IAEA-TECDOC-740

Modelling and data prerequisites for specific applications of PSA in the management of nuclear plant safety

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

The originating Section of this document in the IAEA was

Nuclear Safety Section
International Atomic Energy Agency
Wagramerstrasse 5
P O Box 100
A-1400 Vienna, Austria

MODELLING AND DATA PREREQUISITES FOR SPECIFIC APPLICATIONS OF PSA IN THE MANAGEMENT OF NUCLEAR PLANT SAFETY

IAEA, VIENNA, 1994
IAEA-TECDOC-740
ISSN 1011–4289

Printed by the IAEA in Austria
April 1994

FOREWORD

The IAEA has a programme which supports the performance and use of probabilistic safety assessments (PSAS) to improve nuclear safety internationally. The assistance offered in this area by the IAEA to Member States has traditionally focused on planning, performance and peer review of PSAs. PSA activities within the IAEA's programme in the area of applications are presently being expanded.

The various applications of PSAs require that PSAs being developed have certain characteristics in terms of their scope, the degree of detail in the modelling, the flexibility in performing desired calculations, the quality and type of the data used, and the assumptions made in treating safety significant aspects. In many cases, existing PSAs or PSAs being completed can be extended to fulfil the requirements for uses in many applications to enhance the safety of nuclear power plants. This report provides information on how to carry out such extensions by matching PSA characteristics to various applications that are being considered.

This report was prepared by consultants together with the IAEA following the recommendations of a Technical Committee Meeting on PSA Requirements for Use in Safety Management, held by the IAEA in co-operation with the Swedish Nuclear Power Inspectorate in Stockholm, Sweden, 16–20 September 1991.

EDITORIAL NOTE

In preparing this document for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

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

5/6

1. INTRODUCTION

1.1. BACKGROUND

Over the last ten years, there has been a remarkable growth of the use of probabilistic safety assessments (PSAs), both in the industrial and the regulatory environment. With few exceptions, countries operating or constructing nuclear power plants have national programmes aimed at developing plant specific PSAs. In several countries PSAs are a mandatory part of the licensing process.

The first generation of PSAs usually focused primarily on identifying possible design weaknesses and the potential for improving procedures. These PSA applications may concern different stages in the plant life cycle (e.g., conceptual or final design stage, operating plant) as well as different design types (e.g., present–operating/future–passive). The engineering insights resulting from such PSAs are usually not undermined by the numerical uncertainties involved. Confidence is obtained if the PSA has relevant scope, uses state of the art approaches to modelling topics, and has been reviewed.

The most rapidly growing area of PSA applications is their use to support operation. Many of these applications are characterized by the potential for not only improving (or at least maintaining) the safety level but also for providing guidance on the optimal use of resources and reducing burden.

The wide spectrum of PSA applications and the need to regularly update and/or modify the PSA lead to requirements for the environment where the PSAs will be used. The living PSA programmes being developed, and to a different extent, implemented in several countries, are designed to satisfy these requirements [1]. Such programmes comprise as their basic element a PSA study that is well structured, well documented, reviewed, highly detailed, and plant specific. The study is maintained 'living' by periodically updating it to reflect all relevant plant changes in the front line and support systems, procedures, practices and management of operations. The PSA also is updated to reflect changes in the database, improved understanding of the plant systems, and advancements in PSA methods, to meet the needs of new applications and enhance the completeness of PSA models.

A PSA constitutes a comprehensive and complex logical model supported by a large number of data. Different applications set requirements on the scope of the PSAs, the necessary degree of detail, the quality and coverage of data, and the capabilities of the computer tools used to handle the models.

Reviews of PSAs undertaken by the IAEA within the International Peer Review Service (IPERS) programme [2] demonstrate that the PSA models are not always compatible with some of the intended uses, as specified by the objectives of the PSAs. A recent review [3], which summarizes insights from the IPERS missions, illustrates this point. Extracts from this paper, covering specific modelling problems that are frequently observed during PSA reviews, are given in the Appendix.

