal, design, and operating requirements; inspection and enforcement activities; and performance assessment. Incorporating risk concepts into the regulatory process can range from simply using probabilistic considerations implicitly in the establishment of traditional deterministic requirements to an intensive use of probabilistic safety and risk analysis results to optimize regulatory attention, enforce regulatory requirements and for a more efficient utilization of resources to enhance safety improvements by licensees. Indeed, several years ago, the concept of risk based regulation, in which risk arguments played a dominant role, was promoted. Neither of these extremes is now considered to be the optimal approach. Instead, a consensus appears to be emerging that PSA methods be used to complement rather than replace the traditional approaches to regulation. This is normally referred to as *risk informed regulation*. In the remainder of this section, it is the use of PSA in a risk informed regulatory framework that will be addressed.

Most current regulations have been devised without explicit consideration of risk importance of the contributors. Instead, as discussed above, the existing regulations have been developed based on a relatively ad hoc qualitative perception of important contributors, using

subjective engineering judgement with a large degree of conservatisms built into the deterministic regulatory requirements. What sets apart the concept of risk informed regulation from the existing approach is its explicit use of PSAs. The general objective of risk informed regulation is to focus regulatory attention in a manner that is consistent with the risk importance of the equipment and the events and procedures to which the requirements apply, so that regulatory and licensee resources are used in the most efficient way when making decisions on ensuring the health and safety of the public. The objective implies that the regulatory requirements be commensurate with the risk contribution (i.e. regulations should be more stringent for risk important contributors, and less stringent for risk unimportant contributors). Therefore, provided risk informed regulatory criteria are appropriately developed, a systematic and efficient expenditure of resources is to be expected, while simultaneously, a balance in overall safety can be achieved for the nuclear power plant. These objectives would further strengthen the traditional multi-barrier (i.e. "defence in depth") safety philosophy and provide a quantitative means of demonstrating compliance (or degree of non-compliance) with regulations [99].

4.1.3. Use of PSAs in regulatory decision making

If the regulatory framework is to be modified to include risk insights in a formal way, then a process by which this is to be achieved has to be established. The precise way in which PSA insights are used will vary from country to country, depending on the overall nuclear regulatory philosophy, approach, policy making and legal structure. While it is up to each regulatory body to establish its own approach, it is necessary that the implementation process be clear and allow for interaction between the regulatory organization and the licensees while yet maintaining a clear line of separation and independence.

However, if the results of the PSA are to be used, it will be necessary to formulate some form of acceptance criteria related to PSA results. In this report, we will refer to these acceptance criteria generically as probabilistic safety criteria (PSC), which are defined not only by the numerical values specified, but also by the method of comparison with the PSA results and the decision rule. These PSC will vary from country to country and from application to application, and they may take the form of soft reference points, or hard criteria. This is discussed further in Section 5.

In order to be useful as a regulatory tool however, PSA models will have to meet certain requirements which will vary with the role played by PSA results in the regulatory decision making. This is addressed in the following Section.

4.2. Risk informed regulatory decision making

4.2.1. PSA requirements for regulatory decision making

PSA models may be used by the regulator or by the licensee. In either case, when PSA models are used in regulatory applications, the analyses will need to be presented in such a way that they can be reviewed, and the basis for decisions will be explicit. This entails certain requirements on the performance of the PSA model. Although the requirements set by different regulatory bodies may vary in their detail, they can be specified in a general way. The overriding requirement is that the quality of the PSA should be consistent and commensurate with the intended application and usage of these studies in the nuclear regulatory decision

making process, as described in IAEA-TECDOC-740 [100]. The following paragraphs discuss the general PSA requirements.

PSA scope

The scope of the PSA, in terms of the coverage of the contributors to risk must be sufficient for the proposed applications. For instance, a PSA limited to internal events could be sufficient for some issues but it has limited utility for evaluation of regulatory issues related to externally initiated events (e.g. external floods, seismic events). However, even when the scope does not address all initiating events and operational modes, information from the PSA may still provide risk informed support for decision making in a qualitative sense.

Technical quality of PSA

To the extent possible, plant specific PSAs used within the regulatory process should be based on state of the art, "best-estimate" models, assumptions and data. The PSAs should avoid conservative/bounding models, assumptions and data, or the influence that such conservatisms have on the results should be understood.

Plant specific versus generic

The use of generic PSA studies might introduce additional uncertainties in the decision process. Generic PSA models can be used only when a high degree of standardization in design and operation exists, or when the issue concerned is insensitive to plant specific considerations. For most practical applications, plant specific issues can only be resolved with a high degree of confidence when the PSA studies are based on as designed, as constructed, and as operated plant conditions (i.e. a plant specific PSA). If a plant specific study is not available, the differences between the plant under consideration, and the "generic PSA plant" must be considered as part of the decision process.

Level of detail

When regulatory decisions require high degrees of confidence, they may require detailed PSA models. Use of simplified PSA models may, however, be acceptable for certain decisions. As a general rule, however, the PSA model should be developed to a level of detail such that dependencies and failure modes applicable to the decision are adequately modelled. It should be detailed enough to contain elements that can be used to support the regulatory decision. For example, if the decision is associated with inspection, the issues to be inspected should be represented in the model. As another example, if the decision is dependent on assessing the impact of a change to the plant operation or design, there has to be some way of modelling the impact of the change by, for example, making modifications to the probabilities associated with the basic events of the PSA model, or by making modifications to the logic model structure.

Living/current nature of models

The PSA models need to be updated, so that the models are an adequate representation of the as operated plant conditions. Update and Living PSA requirements differ from one country to another. Here again, the regulatory/safety issue that is being considered must be unaffected by the dated nature of any specific PSA models. Therefore, for each new regulatory

application, the PSA models should be updated to be representative of the latest plant configuration and conditions. This will provide additional confidence for the regulatory decision process.

PSA documentation

PSA models are developed on the basis of many assumptions and approximations, some of which may have a significant effect on the answers. It is important that these be documented clearly. In addition, it is important that the overall documentation of the PSA be well structured so that if modifications are to be made to model the impact of some change for example, the modifications are made at all appropriate places in the model.

Presentation of analysis results

The regulatory decision analysis results should be presented in a transparent and traceable fashion, listing all of the assumptions, limitations and sources of information supporting the decision making process. The different decision options must show compliance with any existing acceptance criteria or regulatory requirements. The robustness of the decision with respect to the analytical uncertainties must be demonstrated. If possible, the attendant uncertainties should be quantified; however, as a minimum, the sensitivity of the decision outcome to the variability in the data, models, and assumptions needs to be demonstrated. All relevant information should be documented. The information needs to be synthesized and summarized in a manner that makes it useful for the decision making process.

4.2.2. Regulatory decisions

Regulatory decisions can be characterized by issues that lead to permanent changes in plant operations, design, or regulatory practices for which immediate decisions are not required, as opposed to decisions on temporary conditions that require interim shorter term actions. The longer term regulatory decisions are less constrained by time than interim regulatory decisions, which may be required within a short time scale.

Longer term regulatory decisions

Longer term regulatory decisions are typically free from major time constraints. This allows for detailed and sophisticated probabilistic and deterministic analyses, considering all of the relevant decision attributes, with appropriate time for feedback from the different parts of the regulatory organization and licensee, if such analyses are required. Some of the longer term decisions might be aimed at reducing the need for interim decisions.

Longer term decisions might often entail “permanent” changes in plant design, procedures, technical specifications, etc. and might therefore, as in the case of backfit considerations, be influenced by cost/benefit considerations, taking into account all relevant factors including the residual plant life expectancy. These regulatory decisions might also have generic, industrywide implications.

Examples of specific regulatory areas where longer term risk informed methods and requirements are applicable include:

- Evaluation of design and procedural adequacy.
- Performance of periodic safety reviews.
- Assessment of changes to the licensing basis, e.g.
  - Technical specification optimization: STIs, AOTs, LCOs.
  - Quality assurance for operation, maintenance and support activities.
  - Graded QA.
- Assessment of operational practices on safety:
  - Plant systems configuration management.
  - Preventive and corrective maintenance prioritization and optimization.
- Inspection activities support:
  - Inspection prioritization.
  - Inspection findings evaluation.
- Investigation of ageing effects:
  - Ageing effects evaluation and assessment.
  - Ageing effects management.
- Assessment of risk based performance indicators.

Interim regulatory decisions

In some cases, regulatory organizations need to implement interim decisions in order to temporarily alleviate a regulatory concern, while a longer term solutions can be evaluated. For these interim decisions, few plant specific analyses may be available, and therefore, the available information (that sometimes may not even be specific to the plant under consideration) would have to be relied on to achieve a short term resolution of the concern. PSA insights can provide very useful information to support the decision making process.

The issues that require an interim decision are typically operational and procedural in nature, and can sometimes be evaluated with plant specific PSAs, if available, or addressed more generically with due caution using the information gained from other recent PSAs for similar plants.

Since the questions that require short term regulatory decisions are often related to operational management, it might be useful to have a qualified detailed, Living PSA as an online monitor of plant safety. In some countries, however, regulators have expressed strong reservations about the use of risk monitors.

The PSA requirements described in Section 4.2.1 are also applicable for a PSA to be used to support interim regulatory decisions. However, since the interim decisions are anticipated to be less challenging, it is to be expected that the results of the PSA can provide sufficient insights to address the issue and support the qualitative regulatory arguments, and that a full quantification to assess the decision attributes and their implications may not be required. Requirements on PSA for use in safety and regulatory decision making are also described in IAEA-TECDOC-740 [100], in IAEA-TECDOC-1106 [2] and in earlier sections of this report.

Typical issues that can require an interim regulatory decision for which PSA can provide input include:

- The need for regulatory action in response to an event at a plant.
- One-time exemptions from technical specifications and other licensing requirements.
- Temporary modifications to hardware configuration and/or procedures.

4.2.3. PSA uncertainties

One of the issues that must be faced is how to deal with uncertainties in PSA results. Typically, PSA results show relatively large uncertainties ranging over several decades. Due to these large uncertainties, the use of a single point estimate, a mean, or a median value alone can lead to a less informed decision. Therefore, the decision process must account for PSA uncertainties. Use of probabilistic based analyses for operational safety decisions requires an adequate degree of confidence by the decision maker as to the validity and robustness of the results. While there are also uncertainties in the deterministic approaches it has been customary to deal with them by adopting conservative approaches such as relying on safety margins and defence in depth. The use of PSA is intended to make the regulatory approach somewhat more realistic by providing a basis for prioritization of issues. PSA, because it provides a framework for assessing the impact of uncertainties on decisions, allows a rational approach to dealing with uncertainty.

The uncertainties associated with estimation of the core damage profile in nuclear power plants result from the uncertainties in failure data (independent and common cause), success criteria, component fragilities, external events loads (seismic and fire loads), and modelling uncertainties. Most PSAs model the effect of data uncertainties, seismic and fire loads and fragilities. However, the uncertainties associated with the thermal-hydraulic success criteria and the modelling issues are typically not quantified. Uncertainties associated with modelling issues are dealt with by making specific assumptions or adopting specific models.

In developing an approach to decision making to take into account these uncertainties, various decisions have to be made. Firstly, it has to be decided how the numerical results are to be compared with any acceptance guidelines, i.e. whether to use the mean value of the probability distribution on the numerical result to compare with a guideline, or whether to compare some percentile of that distribution. The decision on which measure to use cannot be separated from the establishment of the guidelines. This is discussed in somewhat more detail in Section 5. Furthermore, recognizing that not all the uncertainties are represented in the probability distribution, a decision has to be made on how to handle these issues. There are at least two alternatives. The first is to adopt a standard accepted approach that specifies what assumptions and models are acceptable. The second is to allow a variety of models and assumptions, but require that alternates be considered by performing sensitivity analyses to determine whether the decision would change if alternates were used. The decision would then be made by assessing the relative credibility of those alternatives that lead to differing decisions. The approach adopted for dealing with uncertainty will differ from country to country.

4.3. PSA training for regulatory staff

If PSAs are to become part of the regulatory framework, the regulatory authorities need to generate an overall policy on the use of PSA within this framework that is consistent

with their national nuclear safety policy. This is necessary to ensure a smooth, consistent and efficient transition from the traditional deterministic framework to a risk informed approach.

To fully implement and integrate the PSA process into the existing licensing and regulatory framework, the regulatory authorities need to promote PSA technology and to foster the exchange of experience and communication between PSA specialists, non-PSA engineers, and the regulatory staff responsible for inspection and enforcement. This will reduce the potential for misunderstanding and resistance to change. It will also help to focus attention more closely on safety enhancements and the efficient utilization of safety resources.

The regulatory authorities should, if feasible, have staff with sufficient understanding of the underlying PSA methodological framework. Therefore, it is advisable to have at least one PSA expert on the staff of the regulatory body, regardless of its size and organizational structure.

Furthermore, staff in other technical areas also need to have an understanding of the key elements of the PSA process. Therefore, the regulatory authorities need to provide an adequate degree of training for their responsible non-PSA staff members to have a common basis for communication and understanding of the vulnerabilities and strengths that the PSA process elicits.

Therefore, training programmes that include both fundamental and practical aspects of PSA need to be established for non-PSA regulatory staff both at the management level and at the level of the engineers responsible for decision making. These training programmes need to be tailored for the specific needs of the authorities. Ideally they should be a mandatory element of the technical enhancement programme.

The training staff, who should have practical experience within the authorities' PSA team (if available) or at a supporting organization, would need to have well defined and achievable objectives.

Periodic seminars to cover the various safety issues and their significance based on PSA insights would be useful to develop a balanced perspective of the importance of the issues to the overall plant safety. A further aim of such seminars would be to foster mutual understanding, to enhance communication and to promote risk informed skills within regulatory organizations.

Important findings based on plant specific PSAs should be shared with other non-PSA specialists within the regulatory organization. Workshops on PSA related inspection findings and precursor event analysis would reinforce the credibility of the risk informed regulatory implementation process. It would be also worthwhile to develop additional expertise in PSA technology by training selected individuals to become PSA experts.

A comprehensive training programme on regulatory uses of PSA should take into consideration the latest information available in the field and also include exchange of experiences among different regulatory organizations. International training courses could become excellent mechanisms for spreading and promoting the concept of risk informed regulation.

5. NUMERICAL GOALS AND ACCEPTANCE CRITERIA FOR USE IN DECISION MAKING

5.1. Introduction

5.1.1. The need for probabilistic safety criteria

If PSA results are to be used in a formal way for decision making, then it is necessary to establish a formal process for using those results. The details of this process will depend on the purpose of the particular PSA application, the nature of the decision, and the PSA results to be used. When the numerical results of the PSA are to be used, it will often be necessary to establish some reference value with which those results can be compared, as well as a rule, or rules, for how to interpret the results of the comparison. Where the application is directed towards the identification of the dominant contributors to risk or the optimization (minimum risk) among various design options, plant configurations, testing strategies, etc., there may be no need for a reference value at all. Such uses of PSA, depending only on a relative ranking of values, are often claimed to be the most robust. However, where the application involves judging whether a calculated risk value is acceptable, assessing the acceptability of a proposed change to the plant that would produce a calculated increase in risk, or assessing the need for a change in design or operational practices to reduce the level of risk, then a judgement on the significance of the calculated value can only be made by comparing it with some reference value. In the remainder of this Section, these reference values and their associated rules will be called probabilistic safety criteria (PSC), but it is to be understood that the meaning of the numerical value of the PSC and the decision making rule itself will depend very much on its use.

The term “criterion” often has the connotation of a fairly clear cut rule for making decisions. A criterion may, for example, delineate the region of acceptability from that of unacceptability. Since the numerical estimations of risk from a PSA have substantial uncertainty, being an amalgam of many subjective judgements, and perhaps because the concept of risk itself is open to interpretation, many people do not feel comfortable comparing the numerical predictions of PSAs to a fixed criterion or goal. More than thirty years ago, it was observed that, “In general, licensing authorities are reluctant to commit themselves to specific quantitative criteria for safety which relate the risk of a particular fault to its consequences” [101], and this is still broadly true today, not only for the licensing authorities but also for many sections of the industry.

While there are a few countries that have adopted PSC as clear cut decision criteria, it is more usual to find PSC identified as *targets, goals, objectives, guidelines* or *reference values for orientation,* with a somewhat fuzzy decision making rule. A target, goal or objective is something to be strived for. It does not necessarily imply that if it has not been met, then the activity being assessed is unacceptable. The US NRC safety goals [102], for example, are, in fact, lower bounds in the sense that they indicate where no further improvement is necessary (although it is not discouraged), but they are not used to identify when the risk is unacceptable.

5.1.2. Comparison of numerical results with PSC

Regardless of whether the PSC represent criteria, goals, or guidelines, a comparison of the corresponding calculated value obtained from the PSA will be an essential part of the decision making process. Thus, it is necessary to specify how this comparison is to be made. One of the complicating factors is the aforementioned uncertainty associated with the PSA results. In the absence of uncertainties, the decision rules would typically take the form:

If the PSA result X is greater (or less) than reference value Y, do Z.

However, given that there is uncertainty, the rules should look a little different. First, it is necessary to understand how the uncertainty in the PSA result is to be characterized. This is typically done by evaluating a probability distribution on the result, whose percentiles, roughly speaking, represent confidence bounds on the result. If this is the case, then it must be decided how to compare that distribution with the criterion or guideline. The rules could be set to look like:

If the mean value (or any other measure of central tendency) of X is greater (or less) than reference value Y, do Z.

Alternatively they could be set up to read:

Do Z, if the probability *that X is greater (or less) than Y is greater than or equal to* α *(or X is greater (or less) than Y at a confidence level* α*).*

It is clear that the reference values associated with the PSC cannot be chosen independently of the comparison algorithm, since choosing to compare at a high confidence level rather than the mean value would typically be a more stringent test for a fixed reference value. In many cases, however, the definitions of the PSC are rather imprecise with respect to this issue, as will be seen in the discussion in Section 5.3.

5.1.3. Long term and short term risk measures

The PSA applications described in Section 3 are broadly of two types: those where the PSA gives a long term average risk value, and those giving instantaneous or short term risk measures. The former covers applications where the interest is in the permanent status of the plant, such as design or backfit options, periodic safety reviews or graded QA. Such a PSA incorporates a representation of the expected equipment outages for preventative and corrective maintenance, testing and inspection averaged out over a year. The latter covers applications where the interest is in controlling the risk from temporary plant configurations. PSAs used for these applications are required to have the capability for turning components on and off as required.

5.1.4. Summary

The PSA applications for which numerical acceptance guidelines or criteria are required are those that are associated with measures of the overall risk or to changes in those measures resulting from changes to the design or operational practices of the plant. The

process associated with assessing the significance of a change to the plant design or operation requires the following aspects to be addressed:

- evaluation of the risk impact of the change in terms of a suitable measure
- establishment of a PSC for that measure
- comparison of the measure with the PSC and use of the results in a decision process.

In Section 5.2 the commonly used risk measures are discussed, followed, in Section 5.3, by a discussion of a number of PSC that have been adopted, and, in Section 5.4, by a discussion of the role of PSA in decision making. Section 5.5 addresses PSC for the applications discussed in Section 3 of this report.

5.2. Risk measures for use in decision making

This section discusses the potential risk measures commonly used in analyses. The decision making process itself is discussed in Section 5.4.

Taking into account the different possible uses of PSA in decision making, the following types of risk measures are most commonly used (using the term risk in a rather broad sense), i.e. average risk measures, instantaneous risk measures, differential risk measures, and importance measures. Each is discussed below.

5.2.1. Absolute time averaged risk measures

The original, and still the most common purpose of a PSA is to calculate the average risk from a plant as a demonstration of its overall safety, and this type of usage has become incorporated, formally or informally, into the regulatory process in many countries. These measures relate to the existing state of the plant (either before or after the change). A PSA will yield numerical measures of risk at various levels according to the level of consequences calculated in the PSA, and criteria may be set in relation to any or all of the following:

- the unreliability or unavailability of particular safety systems/functions (Level 0)
- the frequency of core damage (Level 1)
- the frequencies of radioactive releases and their associated magnitudes (Level 2)
- the frequency of specified public health effects (Level 3).