1.2. OBJECTIVES OF THE REPORT

The primary objective of this document is to provide guidance to the Member States on the various applications for PSAs and to define the requirements and capabilities that are needed for these applications. These objectives were endorsed by the IAEA Technical Committee Meeting on PSA Requirements for Use in Safety Management, held in Stockholm, Sweden, 16–20 September 1991 [4].

This report may be used by analysts and by reviewers and can be applied when planning a PSA that is intended to meet an extensive set of objectives, including uses for a wide spectrum of different applications. However, most PSA programmes are not all inclusive from the beginning. Rather the scope, degree of detail, and the set of applications are systematically being extended, using a 'base case' PSA model as a starting point. Consequently, this report points out which aspects to keep in

mind when considering the use of an available PSA for different applications, and which features are necessary when extending the set of applications. Therefore, we suggest setting priorities for applications. This recommendation is based on the extent and complexity of the additional features of the PSA, as implied by each application, respectively.

1.3. DEFINITION OF SCOPE

The PSA applications covered in this document are divided into five broad groups:

- Design and procedures adequacy evaluations and improvements;
- Evaluation of operational activities;
- Regulatory and inspection applications;
- Operational experience assessment applications;
- Ageing and life extension evaluations.

Each group contains several subgroups which represent different specific applications. Applications placed in the same group are related in terms of specific PSA requirements. Because there still are differences, the requirements are given explicitly for each application. The applications selected in this report are those where PSAs have already been fruitfully applied or are being applied, and not those which have only been tested in the research environment or are in a conceptual stage of development.

The requirements are provided specifically for:

- PSA models,
- PSA data,
- Calculational capabilities, and
- Presentation of results.

Only requirements for Level 1 PSAs are addressed in this report. This scope is considered adequate and cost effective for a majority of the applications described here, although the applications which require that the containment function be evaluated are not covered. Thus, PSA based accident management is addressed only for pre-accident applications; post-accident aspects are not covered. Modes of operation other than full power are not directly addressed because there still are only few corresponding PSAs, and modelling approaches still are being developed. We anticipate that this report also will be useful for shutdown and low power PSA applications, but modifications and supplements will be necessary.

While computer codes are needed for performing a PSA and for using it, the associated requirements are not the focus of this report. They are, however, implied by requirements concerning calculational capabilities. For example, an on-line application will demand significantly shorter response times than the off-line use of PSA.

1.4. USES OF THE REPORT

This report is expected to serve several purposes. First, it identifies the immediate application areas for PSAs for different countries that are developing PSAs; second, it provides guidance to the PSA developers who can either develop or extend their PSA; third, it will assure greater consistency both in the scope and contents of the PSAs and in their uses; and finally it will promote PSA applications in enhancing safety of nuclear power plants.

1.5. OUTLINE OF THE REPORT

Section 2 outlines the different areas of PSA applications. The requirements for applying a PSA in each area are defined in Section 3. For each specific application objective, PSA modelling and data

requirements, calculational capabilities, and the requirements for presenting the results are provided. Section 4 contains recommendations for prioritizing different PSA applications. Finally, some generic lessons learned from international peer reviews of PSAs are compiled in the Appendix.

2. PSA APPLICATION AREAS

PSAs are increasingly being applied to address a variety of issues, which involve daily activities in the plant to long range issues relating to safety as plants age. Attempts are being made to evaluate almost every aspect of nuclear power plant operation, including design features, operational activities, regulatory requirements, and assessment of safety or risk levels. In this document, we present different applications to allow the reader to obtain an overall picture of the various applications of interest using a PSA.

To bring together such a broad spectrum of applications in a single document, we focused on applications that have been fruitfully demonstrated, or are in progress, or are being given serious consideration. We excluded applications requiring extensive research. We anticipate that, with further research and developments in PSAs, many other useful applications will be identified and performed. Nonetheless, the beneficial applications that can be started following the completion of a PSA are covered here.

The different applications are grouped into the following five main areas:

- Design and procedures adequacy evaluations and improvements;
- Evaluation of operational activities;
- Regulatory requirements and inspection priorities;
- Operational experience assessment;
- Ageing and life extension evaluations.

Each of these applications are independent and can be undertaken separately or together. Recommended priorities are given in Section 4.