Safety system/function unreliability or unavailability

One system may perform several different functions (e.g. the RHR system in a BWR can be used in several modes, including suppression pool cooling, containment spray, shutdown cooling), and therefore for each system there can be several measures associated with its unreliability or unavailability. Care has to be taken to specify the boundary conditions under which the measure is evaluated. For example, the unavailability can be evaluated under the assumption that the support systems are operational, or the failures of support systems can be included in the evaluation.

Core damage frequency (CDF)

Core damage frequency[2] is by far the most common measure of risk in use worldwide, since the majority of NPPs have performed at least a Level 1 PSA, and also because for light water reactors (LWRs) there is a reasonable consistency in the definition of core damage.

Frequency of radioactive release

There are differences in the approach used to characterize a release. It has been specified in various ways, such as in terms of absolute quantities (in Bq) of the most significant nuclides, their fractions of the core inventory, a specified dose to the most exposed person, as giving "unacceptable consequences", or simply left undefined [103, 104].

The large releases are of most interest. While there may not be consensus on how to define a large release, a common thread is that a large release is one that has severe implications for society, with the off-site emergency plan put into effect and predictions of perhaps one prompt death and multiple fatal cancers. It would follow from severe core damage together with a major failure of the containment. Where Cs-137 has been specified as one of the relevant nuclides, this reflects a concern for land contamination, in addition to the direct heath effects. Sometimes the term may refer only to a large *early* release, with the implication that a late failure of the containment may be averted by accident management measures. The large early release frequency (LERF) has been used as a surrogate for the risk of early fatalities [98].

Measures of public health effects

When a Level 3 PSA exists, it can be used to express the risk in terms of the impact on the public, for example as a curve of the probability of exceedance of the number of fatalities or latent cancers per year. Summary measures of risk such as the expected number of fatalities, or the risk to an individual at the site boundary are also evaluated.

Societal effects

Again, a Level 3 PSA can be used to provide estimates of the risk to society in terms of the frequency of land contamination and other such measures.

5.2.2. Instantaneous measures of risk

Any of the measures discussed above can also be evaluated subject to a specific set of boundary conditions, yielding a conditional measure, which is sometimes referred to as an instantaneous measure of risk. Perhaps the most commonly seen are those related to CDF and LERF.

[2] Core damage is defined as resulting from accidents involving loss of adequate cooling (either due to an undercooling or over power event) to reactor fuel elements up to an including major damage to a reactor core with internal release of fission products, but not necessarily involving a release into the environment (loss of containment integrity).

Instantaneous CDF

The most commonly used instantaneous measures of risk are related to core damage frequency. This is a function of the specific plant configuration, of course, but also of the time elapsed since the last test of each of the safety systems. In general, PSAs (on-line or off-line) do not include a time dependent model for system reliability, and therefore take no account of the time since the last test. The calculated CDF is thus not strictly an instantaneous value, though it is still usually referred to as such, but more like an average over the duration of a particular plant configuration. This gives a histogram-like pattern of CDF with time, compared with the sawtooth pattern given by a time dependent model. Clearly, any criterion for the maximum instantaneous CDF must state which type it refers to.

Core damage probability (CDP)

Another commonly used measure is the integral of CDF over some interval. This is sometimes referred to as the core damage probability (CDP).

Instantaneous measures of LERF and large early release probability (LERP) are defined in an analogous manner.

5.2.3. Differential measures

Often useful to measure directly the impact of proposed changes. This can be done for any of the measures discussed in Section 5.2.1. They may be expressed in absolute terms, or as fractions or percentages.

5.2.4. Importance measures

A number of PSA applications make use of the importance factors from a standard Level 1 PSA, along with qualitative engineering judgements, to determine the risk or safety significance of components. Importance measures essentially allow the analyst to measure such things as the contribution a component unavailability makes to one of the measures discussed above, or how much the measure would change if the unavailability were taken to some other value, such as 0 or 1.

There are several importance measures having different characteristics. They include:

- Fussell-Vesely (FV);
- Birnbaum;
- Risk reduction worth (RRW);
- Risk achievement worth (RAW);
- Criticality importance;
- Upgrading function.

Commonly used importance measures are defined in Ref. [105].

5.3. Types of decisions and associated PSC

Different PSC are adopted for different decisions. As discussed earlier, the PSC is specified not only by the numerical values proposed — it is also necessary to specify what value, calculated from the PSA, should be used for comparison purposes, and to indicate how to interpret the results of the comparison. As an example, when specifying the safety goals in its Safety Goal Policy, the US NRC specified that it was the mean values estimated from the PSA that were to be compared with the goals, that all contributions to risk were to be considered and that meeting the goal means that the plants are safe enough. In this section, some of the proposed PSC are discussed.

5.3.1. PSC on average risk measures

Typically PSC on average risk measures have either been defined as targets, goals, or objectives, or they have been defined as limit values that are not to be exceeded. IAEA Safety Series No. 106 [103] in fact recommended a framework for PSC in which both concepts are present, with an upper level (or fuzzy zone) representing the threshold of intolerability and a lower one representing the design target or objective. Between these two levels is a region of conditional acceptability where all reasonably practicable measures should be taken to reduce risk. Below the target level, there would be no further pressure from the regulatory body to reduce the risk, although of course the designer or operator may choose to do so. It was pointed out that with such a framework there is no need to define separate levels for old and new plants; the old plants would be expected to be somewhere in the middle region while new plants would be near or below the target. An IAEA Technical Committee Meeting on the Use of Probabilistic Safety Assessment in the Regulatory Process, held in Vienna in December 1994 re-affirmed its support for such a two tier framework, although at present it appears that it is formally adopted in only one member country [106]. The basic idea behind it does, however, appear to be in more widespread use. In the Netherlands, this two tier approach was initially adopted, but, afterwards, the lower limit was removed and replaced by a requirement to reduce risk via the ALARA/ALARP principles. The following paragraphs discuss some of the better known PSC.

PSC for safety system/function unreliability or unavailability

Most designers and regulators would expect the unavailability of a well engineered, non-diverse but redundant, safety system to be in the range 1E-3 failures per demand (f/d) to 1E-4 f/d, and this could be regarded as a very informal guideline. It is therefore not surprising that, when PSC have been established for system unavailabilities, the numerical values have typically been set at around 1E-3 to 1E-4 f/d. PSC for the main safety systems have been set in some countries, e.g. Canada, Finland and Slovakia. There are also a few examples of ad hoc PSC being introduced to address particular safety issues; e.g. 1E-4 f/d for AFWS in the USA.

To complete the definition of the PSC, the rule for comparison has to be specified. The PSC might be a design goal or something that should be striven for, but, as in the case of the Finnish PSC, it might also be a criterion that has to be satisfied for acceptability. Most often it is the mean value or the best estimate that is prescribed as the value to be used in the comparison. However, in the Finnish case, it has to be demonstrated that the criterion has been met with a 90% confidence [104], thus making this PSC a more stringent one.

There are complications in specifying PSC at this level other than in relation to a specific plant design due to differing requirements for a particular system to respond to different faults: most countries have preferred to exercise control at the CDF level. Furthermore, as discussed above, care would have to be taken to specify the boundary conditions under which the measure is evaluated. For example, the unavailability could be evaluated under the assumption that the support systems are operational, or the failures of support systems could be included in the evaluation.

No examples of PSC at the *safety function* level have been found.

PSC for CDF

The best known example of PSC for CDF is the set of objectives put forward by INSAG in 1988 — a CDF of 1E-4/year for existing plants and 1E-5/year for future designs [107]. These values are widely used as objectives, formally and informally, in many countries. There are some regulators, however, that feel that a CDF above 1E-4/year would signal a need for action to reduce the risk, and in this way treat the PSC in fact more like a limit. In two countries (Netherlands and UK) the 1E-4/year value is in fact a formal limit, and in the UK 1E-5/year is regarded as the objective for old or new plants. The latter value was suggested as the target frequency for core damage in the IAEA Safety Series No. 106 [103]. In evaluating the CDF for comparison with these values, there is no requirement to address uncertainty in a formal way; the values are expected to be best estimates.

While not adopted as a formal goal, the value of 1E-04/reactor year has been adopted as a subsidiary objective of the US NRC's Safety Goal Policy Statement, and is a goal in the sense that it relates to the decision of how safe is safe enough. The safety goal policy statement is explicit in saying that it is the mean value of the probability distribution on CDF that should be used in the comparison, and further, that all contributions to risk, with the exclusion of sabotage and offsite fuel handling accidents, should be considered.

The US nuclear industry has set a design criterion of CDF < 1E-5/year for the advanced LWRs, but the purpose of this is to protect investment. It is not a safety criterion.

In the Swiss regulatory framework, the CDF of 1E-4/year is proposed as a limit with the requirement that it be met at the 95th percentile [97, 108].

Care must be taken when comparing quoted values of CDF criteria as they may be referring to different scopes of PSA (e.g. no external events, no accident management measures) or to compliance at a specified confidence level.

PSC for large release frequency

With respect to the frequency of the large release, the figures proposed as objectives by INSAG are an order of magnitude less than those for core damage, i.e. 1E-5/year for existing plants and 1E-6/year for future plants [107]. The latter figure (1E-6/year) is suggested in the IAEA Safety Series No. 106 [103] as a target for either, this being the value adopted in France and the UK, and proposed in the USA at the time. Since then, the UK has specified an objective of 1E-7/year (as a challenge for future plant) but with a limit of 1E-5/year [106]. Some countries give the target frequency as a fraction of the CDF (e.g. 5%, 10%), implying a target for containment failure probability, given core damage.

The US industry has set a criterion for its ALWRs that releases giving a dose greater than 0.25Sv at the site boundary should have a cumulative frequency of less than 1E-6/year. This is reckoned to provide a considerable margin to the US NRC's safety goals. Unlike their CDF criterion, this is a PSC intended as part of the justification that these advanced designs will have an improved level of safety.

Other example is the acceptance criterion for nuclear plants established by the Argentine regulatory authority. The criteria is expressed in the form of two curves (one for the public and one for NPP workers). These curves plot the yearly probability of accident sequences against the effective dose. The areas under the curves are the acceptable regions [109].