Design evaluation and procedures improvements are natural extensions of conducting a basic PSA. A PSA identifies the dominant risk contributors in the plant and at the same time, reveals deficiencies and inadequacies. Specific applications that can be performed in this area are:

- Evaluation of design features and procedures;
- Consistency with safety goal(s);
- Decisions on design modifications/backfitting;
- Important procedures requirements and operator training.

PSAs can be used to evaluate activities during operation to understand their risk significance and to prioritize these activities to increase risk effectiveness and to address the burden associated with them. In this area, applications are defined which can be carried out within the regulatory requirements. Many of these activities are controlled by regulatory bodies, and as such, these applications are related to the applications defined in the next area. Specific applications covered in this area are:

- Evaluation of surveillance and maintenance activities;
- Configuration management activities;
- Maintenance planning;
- Surveillance test arrangements.

Regulatory and inspection requirements are intended to assure safe operation of nuclear power plants. However, because these requirements were defined without the benefit of a systematic quantitative risk evaluation, such as a PSA, many could be modified to improve safety or to reduce operational burden, or both. Also, these requirements can be focused on risk important areas to increase their effectiveness. The types of applications discussed are:

- Guidance for inspections;
- Modification of allowed outage time (AOT) and requirements for surveillance test intervals (STIs);
- Limiting conditions of operation (LCOs) action statements;
- Quality assurance;

Feedback from experiences gained during operation is essential in for assuring continued safety. PSAs provide a structured framework for understanding the significance of an operational event. They also address 'what if' questions in a quantitative manner to provide lessons for the future. Two types of operational experience assessments are addressed:

- Incident analyses (off-line evaluations);
- On-line or real time assessment of events;

Finally, as plants age, their safety margins may be reduced. Systems, components, and structures susceptible to age can degrade, whereby a plant's ability to respond to an accident can be seriously undermined. PSAs can be used to assess ageing effects and provide priorities for ageing management. Specific applications discussed are:

- Safety implication of ageing effects;
- Prioritizing ageing management activities.

3. CAPABILITIES AND REQUIREMENTS FOR VARIOUS PSA APPLICATIONS

3.1. ELEMENTS

In this section, the PSA requirements and capabilities that are necessary for each application are described. For all cases, a brief discussion of the reasons such an application may be carried out and the objectives of the application are presented.

The aspects covered are the following:

- PSA modelling requirements;
- Data requirements;
- Calculational capabilities;
- Requirements for presenting of results.

The purpose of presenting these requirements is to provide an overview of the details needed in the PSA and an understanding of what is involved in the application. The discussions do not present the methodology for the application, nor do they present procedure for carrying out the application. Mathematical formulations of the measures are not included. However, the requirements for the methodology are clearly presented. The details of the methodology can be obtained in the References.

In presenting requirements and capabilities, the important aspects are essentially addressed. As mentioned previously, many of the applications have been successfully demonstrated, while others

are being planned or in progress. Thus, in certain cases, the tools required to efficiently satisfy the requirements are not available.

In addition, the requirements for the regulatory authorities in individual Member States vary and those also should be satisfied. This document does not address any such requirements. However, we anticipate that the requirements, as presented, when carried out, will form the essential basis to address any specific requirements. For example, many of the applications may require certain safety criteria or numerical criteria that are acceptable to regulatory authorities. This document does not present or address such criteria, but, the requirements presented will provide the technical basis to demonstrate acceptability to such criteria.

In presenting the requirements, each section is treated independently, i.e., if any requirement is needed across the sections, it still is mentioned in all the sections. Subsections, however, will refer to previous requirements to the extent possible. The reasons for this style of presentation is because a reader may be interested only in a particular area of application and may not read the entire document. This style causes some duplication, but will conveniently allow selective reading. The only exception is the fundamental requirements for 'base case' Level 1 PSA, which are given only in Section 3.2.

3.2. REQUIREMENTS FOR DESIGN AND PROCEDURE ADEQUACY: EVALUATIONS AND IMPROVEMENTS

The basic and traditional uses of a PSA include:

(1) Evaluating design features and procedures.
(2) Demonstrating consistency with safety goals.
(3) Decisions on design modifications and backfitting.
(4) Important procedures requirements and operator training.

These applications are covered in this section, although the objectives are different. However, the principal requirements are similar. The main differences are associated with the scope, level of detail, and degree of conservatism (if any), in the PSA model. Generally, for a more detailed description of Level 1 PSA tasks, the IAEA Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants [5], or other PSA guidance documents [6–8], should be consulted.

A PSA can be performed at any stage of the plant life cycle, namely:

- at the conceptual/early design stage;
- at the final design stage;
- at the operating plant.

Depending on the actual stage, certain details concerning plant design and operation may not be available. Thus, the may not be the detailed balance-of-plant information, site specific information, plant specific data, or detailed operating procedures at the time the PSA is being performed. Relaxed requirements must be set for such situations, but the PSA models and documentation should be maintained and updated throughout the operating life of the plant to provide relevant representation of its features. This approach will include incorporating as-built features, and detailed operating and maintenance procedures. Some of the details are developed during construction and some as-built features will be known at a relatively late stage.

3.2.1. Evaluation of design features and procedures [2, 5–10]

Because the PSA model used for this application normally forms the basis for all other applications, we present the requirements with more detail here than for the other cases.

Objectives

Some specific objectives can be defined for this basic application:

(1) To identify and rank dominant accident sequences (i.e. risk contributors).
(2) To identify systems, components, and human actions important for safety.
(3) To assess important dependencies (system and human–machine).

PSA modelling requirements

- A set of initiating events grouped into classes based on similarity of plant response are required. The set must be sufficiently complete to ensure that all the safety functions and the associated systems are thoroughly examined in the event trees. The set should include transients, loss of coolant accidents (LOCAs) and common cause initiators that are associated with the loss of support systems. Inclusion of external events is desirable; if they are not within the scope of the analysis, insights obtained for other initiators still are relevant, although the risk profile is not complete. If the site is not determined, external events still can be analyzed using 'typical' site characteristics.

- Success criteria developed for all front line systems and each support system of interest should be listed. The success criteria should adequately represent the plant's capability and should be closely connected to a rigorous definition of core damage/core melt. The success criteria should be based on realistic assumptions which are justified by analyses. The use of conservative success criteria may bias the estimates and should be avoided.

- A set of event trees for all the initiating events should be considered. If possible, the headings of the event trees should be ordered chronologically. Major human actions, which involve diagnosis and decision making in accident situations, should be modelled in the event trees.

- A set of fault trees for all the system failures which are considered, including front line system failures and support system failures should be included. The models must be developed to sufficient depth to identify, represent, and quantify dependencies. In general, this corresponds to system modelling at the component level, although in special cases it might be necessary to include detail at the subcomponent level. The fault trees should adequately account for maintenance and testing unavailabilities and for human actions that involve operating the plant. In case procedures (operating and emergency, surveillance/ maintenance) are not available for a plant that is not yet operating, substitute procedures from a similar plant can be used.

- Component unavailability model should include random failure contributions, test and maintenance unavailabilities, and common cause failure contributions for all redundant components that are susceptible to common cause failures.

- A discussion of the treatment of different types of dependent failures, including any qualitative or quantitative screening method used to identify the significant contributions of common cause failures should be presented. In particular, a systematic approach should be used to establish common cause component groups, and an effort should be made to understand the associated failure mechanisms and existing defenses. Preferably all applicable common cause failure (CCF) multiplicities and run-mode CCFs should be included. Reasons for excluding any CCFs should be documented.

- The operator's actions should be addressed in detail; however, if procedures for a non-operating plant have not been developed, the operator's actions are subject to limitations. In such cases, the focus should be on identifying important actions, and test and maintenance tasks where detailed procedures are needed, and on ranking the importance of different procedures. The actions to be covered include: (1) those which occur before an initiating event; (2) those which

lead to a plant transient; (3) those taken after the initiating event to tentatively bring the plant to a safe state.

- An analysis of external events (if within the scope of a PSA) should be provided. The analysis usually comprises the assessment of the frequency of each initiating event, the effect on equipment, and accounts for the effect of degraded or disabled systems and components through the plant model. Great care must be exercised when dismissing specific external events on the basis of low frequency, and when screening out particular accident scenarios. Possible differences in operator response, as compared to accident situations initiated by internal events, should be accounted for.