Goals for public health effects

Goals for public health effects had been developed in only a few countries. In spite of some superficial resemblances, there are so many differences between these examples, in their concepts, definitions and numbers, that it is difficult to find any common threads, or even to make a sensible comparison. PSC at this level may be used in licensing, but are, however, hardly ever used in connection with any PSA application and therefore need not be discussed any further in this report. Some details in this regard can be found in Refs [114] and [110].

5.3.2. PSC associated with the evaluation of changes to plant design or operational practices

Examples

The examples in this section come from the United States, the first being that incorporated in Regulatory Guide RG 1.174 [98], the second being the proposal from the Electric Power Research Institute (EPRI). It is worth mentioning that both examples allow for the change to lead to an increase in risk.

PSC based on absolute measures

The US NRC has adopted PSC for assessing changes. The Regulatory Analysis Guidelines [111] have established PSC for the US NRC staff to use as input to their assessment of the requirement for backfitting.

Recently, in regulatory guide RG 1.174 [98], PSC have been established that can be used to justify changes to a plant's licensing basis taking into consideration the impact on plant risk to assess when changes in plant risk might be acceptable. They are structured as set forth below.

Regions are established in the two planes generated by a measure of the baseline risk metric (CDF or LERF) along the x-axis, and the change in those metrics (ΔCDF or ΔLERF) along the y-axis (Figures 2 and 3), and acceptance guidelines are established for each region as discussed below. These guidelines are intended for comparison with a full scope assessment of the change in risk metric (including internal events, external events, full power, low power and shutdown), and, when necessary, the baseline value of the risk metric (CDF or LERF) as discussed below. However, it is recognized that many PSAs are not full scope and

the use of less than full scope PSA information may be acceptable when supplemented by qualitative arguments, bounding analyses or well chosen sensitivity studies.

There are two acceptance guidelines, one for CDF and one for LERF, *both* of which should be used.

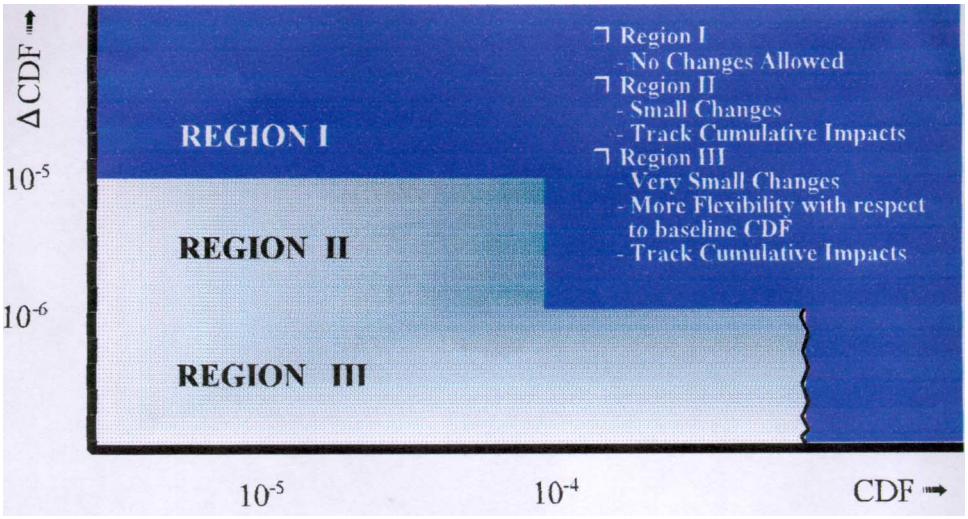

FIG. 2. Acceptance guidelines for CDF.

The guidelines for CDF are (see Fig. 2):

- If the application can be clearly shown to result in a decrease in CDF, the change will be considered to have satisfied the relevant principle of risk informed regulation with respect to CDF. (Because Fig. 2 is drawn on a logarithmic scale, this region is not explicitly indicated in the figure.)

- When the calculated increase in CDF is very small, (less than 1E-6 per reactor year), the change will be considered regardless of whether there is a calculation of the total CDF (Region III). While there is no requirement to calculate the total CDF, should there be an indication that the CDF may be considerably higher than 1E-4 per reactor year, the focus should be on finding ways to decrease rather than increase it. Such an indication would result, for example, if: (1) the contribution to CDF calculated from a limited scope analysis, such as the IPE, and, if appropriate the IPEEE, significantly exceeds 1E-4; (2) there has been an identification of a potential vulnerability from a margins type analysis; or (3) historical experience at the plant in question has indicated a potential safety concern.

- When the calculated increase in CDF is in the range of 1E-6 per reactor year to 1E-5 per reactor year, applications will be considered only if it can be reasonably shown that the total CDF is less than 1E-4 per reactor year (Region II).

- Applications which result in increases to CDF above 1E-5 per reactor year (Region I) would not normally be considered.

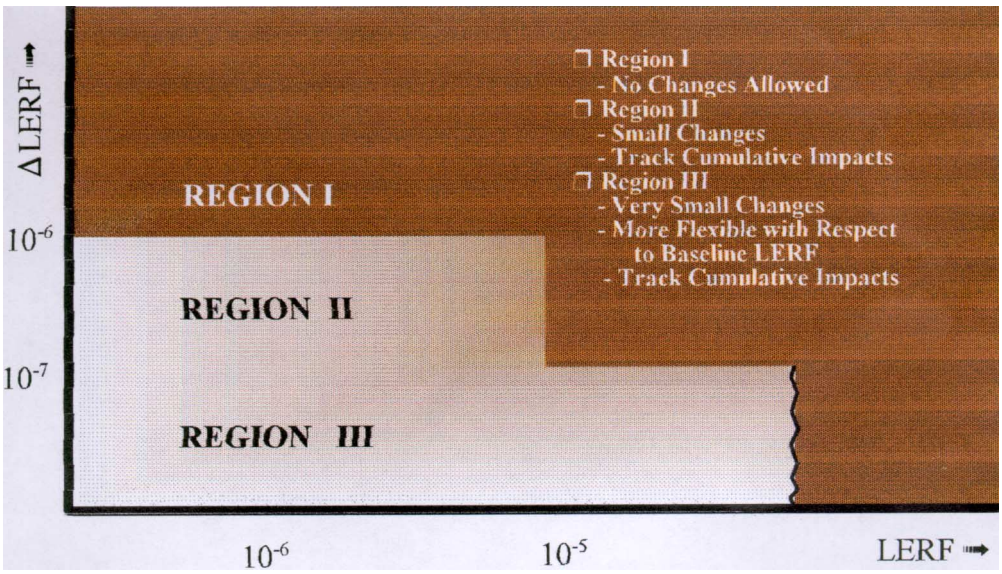

FIG. 3. Acceptance guidelines for large early release frequency (LERF).

AND

The guidelines for LERF are (see Fig. 3):

- If the application can be clearly shown to result in a decrease in LERF, the change will be considered to have satisfied the relevant principle of risk informed regulation with respect to LERF. (Because Figure 3 is drawn with a logarithmic scale, this region is not explicitly indicated in the figure).

- When the calculated increase in LERF is very small, (less than 1E-7 per reactor year) the change will be considered regardless of whether there is a calculation of the total LERF (Region III). While there is no requirement to calculate the total LERF, should there be an indication that the LERF may be considerably higher than 1E-5 per reactor year, the focus should be on finding ways to decrease rather than increase it. Such an indication would result, for example, if: (1) the contribution to LERF calculated from a limited scope analysis, such as that the IPE, and, if appropriate the IPEEE, significantly exceeds 1E-5; (2) there has been an identification of a potential vulnerability from a margins type analysis; or (3) historical experience at the plant in question has indicated a potential safety concern.

- When the calculated increase in LERF is in the range of 1E-7 per reactor year to 1E-6 per reactor year, applications will be considered only if it can be reasonably shown that the total LERF is less than 1E-5 per reactor year (Region II).

- Applications which result in increases to LERF above 1E-6 per reactor year (Region I) would not normally be considered.

These guidelines are intended to provide assurance that proposed increases in CDF and LERF are small and are consistent with the intent of the Commission's Safety Goal Policy Statement.

As can be seen, these criteria are quite complex in their structure. The regulatory guide further specifies that the acceptance guidelines are to be compared to mean values. However, it is recognized that not all sources of uncertainty are evaluated quantitatively in PSAs. Thus it has been stated as a requirement that the way in which the decision is to be made hinges on whether there are sources of uncertainty that might affect the decision.

PSC based on relative measures

The PSC proposed in the EPRI PSA Applications Guide [4] were constructed as quantitative screening criteria, which are used to determine whether a proposed change is unacceptable, requires further evaluation, or is non-risk significant, based on the fractional increase in CDF (or LERF), the boundaries between the regions being dependent on the baseline values of CDF (or LERF). It is specified that the values to be used should be best estimates or mean values.

PSC associated with temporary changes to plant design or operation

The previous PSC were intended for assessing the acceptability of, or, in the case of backfit, the need for, a permanent change to the plant. Other criteria are required for assessing the acceptability of temporary changes.

Limits on conditional measures of risk

The instantaneous CDF will vary above and below the average CDF and there is some concern that its value should not become unduly high for any configuration that is permitted under the TS. Criteria for the average CDF may be related ultimately, at least in principle, to average non-nuclear risks such as fatalities due to cancer or to accidents, for which statistics are available. It is apparent that qualitative or deterministic controls are exercised on instantaneous risk, but there is no quantified information on the maximum levels which are tolerated by individuals or by society. Thus limiting values for instantaneous CDF are essentially a matter of judgement.

Limiting values for instantaneous CDF may be set as absolute values or in relative terms. In the latter case, they are commonly taken relative to the *baseline CDF* which refers to the state of the plant with all its equipment available (the lowest value). With time dependent reliability modelling, this is not a fixed quantity and therefore a further specification of the baseline has to be made, for example that all systems have just been tested [112]. A significant example of an absolute criterion for instantaneous CDF is a recommendation of EPRI [4] that it should be less than 1E-3/a, and this has been followed in some other countries (e.g. Ref. [113] and paper by J. Suárez and M. Moreno in IAEA-TECDOC-1138 [6]). In the UK, the Nuclear Installations Inspectorate (NII) proposed that the upper limit on average CDF (1E-4/a) should be applied as a criterion for instantaneous CDF, at least for planned operations. As regards relative criteria, at two NPPs in the UK with installed risk monitors, a factor of ten on the baseline CDF triggers a requirement to shut down within three days and a factor of 100 or 300 calls for an immediate controlled shutdown.