- The frequencies of accident sequences defined in the event trees and the identification of the dominant contributors should be quantified. Valid quantification formulas that account for the high order terms should be used. Dominant cut sets for the dominant sequences should be given. Importance, sensitivity, and uncertainty analyses should be included as an integral part of the quantification. However, a formal uncertainty analysis may not be necessary for plants that are in the early/conceptual design stage. Sensitivity analyses may be a preferable option to formal uncertainty propagation when investigating modelling issues which are not well understood.

- If the PSA is carried out for an operating plant, conservative assumptions should be avoided or used mainly for screening accident sequences. The same applies to plants in earlier stages of life cycle, although avoiding these assumptions may be difficult. Whenever possible, conservative assumptions should be revised for dominant contributors. Bounding assumptions, if used, should be explicitly identified.

- Plant status/configuration considered as the reference should correspond to the base case situation.

Data requirements

- The data needed comprise initiating event frequencies, component failure rates, parameters for common cause failures, test, maintenance, and repair times, human reliabilities, external events analyses (e.g. fragilities), and the associated distributions.

- Plant specific data are preferable, if they exist. For PSAs for a plant that is not yet built, generic data have to be used. Generally, a discussion is needed concerning the rationale for selecting a particular database and the applicability of the selected data to the plant being analyzed.

- For transient frequencies, generic data are applicable only if the analyzed plant is very similar to the source plant(s) and the operational environments are similar. Generally, when using generic data, consideration must be given to screening generic events, which due to specific features of the investigated plant, may be excluded, or there may be an impact on the event frequency. For common cause initiators associated with the loss of support systems, it may be necessary to construct logic models and use them to estimate the corresponding frequencies. Analytical models also are used to estimate frequency for low frequency initiating events, such as interfacing system LOCAs.

- The PSA should consider the use of plant specific experience and generic data to obtain distributions of component failure rates. Bayesian approaches have generally been used for the combination process. Care should be taken, however, that the generic data and Bayesian priors are consistent with plant specific data. If there are no plant data, generic data should be reviewed with respect to applicability criteria. These criteria include component design characteristics, component boundaries, maintenance and test procedures, and modes of operation. Data based on expert judgement should be clearly identified.

- Standby component failure rates should preferably be in rates per hour to account for the effect of different test intervals and to facilitate future PSA application extensions. If rates are given per demand, there should be an explanation of how the numbers were derived.

- The human reliability database covers data for pre-initiator errors, for errors which lead to a plant transient, and for post-initiator interactions. Usually, a distinction is needed between the diagnosis part of the interaction and the errors in carrying out the action. Pre-initiator errors involve reconfiguration errors after test or maintenance, and miscalibration errors. For important and complex pre-initiator errors, it is necessary to apply logical models to generate realistic estimates, although quantification of the basic contributions is to some extent judgmental. Errors leading to a plant transient are implicitly reflected in the frequencies of the initiating events. Breakdown into specific causes and corresponding numerical contributions may be necessary for these errors to assess the probabilities of recovery. Data for post-initiator interactions may originate from available records, generic experience, simulator runs and from expert judgement. Recoveries should preferably be linked to combinations of events (minimal cut sets), and their quantification should take into account the time available, environmental conditions, cues, and stress level. Errors of commission should be considered as a minimum on a case by case basis or treated in sensitivity analyses; however, no proven systematic methodology for identifying such errors, and few data are available.

- Screening values may be used to quantify those human errors which are found to be non-dominant contributors in preliminary quantifications. For plants in early design stages and/or for cases where procedures are not yet developed, screening values constitute the only possible approach.

- The most appropriate estimates of common cause failure (CCF) contributions would be obtained from plant specific data. Because a statistically adequate, plant specific CCF database is unlikely to be available, we recommend pooling data from a variety of plants, and constructing a pseudo plant specific database by reinterpreting historical events of the plant. Constructing this database includes considering the existing defenses against CCFs. If there is insufficient data, the CCF contributions are non-dominant, or if the plant is in an early design stage, generic parameter estimates may be used. However, we do not recommend using these estimates, because they do not provide any insights into what precautions could be taken, or defenses implemented at the plant to improve safety.