Limits on incremental risk

Given that both the average and peak instantaneous CDFs are acceptable, there may still be a wish to put a limit on the added risk contribution due to a particular activity, such as

an equipment outage for repair. This can be measured as the increment in the CDF integrated over the duration of the activity, sometimes referred to as the Conditional Core Damage Probability (CCDP) or ΔCDP. Values of 1E-6 [3], or 1E-7 [114], have been proposed for ΔCDP. This quantity is mainly of interest for the on-line calculation of AOTs by a risk monitor, using a formula such as:

$$AOT \times \Delta CDF = \Delta CDP_{max}$$

where ΔCDF is the anticipated incremental CDF averaged over the duration of the outage, or other activity.

ΔCDP only refers to one activity and there may also be a wish to restrict the cumulative effect of risk increasing activities over a year. There are various ways of controlling this, such as counting the number of times that the risk exceeds a reference value, but perhaps the most straightforward way is to sum the ΔCDPs over the year and to set a limit to the summation. This is then identical to the increment in the average CDF over the year due to such activities.

5.3.3. PSC for categorization

One use of categorization is seen in conjunction with reliability centered maintenance, or with the US Maintenance Rule, under which the SSCs with a high risk significance should be identified so that they can be subjected to a programme of enhanced monitoring. An example of criteria for selecting risk significant SSCs, involving risk reduction worth (RRW) and risk achievement worth (RAW), is given in the paper by A. Rodríguez and R. Camargo in Ref. [6], and the experience in France is referred to in Section 3.2.1.2 above.

At the other end of the scale, there is a desire to reduce the burden of ongoing programmes, such as QA, in-service testing, and in-service inspection by reducing requirements for those components of very low significance to risk. The identification of components as candidates for classification as “low risk significant” can be done using criteria on, e.g. the Fussell-Vesely (FV) and RAW importance factors. EPRI has proposed criteria of FV < 0.005 and RAW < 2 for categorization [4] a programme in Spain [115] is a variation of this, using three categories, high, medium, and low, with the FV criterion for the low category conservatively tightened to FV < 0.001. Since such programmes involve a deliberate, albeit very small, increase in risk, a cautious approach is warranted and the procedure calls for the scrutiny of each item by an expert panel in addition to passing the risk importance criteria.

Reference [105] discusses several issues related to the use of importance measures for categorization, and, in particular, points out that the use of universal screening values for importance measures is not necessarily appropriate, as their implications are different depending on the absolute value of the CDF, LERF, or whatever other measure is being used.

5.4. Decision making process

As discussed in the preceding section, the definition of the PSC should specify how the comparison with the estimate from the PSA should be performed. This comparison is complicated by the uncertainties in PSA results. Furthermore, as indicated, the PSA input is typically only one of many inputs to the decision making process.

There is general agreement that there are substantial uncertainties in any risk measure calculated from a PSA. For most applications, it is left as a general expectation that a decision maker will give less weight to risk values with a larger uncertainty when considering them together with deterministic, engineering and economic evaluations.

With few exceptions [108], it appears to be accepted that the mean value of the risk measure should be compared with the value in the PSC. Whenever a probability distribution has been calculated in the PSA, the mean of this distribution is to be used. Whenever the PSA is a point value calculation, the input data and assumptions should be such that, as well as can be judged, the resulting risk value is a best estimate of the mean.

In the exceptions, the risk value at a specified confidence level is compared with the criterion. In Switzerland, the proposed CDF criterion of 1E-4/year should be met at the 95th percentile [97, 108]. In Finland, compliance with the criteria for safety system reliability has to be shown at the 90th percentile [104]. Such requirements mean, of course, that these criteria are tighter than they appear to be.

The impact of many sources of uncertainty, especially model uncertainty, is not incorporated into the probability distributions that characterize uncertainty, and yet it can be significant. An understanding of these uncertainties and their potential impact on whether the PSC is met should be taken into account when comparing the calculated value with a numerical criterion. Various approaches are available, including the use of bounding analyses and sensitivity studies, although there does not appear to be a generally accepted formal process. Similarly, there does not appear to be a formal process for combining all the different inputs that go into making a decision. However, one tool that has been used is cost benefit analysis (CBA).

Regulatory bodies take cost into account, at least implicitly, once basic standards of safety have been met, when deciding whether to impose further safety requirements, on a plant specific or a generic basis, particularly in respect of backfits to operating plants. It appears, however, that none of them require a utility to carry out a CBA to show that the risk of their proposed new designs or modifications is as low as reasonably achievable (ALARA) or practicable (ALARP) [108, 116]. In some countries there is a requirement for an ALARA or ALARP demonstration, but this may be made in a qualitative or semi-quantitative way, with no specific criteria laid down. A utility may, however, decide to perform a CBA to support its choice of design/backfit option over other more expensive ones.

CBA is related to PSA through the benefit being an expectation value, i.e. multiplied by the probability of it being realized. The benefit of a safety measure under consideration is the risk of harm which it is predicted to avert.

In principle, a CBA seeks to show that the benefits outweigh the costs of a proposal, and no further specific criterion is therefore needed. In practice, however, a set of rules is required relating, for example, to discounting of future benefits, factors for aversion to types and magnitudes of consequences, proximity to risk limits, etc. Such rules are not usually regarded as PSC, but one which may be is the “value of life”, or of a death averted, which is needed to assign a monetary value to the benefits. This is naturally a controversial matter and tends to be avoided whenever possible. In the UK, a Department of Transport figure of £784,000 (1994) has been used [117], but this is considered to be a lower bound and values of £1m or £2m are more commonly used. In the USA, it is expressed in terms of the expected

collective dose, with a value of $1000/person Rem, although this is used by the US NRC specifically to justify that a generic safety issue warrants regulatory action and that a proposed backfit requirement will be cost beneficial on a generic basis.

5.5. PSC and PSA applications

This section considers which types of PSC, targets, etc. are appropriate for each of the PSA applications discussed in Section 3.

5.5.1. Use of PSA to support NPP design, upgrade and backfitting activities and plant modifications

The PSA applications to the design of new plants, upgrades, backfits and other modifications may make use of criteria and targets for the full range of long term average risk measures, from system reliability to public health effects, or rather to a selection of these appropriate for the country and the application. The criteria for new plants will generally be more stringent than those for backfits. Whenever an old plant is seen to be in need of widespread upgrading to bring it up to an acceptable safety standard and money is short, the main use of PSA is to assist in prioritizing the potential modifications and no specific criteria are needed for this. It must be said, however, that the broader the scope of the PSA and the PSC, the greater the flexibility in the related decision making, because of the increased probability of identification of potential modifications and of additional weaknesses, which might be more important than those found in a limited scope PSA.

5.5.2. Use of PSA in connection with NPP operation

Maintenance planning

Decisions on the overall strategy for maintenance may be made using a long term average risk measure, as above, usually CDF. Within the CDF criterion, optimization might use relative CDF with no specific criterion.

For detailed maintenance planning, the main criterion would be on instantaneous CDF, either absolute or relative. Such planning may also be constrained by criteria on the contribution to CDP for particular operations and the cumulative ΔCDP over the year.

Reliability centered maintenance (RCM) programmes

The more risk significant components may be selected using criteria involving RRW and RAW importance factors from the time averaged PSA, although it would be more appropriate to use an importance measure such as the upgrading function, as the components cannot be made perfect and are unlikely to degrade completely. An RCM programme also involves a follow-up using PSA to check its effectiveness, but in this case, system level or CDF PSC could be used to monitor the performance of the plant following the revised maintenance programme.

In-service testing

For changes to the overall testing strategy, the less risk significant components may be selected using criteria involving FV and RAW importance factors. When the purpose of this application is to reduce the burden of testing, deterministic and qualitative criteria must also be met. The more risk significant components may also be selected for enhanced testing, as for RCM, above. The PSC for acceptability of the change may be that the average CDF does not increase by more than a small fraction.

When a temporary change to a testing schedule is being considered, the relevant criterion would probably be on the instantaneous CDF, perhaps with ΔCDP.

In-service inspection

The classification of SSCs as of low risk significance may be done using essentially the same criteria as those for in-service testing, in so far as the relevant components (typically pipe segments) are modelled in the PSA. This, however, is atypical, and for this application it is likely that the PSA will have to be modified in a significant way or that components modelled in the PSA will have to be selected as surrogate elements. The risk impact of changes in the ISI schedule may be judged against a small increase in CDF, however, it is bound to be great uncertainty and more weight would then be placed on the deterministic considerations.

Modifications to AOTs in the TS

The appropriate criteria are those for instantaneous CDF, ΔCDP (increase in CDP associated with the component out of service) and the cumulative ΔCDP (or average ΔCDF) over a year.

Modifications to STIs in the TS

The criteria are essentially the same as for *In-service testing* above.

Exemptions to TS

Exemptions to TS are basically as for AOTs and STIs, but since the exemptions are generally for one-off occasions, the relevant risk criteria are those for instantaneous CDF and for ΔCDP. Allowance should be made for any compensatory risk reducing measures, and deterministic considerations are generally important.

Configuration control

This application is essentially concerned with optimization within the constraints of the TS, and as such does not need specific criteria. A criterion on instantaneous CDF may be applied, although the optimization would be expected to have reduced the peaks below any limit value.

Risk based safety indicators

These are mainly used for monitoring trends in the performance of the plant and therefore externally imposed criteria or targets are not appropriate. After a period of use, normal ranges will become established for each of the indicators, but whether these should be regarded as targets is a matter for the station management to decide.

Evaluation of operational events

The most common risk measure is the conditional probability of core damage, given the occurrence of the event, but there are several other measures of the severity of the event, such as the instantaneous CDF relative to the baseline. Either way the main use of such measures is to provide a relative scale for ranking the events. In some schemes a criterion may be used to select the most severe events for deeper analysis, but the level is really a matter of convenience and would not be regarded as a PSC.