- For operating plants, actual maintenance records should be used to estimate maintenance unavailabilities. Such data are not available for plants starting operation. Thus, data from similar plants (not only in terms of design, but also with respect to operational environment) may be used. Another possibility is to use (only in cases where the data are not known in detail) data which reflect the range of values used in plants. This applies not only to maintenance downtime but also to test duration times and test intervals of components. The primary set of values should be representative for average to upper bound values used in PSAs. The important identified contributors can then be changed in sensitivity studies. Sometimes manufacture specifications provide recommended test intervals.

- Typical data needed for external events analyses include, for example, a seismic hazard curve, characteristics of the soil structure around the plant, component and structural fragilities to earthquakes, frequency and location of fires of different sizes, non-detection and non-suppression probabilities, a component's 'susceptibility' to fire and combustion products, frequency of flooding from different water and steam sources, the size, duration, and coverage of floods, effects of floods on equipment, high wind hazard curves, probabilities of tornado induced missiles, building and equipment fragilities to winds, and the effects of operator's errors related to external events.

Calculational capabilities

- The primary capability is to determine the accident sequence and system minimal cut sets, and quantify the associated core damage frequencies (CDFs) and the total CDF with associated uncertainties.

- The ability to calculate importance measures such as Birnbaum, Fussel-Vesely, risk achievement worth (RAW), risk reduction worth (RRW) is necessary. This should be possible not only for individual basic events, but also for user defined groups of events.

- The ability to carry out uncertainty propagation and to perform sensitivity analyses is needed.

The following additional features of a PSA computer code package to be used are not requirements, but are highly desirable because they enable rationalization of work, enhance quality assurance, make other applications feasible, and are generally a part of a 'living' PSA.

- Reasonably short response times, typically 30 minutes or less per accident sequence quantification. The computer package should be able to handle large plant models without the need of manual modularization.

- The possibility to easily update PSA models and data, to easily retrieve information from the model and database, and to efficiently perform a large number of recalculations. This leads to requirements on availability of user friendly functions for editing the logic models, for input/output handling, for searching, viewing and report printing, and requirements on expanding the package in terms of additional analysis functions.

- The ability to handle NOT logic, either explicitly or implicitly, by automatically deleting dual cut sets.

Presentation of results

- The results should be presented clearly and in a balanced manner. The bottom line numbers should not be the principal focus. Instead the important contributions should be identified, and the findings concerning plant strengths and vulnerabilities should be emphasized.

- The results calculated in a PSA should include the following:

  - the mean CDF, with 5% and 95% bounds;

  - the mean frequency for each accident sequence, with 5% and 95% bounds;

  - the mean system unavailability for each system failure mode in the event trees, with 5% and 95% bounds;

  - the percentage contribution of each accident sequence to the mean CDF;

  - the percentage contributions of the dominant minimal cut sets to the mean CDF, each mean accident sequence frequency, and each mean system unavailability;

  - the Birnbaum importances and Fussel-Vesely importances of the dominant contributors to the mean CDF, each mean accident sequence frequency, and each mean system unavailability;

  - risk reduction worth (RRW) and risk achievement worth (RAW) for basic events represented in the plant model;

- results of sensitivity studies on high importance contributors and on all questionable assumptions, models, and data values that are not covered by the uncertainty analyses.

- The results of the presentation should include and discuss in detail the following:

  - the importance of event class with respect to core damage frequency, including for example, human errors, test and maintenance unavailabilities, initiating events, and classes of hardware faults;

  - the importance of the system with respect to core damage frequency;

  - the effects of various sensitivity issues on the dominant sequences and core damage frequency;

  - the important assumptions, limitations, and constraints of the PSA;

  - the comparison of results with those of previously published PSAs for similar designs (with identification of reasons for differences);

  - the completeness of the analysis;

  - the achievement of the objectives of the study.

- The dominant event sequences and dominant contributors should be described in a manner that non-specialists can understand. The results should be presented in a numerical or tabular form, but graphs or bar charts of the contributors should be presented to more effectively show the findings. Dominant contributors should be cross-referenced to the relevant event sequences and systems; contributors also should be cross-referenced to design drawings.