Evaluation of safety issues

The same long term average risk measures, with their PSC, targets, etc. as were used for design and backfits, are used in this application. On identification of a new safety issue, the calculated values of the risk measures, CDF say, will increase. Provided it is within any relevant limit, the question of whether the new elevated CDF will be allowed to continue indefinitely, or whether operation will be allowed for a limited period while the issue is resolved and any necessary fixes have been implemented, is one which is usually decided on a case by case basis in negotiations between the regulator and the utility. The plant specific resolution of such issues will take account of the feasibility and costs of the fixes considered (without a formal CBA) and of course of the deterministic and engineering requirements.

The situation on generic safety issues in the USA is peculiar to the regulatory system in that country. The US NRC uses criteria involving the increment in average CDF and in the collective dose attributable to the issue, with their standard value/impact ratio, to assign priorities to the issues. If an issue is not dropped, decisions on possible fixes are then made using criteria on the estimated reduction in CDF and on the conditional containment failure probability. A value/impact assessment (CBA) is also used, unless the fix has already been dropped on the grounds of very low impact on the frequency of a large release. The main objective of this process appears to be to avoid placing unwarranted regulatory burdens, in the form of backfit requirements, on the industry. For this reason the criteria involved are not regarded as PSC.

Graded QA

The position is essentially the same as that for in-service testing and inspection, with the procedure for identifying SSCs of low safety significance involving criteria on their importance factors.

Periodic safety reviews (PSR)

It is fairly standard nowadays for a PSA, at least to Level 1, to be a required element of a PSR. Essentially the same criteria, targets, etc. are applied to that PSA as are used for design and backfits. Towards the end of a plant's life, its anticipated remaining life may be taken into account in decisions on backfits, but usually without any specific criterion.

5.5.3. Use of PSA in the area of incident and accident mitigation and management

Although the inputs from PSAs can be of great value in these areas, the applications are concerned with improvements and optimizations using relative risk measures or qualitative insights and consequently there appears to be no particular role for PSC.

5.6. Final remarks

It can be seen that in general the formulation of PSC and targets arises naturally from the particular PSA application and its objectives. The main distinction is between applications where measures of the long term average risk are appropriate and those using short term measures, usually calculated by a risk monitor. For many PSA applications the objective is one of optimization and for these it is appropriate to use a target which is relative, rather than absolute, if one is needed at all. It is far more common to find PSC expressed as targets, rather than as formal limits, and these are often based on previous experience with PSA and its applications. The relatively few examples of PSC incorporating formal limits are likely to be associated with high level safety goals. Finally, PSC or targets are always applied in conjunction with deterministic rules and engineering evaluations: PSA results are never used as the sole basis for decisions on safety.

REFERENCES

[1] NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Rep. NUREG-1150, Washington, DC (1990).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, Vienna (1999).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Harmonization of WWER PSA Model Assumptions and Data, Rep. WWER-SC-195, IAEA, Vienna (1996).

[4] ELECTRIC POWER RESEARCH INSTITUTE, PSA Applications Guide, EPRI TR-105396, Palo Alto, CA (1995).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101, Vienna (1999).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Safety Related Maintenance, IAEA-TECDOC-1138, Vienna (2000).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Application and Development of Probabilistic Safety Assessment for Nuclear Power Plant Operations, IAEA-TECDOC-873, Vienna (1996).

[8] KAFKA, P., "Risk monitoring — International status and current developments", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).

[10] HAAG, C., SCHULZ, T., SCOBEL, J., SANCAKTAR, S., "The use of PRA in designing the Westinghouse AP600 plant", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).

[11] HAAG, C., SCHULZ, T., SCOBEL, J., SANCAKTAR, S., "Insights gained from the Westinghouse AP600 PRA", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).

[12] SALTOS, N. T., EL-BASSIONI, A., " Use of PRA in the AP600 design certification review",, PSA'99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[13] CARON. J. L., ELLIA-HERVY, A., FEIGEL, A., SOURSOU, E., KOLLASKO, H., "The station blackout mitigation concept in the design of the EPR", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).

[14] GERMAN REACTOR SAFETY COMMISSION (RSK), Gemeinsame Empfehlungen von RSK und GPR für Sicherheitsanforderungen an zukünftige Kernkraftwerke mit Druckwassereaktor, Bundesanzeiger Nr. 127, Bonn (1995).

[15] BASSANELLI, A., SCHULZ, T., "Application of European utility requirements (EUR) for the development of the PSA for the European passive plant",, PSA'99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[16] NA, J. H., OH, H. C., LEE, J.S., LEE, B.S., "Probabilistic safety assessment for integrated design process for KNGR development",, PSA '99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[17] TOKMACHEV, G., "Application of PSA to resolve design and operational issues for VVER", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[18] PNACEK, I., KOVACS, Z., "PSA applications for safety upgrading of J. Bohunice V1 NPP", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[19] LIOUBARSKI, A., "NVNPP-5 plant modifications that have been performed based on PSA results. Living PSA model development", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, Spain, 1998.

[20] FAIG, J., "PSA applications at Asco NPP", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, Spain, 1998.

[21] BUNDESMINISTERIUM FÜR UMWELT, NATURSCHUTZ UND REAKTORSICHERHEIT, Bekanntmachung der Leitfäden zur Durchführung von Periodischen Sicherheitsüberprüfungen (PSÜ) für Kernkraftwerke in der Bundesrepublik Deutschland vom 18. August 1997, Bundesanzeiger Nr. 232a, Bonn (1997).

[22] BUNDESAMT FÜR STRAHLENSCHUTZ (BfS), FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-KT-16/97, Salzgitter (1997).

[23] BUNDESAMT FÜR STRAHLENSCHUTZ (BfS), FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, BfS-KT-18/97, Salzgitter (1997).

[24] NUCLEAR REGULATORY COMMISSION, Emergency Diesel Generator: Maintenance and Failure Unavailability, and their Impacts, Rep. NUREG/CR5994, Washington, DC (1994).

[25] KNOLL, A., SAMANTA, P., VESELY, W.E., "Risk based optimization of the frequency of EDG on-line maintenance at Hope Creek", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).

[26] HOOK, T.G., "Risk impact of switchyard maintenance through use of the safety monitor", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).

[27] NUCLEAR ENERGY INSTITUTE, Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, NUMARC 93-01, Washington, DC (1996).

[28] MELNICOFF, M., "PSA support of implementation of the maintenance rule at COMED", PSA'99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[29] SUAREZ, J., "Maintenance optimization program at Cofrentes NPP", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[30] RODRIGUEZ, A., “PSA and methods to optimize the maintenance of safety related equipment at Laguna Verde NPP”, paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[31] MARTORELL, S., “Use of PSA to support surveillance and maintenance planning”, paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[32] AFZALI, A., “Application of risk-informed approach to enhance plant safety and reduce cost”, paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[33] GREGORIO DE, S., “In-service testing optimization at Cofrentes NPP”, paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.

[34] HEIBA, M., ZAMANALY, J., “On-line maintenance and Maintenance Rule implementation at both Turkey Point and St. Lucie Nuclear Plants”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[35] ANDERSON, R., et al, “Probabilistic Risk Assessment in support of on-line maintenance at Virginia Power”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Surveillance of Safety Related Maintenance Activities at Nuclear Power Plants, IAEA-TECDOC-960, Vienna (1997).

[37] HUTIN, J.P., VILLEMEUR, A., Reliability centered maintenance at EDF’s nuclear power plants, Revue Générale Nucléaire (1995).

[38] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Risk-Based Inservice Testing — Development of guidelines: Volume 2, Light Water Reactor (LWR) Nuclear Power Plant Components, CRTD-Vol. 40-2, ASME, New York (1996).

[39] BALKEY, K., ART, R., BOSNAK, R., ASME Risk-based inservice inspection and testing: An outlook for the future, Risk Analysis **18** 4 (1988).

[40] SUAREZ, J., DE GREGORIO, S. PARKINSON, W., “Cofrentes NPP risk-informed inservice testing project results”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[41] HAMZEHEE, H., “Comanche peak steam electric station — Risk-based optimization of in-service testing”, paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.

[42] SARAGRACE, K., LINDENLAUB, B., LINTHICUM, R., “Risk-Based In-service Testing at Palo Verde Nuclear Generation Station”, paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.

[43] HENNEKE, D., CHUNG, G., COVENEY, M., “Risk-informed IST PRA results for San Onofre (SONGS), including fire, seismic and shutdown quantitative PRA”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[44] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, SOCIETE FRANCAISE D'ENERGIE NUCLEAIRE, JAPAN SOCIETY OF MECHANICAL ENGINEERS, Proc. Eighth Int. Conf. on Nuclear Engineering, ICONE 8, ASME, Baltimore (2000).
[45] NUCLEAR REGULATORY COMMISSION, An Approach for Plant specific, Risk-Informed Decision-making: Inservice Testing, Regulatory Guide 1.175, USNRC Washington, DC (1998).
[46] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Risk-Based Inspection — Development of guidelines: Volume 2, Part 1, Light Water Reactor (LWR) Nuclear Power Plant Components, CRTD-Vol. 20-2, ASME, New York (1992).
[47] NUCLEAR REGULATORY COMMISSION, An Approach For Plant-Specific Risk-informed Decision-making: Inservice Inspection of Piping, Regulatory Guide 1.178, USNRC, Washington, DC (1998).
[48] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants, IAEA-TECDOC-729, Vienna (1993).
[49] NUCLEAR REGULATORY COMMISSION, Handbook of Methods for Risk-Based Analyses of Technical Specifications, Rep. NUREG/CR-6141, Washington, DC (1994).
[50] NUCLEAR REGULATORY COMMISSION, Reviewing PSA Based Analyses to Modify Technical Specifications at Nuclear Power Plants, Rep. NUREG/CR-6172, Washington, DC (1995).
[51] NUCLEAR REGULATORY COMMISSION, An Approach for Plant specific, Risk-informed Decision-making: Technical Specifications, Regulatory Guide 1.177, USNRC, Washington, DC (1998).
[52] HACKEROTT, A. "Use of PSA in optimization of technical specifications", Lecture presented at the IAEA/ANL interregional training course on Advances in Monitoring, Assessment and Enhancements of Operational Safety of Nuclear Power Plants, Chicago, 1998.
[53] MLADY, O., "Temelin Safety Monitor™", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.
[54] XUE, D., "The intention of using PSA in Guandong NPP", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.
[55] FLEMING, K., "Advanced applications in configuration risk management", paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.
[56] WARREN, V., "Nuclear, on-line work scope vs. shutdown work scope", paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.
[57] TRUE, D., "Utilizing ORAM PSSAs to support shorter outages", paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.
[58] GRAHAM, R., "South Texas Project, outage planning and risk management", paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.
[59] KNOLL, A., "Pre-quantified user's manual for on-line maintenance", paper presented at the ANS Executive Conf. on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.

[60] BONACA, M., “PSA applications and risk-based regulations”, (Proc. Executive Mtg on Risk Based Regulations and Inspections, Stockholm, 1996), SKI 96-69/HSK-AN 3058/ERI-CONF 96-600, Energy Research, Inc., Maryland (1996).
[61] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Safety Performance Indicators for Nuclear Power Plants, IAEA-TECDOC-1141, Vienna (2000).
[62] MINARICK, J.W., The USUS NRC accident sequence precursor program: Present methods and findings, Reliability Engineering and System Safety **27** (23–51) (1990).
[63] NUCLEAR REGULATORY COMMISSION, Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report, Rep. NUREG/CR-2497, Vols 1 and 2, Oak Ridge, TN (1982).
[64] MINARICK, J.W., “Accident Sequence Precursor Program Methods", presentation by NUREG CP-0124 (Proc. Workshop on the Use of PRA Methodology for the Analysis of Reactor Events and Operational Data, Annapolis, 1992).
[65] NUCLEAR REGULATORY COMMISSION, Precursors to Potential Severe Core Damage Accidents 1992: A Status Report, Rep. NUREG/CR-4674 (ORNL/NOAC-232), Vols. 17 and 18, Washington, DC (1993).
[66] INTERNATIONAL ATOMIC ENERGY AGENCY, Combining Risk Analysis and Operating Experience, IAEA-TECDOC-387, Vienna (1986).
[67] HOERTNER, H., BABST, S., “Results of the precursor analysis for German nuclear power plants”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).
[68] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Plant Specific PSA to Evaluate Incidents at Nuclear Power Plants, IAEA-TECDOC-611, Vienna (1991).
[69] DUBREUIL-CHAMBARDEL, A., FRANCOIS, P., PESME, H., MALIVERNEY, B., “An operating PSA application at EDF: The Probabilistic Incident Analysis”, (Proc. Probabilistic Safety Assessment and Management ’96, ESREL’96 — PSAM-III, Crete, 1996), Springer-Verlag London Limited, London (1996).
[70] FAUCHILLE, V., LANORE, J.M., PICHEREAU, F., TIRIRA, J., “French precursor studies methods and insights”, PSA ’99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).
[71] HADNAGY, L. “Use of PSA at Paks NPP — PSA based event analysis”, paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.
[72] FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY (STUK), TVO II — Risk Follow-up Study of Precursors and Component Failure Leading to LCOs, Jan 1985–May 1994, Draft Report, Helsinki, (1994).
[73] SWEDISH NUCLEAR POWER INSPECTORATE (SKI), Demonstration Case Studies on Living PSA, SKI Technical Report 93:33, NKS/SIK-1 (92)27, Stockholm (1993).
[74] BONEHAM, P., “The benefits of using PSA to enhance the feedback of operational experience at nuclear power plants”, paper presented at Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA’97, Edinburgh, 1997.
[75] SWEDISH NUCLEAR POWER INSPECTORATE (SKI), Safety Evaluation by Living Probabilistic Safety Assessment, Procedures and Applications for Planning of Operational Activities and Analysis of Operating Experience, SKI Report 94:2, Stockholm (1994).

[76] MARCHESE, A.R., NEOGY, P. "Risk-based approach to analyzing operating events" (Proc. Probabilistic Safety Assessment and Management '96, ESREL'96 — PSAM-III, Crete, 1996), Springer-Verlag London Limited, London (1996).
[77] INTERNATIONAL ATOMIC ENERGY AGENCY, Topical Issues in Nuclear, Radiation and Radioactive Waste Safety, IAEA-TECDOC-1031, Vienna (1998).
[78] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards — A Common Basis for Judgement, Safety Reports Series No. 12, IAEA, Vienna (1998).
[79] PNACEK, I., "Description of PSA activities at the Bohunice V1 and V2 nuclear power plants", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).
[80] HERNANDEZ-ARTEAGA, J., **"**Use of Laguna Verde PSA to analyze the ECCS strainer blockage issue", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.
[81] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS OF THE OECD NUCLEAR ENERGY AGENCY, Level 2 PSA Methodology and Severe Accident Management, Rep. NEA/CSNI/R(97)11; OCDE/GD(97)198, Paris (1997).
[82] NUCLEAR REGULATORY COMMISSION, An Approach for Plant specific, Risk-Informed Decision-making: Graded Quality Assurance, Regulatory Guide 1.176, USNRC, Washington, DC (1998).
[83] GRANTOM, C.R., "Graded quality assurance application at South Texas Project", paper presented at the ANS Executive Conference on How to Leverage your PSA for Excellence in Safety and Economic Performance, San Antonio, 1996.
[84] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review of Operational Nuclear Power Plants, Safety Series No. 50-SG-O12, IAEA Vienna (1994).
[85] GRAHAM, A., HORSLEY, D., "PSAs and their applications at British Energy's reactors", paper presented at the Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, 1998.
[86] VAYSSIER, G., "The use of risk-based regulation in the modernization projects of two Dutch nuclear power plants" (Proc. Executive Meeting on Risk Based Regulations and Inspections, Stockholm, 1996), SKI 96-69/HSK-AN 3058/ERI-CONF 96-600, Energy Research, Inc, Maryland (1996).
[87] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes in Nuclear Power Plants — A Guidebook, Technical Reports Series No. 368, IAEA, Vienna (1994).
[88] HOLLINGWORTH, J.J., POD, G., "Application of MAAP in evaluation of ILRT frequency", paper presented at the American Nuclear Society Annual Meeting/MAAP International Conference, Reno Nevada, 1996.
[89] VAN DER. BORST, M., VERSTEEG, M.F., **"**PSA supported severe accident management strategies for the Borssele NPP", PSA '96 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Park City, 1996), American Nuclear Society, Inc., La Grange Park, Illinois (1996).
[90] KAJIMOTO, M., "Severe accident strategies in Japan and analysis of accident mitigation based on the PSA applications at NUPEC/INS", paper presented at the IAEA Technical Committee Meeting on PSA Applications and Tools to Improve NPP Safety, Madrid, Spain, 1998.

[91] ANG, M., BUTTERY, N., DAWSON, C., "The application of PSA in the assessment of severe accident management options for Sizewell "B" PWR", paper presented at the Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA'97, Edinburgh, 1997.

[92] ANG, M. et al., "Structured approach for the assessment of severe accident management strategies: some methods & case studies", paper presented at the Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA'97, Edinburgh, 1997.

[93] NUCLEAR REGULATORY COMMISSION AND FEDERAL EMERGENCY MANAGEMENT AGENCY, Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants — Criteria for Protective Action Recommendations for Severe Accidents, Draft report for Interim Use and Comment, Rep. NUREG-0654, FEMA-REP-1, Rev. 1, Supp.3, Washington, DC (1996).

[94] DUTTON, M., FRENCH, S., KELLY, G., "The use of PSA to assist emergency response", paper presented at Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA'97, Edinburgh, 1997.

[95] PERRYMAN, L., MAGUGUMELA, M., "The technical basis for off-site emergency planning", PSA '99 (Proc. Int. Top. Mtg on Probabilistic Safety Assessment, Washington, DC, 1999), American Nuclear Society, Inc., La Grange Park, Illinois (1999).

[96] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev. 1), IAEA, Vienna (1988).

[97] SCHMOCKER, U., PRETRE, S., CHAKRABORTY, S., KHATIB-RAHBAR, M., CAZZOLI, E., "Risk analysis and regulatory safety decisions", Advances in the Operational Safety of Nuclear Power Plants (Proc. Int. Symp. Vienna, 1995), IAEA, Vienna (1996).

[98] NUCLEAR REGULATORY COMMISSION, An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant Specific Changes to the Licensing Basis, Regulatory Guide 1.174, USNRC, Washington, DC (1998).

[99] VESSELY, W.E., "Risk-Based Regulation and Risk-Based Ageing Management", paper presented at the IAEA Specialists' Meeting on Use of PSA in the Regulatory Process, Vienna, 1993.

[100] INTERNATIONAL ATOMIC ENERGY AGENCY, Modelling and Data Prerequisites for Specific Applications of PSA in the Management of Nuclear Plant Safety, IAEA-TECDOC-740, Vienna (1994).

[101] JOKSIMOVIC, Statistical fault analysis method applied to advanced gas-cooled reactors, J. British Nuclear Energy Society. c. (1969).

[102] NUCLEAR REGULATORY COMMISSION, Safety Goals for the Operations of Nuclear Power Plants: Policy Statement, U.S. Federal Register, 51 FR 30028, Washington, DC (1986).

[103] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna (1992).

[104] VERSTEEG, M., ANDREWS, R., "Consideration of probabilistic safety objectives in OECD/NEA member countries; Short overview and update", paper presented at the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Assessment in the Regulatory Process, Vienna, 1994.

[105] CHEOK, M., PARRY, G., SHERRY, R., Use of importance measures in risk-informed regulatory applications, Reliability Engineering and System Safety **60** (1998) 213–226.
[106] UK HEALTH AND SAFETY EXECUTIVE (HSE), Safety Assessment Principles for Nuclear Plants, HMSO, London (1992).
[107] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic safety principles for nuclear power plants, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).
[108] COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES (CNRA) OF THE OECD NUCLEAR ENERGY AGENCY (NEA), Regulatory Approaches to PSA: Report on the Survey of National Practices, NEA/CNRA/R(95)2; OCDE/GD(96)7, Paris (1996).
[109] ARGENTINE NUCLEAR REGULATORY AUTHORITY, "Criterios radiológicos relativos a accidentes en CCNN", Norma regulatoria AR.31.3., Buenos Aires (1997).
[110] HILL, T., "Use of PRA in the nuclear regulatory field in South Africa", paper presented at the IAEA Technical Committee Meeting on the Use of Probabilistic Safety Assessment in the Regulatory Process, Vienna, 1994.
[111] NUCLEAR REGULATORY COMMISSION, Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission, Rep. NUREG/BR-0058 Rev. 2, Washington, DC (1995).
[112] HOLMBERG, J., JOHANSON, G., SANDSTEDT, J., "The generation of probabilistic safety indicators from the risk follow-up results", paper presented at the NEA/PWG-5 3rd TÜV Workshop on Living PSA Application, Hamburg, 1992.
[113] KIM, K., HAN, S., KIM, T., "Risk monitor application for UCN 3,4 NPP of Korea", paper presented at the Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA'97, Edinburgh, 1997.
[114] SANDSTEDT, J., BERG, U., "Living PSA applications for a Swedish BWR with the aid of Risk Spectrum", paper presented at the 3rd TÜV Workshop on Living PSA Application, Hamburg, 1992.
[115] SUÁREZ, J., DE GREGORIO, S., "Cofrentes NPP developments on PSA applications", paper presented at Int. Conf. on the Commercial and Operational Benefits of Probabilistic Safety Assessment, COPSA'97, Edinburgh, 1997.
[116] NUCLEAR REGULATORS WORKING GROUP OF THE EUROPEAN COMMISSION, Regulatory Action Related to Probabilistic Safety Assessment Studies, a Review of Current Practices, EUR 15720 EN, Brussels (1994).
[117] VAUGHAN, G., "Demonstrating risks are as low as reasonably practicable: A regulator's perspective" (Proc. 5th Annual Conference on Recent Developments in Probabilistic Safety Assessment in Nuclear Safety, London, 1996), IBC Technical Services, London (1996).

ABBREVIATIONS

ΔCDF	increment in core damage frequency
ΔCDP	increment in core damage probability
ΔLERF	increment in large early release frequency
AC	alternating current
AFWS	auxiliary feedwater system
ALARA	as low as reasonably achievable
ALARP	as low as reasonably practicable
ALWR	advanced light water reactors
AOT	allowed outage time
ASME	American Society of Mechanical Engineers
ASP	accident sequence precursors
Bq	Becquerel
BWR	boiling water reactor
CATHARE	Code for Analysis Thermal-Hydraulics during Accident of Reactor and safety Evaluation
CBA	cost benefit analysis
CCDP	conditional core damage probability
CCF	common cause failure
CDF	core damage frequency
CDP	probability of core damage
CE	Combustion Engineering
CEOG	Combustion Engineering Owners Group
CFR	Code of Federal Regulations (USA)
CMF	core melt frequency
COSYMA	code system from MARIA (method for assessing the radiological impact of accidents)
CPCD	conditional probability of core damage
Cs	caesium
DBA	design basis accident
DC	direct current
DCMF	increment of core melt frequency
ECCS	emergency core cooling system
EDG	emergency diesel generator
EOP	emergency operating procedures
ERO	emergency response organization
f/d	failures per demand
FMEA	failure mode and effect analysis
HRA	human reliability analysis
HSSC	high safety significant components
IE	initiating event
IPE	individual plant examination
IPEEE	individual plant examination for external events
ISI	in-service inspection
IST	in-service testing
LCO	limiting conditions for operation
LERF	large early release frequency
LERP	probability of large early release
LOCA	loss of coolant accident

LOOP	loss of off-site power
LPSA	living probabilistic safety assessment
LSSC	low safety significant components
LWR	light water reactor
MAAP	modular accident analysis program
MACCS	MELCOR accident consequence code system
MELCOR	(NRC) code for severe accident analysis
NDE	non-destructive examination
PIE	postulated initiating event
PM	preventive maintenance
POSR	pre-operational safety report
PRA	probabilistic risk assessment
PSA	probabilistic safety assessment
PSC	probabilistic safety criteria
PWR	pressurized water reactor
QA	quality assurance
RAW	risk achievement worth
RCM	reliability centered maintenance
RCS	reactor coolant system
RELAP	reactor excursion and leak analysis program
RG	regulatory guide
RHR	residual heat removal
ROAAM	risk oriented accident analysis methodology
RODOS	real-time online decision support system
RRW	risk reduction worth
SAM	severe accident management
SAMG	severe accident management guidelines
SAR	safety analysis report
SGTR	steam generator tube rupture
SPSA	shutdown probabilistic safety assessment
SR	surveillance requirement
SSC	structures, systems and components
STCP	source term code package
STI	surveillance test interval
Sv	sievert
TS	technical specifications
WOG	Westinghouse Owners Group
WWER	pressurized water reactor (Russian design)

CONTRIBUTORS TO DRAFTING AND REVIEW

Adamec, P.	Nuclear Research Institute Rez plc., Czech Republic
Ahmed, K.	Chashma NPP, Pakistan
Babar, A.K.	Bhabha Atomic Research Centre, India
Berg, H.P.	Federal Office for Radiation Protection, Germany
Boneham, P.	ENCONET Consulting, Austria
Burgazzi, L.	ENEA, Italy
Campbell, F.	Swallow Barn, United Kingdom
Carlsson, L.	SKI, Sweden
Caruso, G.	National Board of Nuclear Regulation, Argentina
Čepin, M.	"Jozef Stefan" Institute, Slovenia
Chakraborty, S.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Chang, Y.N.	KOPEC, Republic of Korea
D'Eer, A.	Tractebel, Belgium
Demcenko, M.	Lithuanian State Nuclear Power Safety Inspectorate (VATESI), Lithuania
Dickstein, P.	Israel Atomic Energy Commission, Israel
Duchác, A.	Nuclear Regulatory Authority of the Slovak Republic, Slovakia
Ellia-Hervy, A.	Framatome, France
Evans, M.G.K.	Scientech, Inc., United Kingdom
Faig, J.	Asociación Nuclear Asco, Spain
Fulford, J.	Scientech, Inc., United States of America
Georgescu, G.	Centre of Techology and Engineering for Nuclear Projects, Romania
Gibelly, S.	Comissao Nacional de Energia Nuclear, Brazil
Goertz, R.	Bundesamt für Strahlenschutz, Germany

Gómez Cobo, A.	International Atomic Energy Agency
Gregorio de, S.	IBERDROLA Ingeniería y Consultoría, Spain
Gunnarsson, K.E.O.	OKG AB. Oskarshamn Nuclear Power Plant, Sweden
Hadnagy, L.	Paks NPP, Hungary
Hallman, A.	Swedish Nuclear Power Inspectorate, Sweden
Hernández-Arteaga, J.	Comisión Nacional de Seguridad Nuclear y Salvaguardias (CNSNS), Mexico
Himanen, R.P.	Tellisuuden Voima Oy, Finland
Hirose, M.	Institute of Nuclear Safety, Nuclear Power Engineering Corporation (NUPEC), Japan
Hladký, M.	Dukovany NPP, Czech Republic
Hoehn J.	International Atomic Energy Agency
Horsley, D.	Scottish Nuclear, United Kingdom
Kajimoto, M.	Institute of Nuclear Safety (INS), Nuclear Power Engineering, Corporation (NUPEC), Japan
Kastelan, M.	Krsko Nuclear Power Plant, Slovenia
Khatib-Rahbar, M.	Energy Research Inc., United States of America
Koberlein, K.	GRS Forschungsgelände, Germany
Kohn, H.M.	Nucleoelectrica Argentina S.A. Central Nuclear Atucha 1, Argentina
Kolár, L.	Nuclear Research Institute Rež plc., Czech Republic
Kooyman, P.	ESKOM (Koeberg NPP), South Africa
Lanore, J.M.	FAR/DES/DIR, Institut de Protection et de Sûreté Nucléaire, France
Lee, J.	Korea Institute of Nuclear Safety, Republic of Korea
Leyshon-Jones, P.	Electrowatt Engineering (UK) Ltd, United Kingdom
Macsuga, G.	Hungarian Atomic Energy Authority, Hungary
Meslin, T.	Centre Nucléaire de Production d'Electricité de Saint Laurent-des-Eaux, France

Morales, M.D.	Central Nuclear Almaraz, Spain
Øien, K.	SINTEF, Norway
Ortega, P.	UNION FENOSA, Spain
Otero, M.T.	Asociación Nuclear Vandellos, Spain
Paepe de, C.	TRACTEBEL S.A, Belgium
Parry, G.	United States Nuclear Regulatory Commission (US NRC), United States of America
Pichereau, F.	Institut de Protection et de Sûreté Nucléaire, France
Pnacek, I.	NPP Bohunice, Slovakia
Ranguelova, V.	Committee on the Use of Atomic Energy for Peaceful Purposes, Bulgaria
Rogers, P.	Rolls Royce and Associates Ltd, United Kingdom
Rösli, B.	Kernkraftwerk Leibstadt AG, Switzerland
Schneider, U.	Institut für Baustofflehre Bauphysik und Brandschutz, Technische Universität Wien, Austria
Sklet, S.	SINTEF, Norway
Sorenssen, A.	Institutt for energiteknikk, OECD, Halden, Norway
Stanícek, J.	Energoprojekt Praha, a.s., Czech Republic
Stetkar, J.	PLG, Inc., United States of America
Szikszai, T.	Paks Nuclear Power Plant, Hungary
Takasan, S.	Institute of Nuclear Safety, Nuclear Power Engineering Corporation (NUPEC), Japan
Tokmachev, G.V.	Institute Atomenergoproekt, Russian Federation
Tzvetanova, E.	Committee on the Use of Atomic Energy for Peaceful Purposes, Bulgaria
Vehec, T.	Pacific Northwest National Laboratory, United States of America
Venkat Raj, V.	BARC, India

Versteeg, M.F.	Ministry of Social Affairs, SZW/KFD, Netherlands
Vincent, J.L.	Technicatome, France
Vojnovic, D.	Slovenian Nuclear Safety Administration, Slovenia
Williams, R. J.	British Nuclear Fuels plc, United Kingdom
Windle, P.L.	Royal Naval College Greenwich, United Kingdom
Yllera Sánchez, J.	Consejo de Seguridad Nuclear, Spain

Technical Committee Meetings

Vienna, Austria: 4–8 December 1995, Madrid, Spain: 23–27 February 1998

Consultants Meetings

Vienna, Austria: 6–8 March 1996, 21–25 October 1996,
1–5 September 1997, 27–31 July 1998