- Conclusions and recommendations, including applications to design and improvements of procedures, should be highlighted. Thus, important insights should be focused on and prioritized, for example, in the following manner:

  - contributions are prioritized according to their CDF and unavailability contributions;

  - support systems dependencies are highlighted;

  - manual actuations and reconfigurations required by the design are identified;

  - non-deductible failure modes associated with the design are highlighted;

  - test and maintenance difficulties associated with the design are identified.

  - single active and passive component failures which lead to system failure, single human actuation or reconfiguration errors, single passive component failures, which are not detectable under normal testing, and two similar component failures or human actuation/reconfiguration errors, are identified as design associated contributors with highest priority;

  - all contributors are ranked according to their risk achievement and risk reduction importances; contributors with importance worths greater than 10 are singled out;

  - all contributors, which can cause the core damage frequency to increase above a predefined level (e.g., 1×10^{-3} per year or 1×10^{-4} per year), when sensitivity studies are performed, are identified.

3.2.2. Consistency with safety goal(s) [11]

If a safety goal or target or criterion is available, the PSA can be used to compare the safety level of the plant against these criteria. Here the most demanding application, when the goal is defined at a high level (core damage frequency), is addressed. Evidently, lower level goals (defined for safety function and/or system unavailability) lead to much more relaxed requirements in terms of the scope of the analysis and, consequently, corresponding verifications of consistency with these goals do not automatically require a full scope Level 1 PSA. High level goals also can be defined in relation to radioactivity releases or health risks. This goal requires, however, Level 2 and Level 3 PSAs, respectively, and is not covered in this report.

Generally, PSAs are seldom performed for the sole purpose of comparison with a safety goal. Usually, the design related insights are in focus and compliance with a safety goal (if such a goal exists) is investigated in parallel, basically using the same PSA. The main differences are the following:

- The acceptable degree of conservatism (i.e., conservative bias is acceptable in safety goal applications as opposed to the realism needed in design evaluations focused on engineering insights); however, it might be difficult to meet the criteria if excessively conservative assumptions and data are being used.

- Demands on scope (i.e., valid engineering insights may be obtained even when the scope is limited, while demonstration of compliance with safety goals implies need of an all inclusive scope; which may, however, depend on the regulatory criteria).

- Necessary degree of modelling detail (i.e., as long as it can be assured that the approach chosen leads to numerically conservative results, shortcuts and simplifications are possible in safety goal applications).

The focus of the requirements below is on providing some examples where the requirements in safety goal related applications are either more stringent or more relaxed, as compared to those of Section 3.2.1.

Objectives

The objective of this application is to compare the estimated frequency of core damage of the analyzed plant with a predefined target value.

PSA modelling requirements

PSA modelling requirements are to a large extend similar to those defined in Section 3.2.1, with the following modifications and emphasis:

- External events must be included in the analysis, unless a safety goal is specifically defined for internal events. In principle, the same applies to modes of operation other than full power.

- Components can be lumped together in fault tree models, if it can be assured that no significant dependencies are being overlooked.

- The level of detail in modelling common cause failures and operator's actions can be relaxed, if all significant contributors are included, and the assigned probabilities can be regarded as conservative. Including recovery actions is optional.

- Use of simple estimators (first moment approximation) is allowed, but may lead to substantial overestimation in cases with high probabilities (e.g., external events) and/or when many cut

sets share the same basic event. Cut set truncation on low probability ground must be done with great care because a large number of low probability cut sets can potentially and significantly contribute to the numerical result.

- Uncertainty propagation must be carried out.

Data requirements

Data requirements may be relaxed as compared to those stated in Section 3.2.1.

- Plant specific data are preferable, but use of generic data is acceptable if their applicability can be defended, or if they are obviously conservative.

- Screening values can be used for human errors and for common cause failures. For example, a generic beta factor of 0.1 is likely to be conservative for most of the cases. Engineering assessment will, however, be necessary to support lower values.

- Failure-on-demand data can be used for this application.

Calculational capabilities

The calculations will normally be done using the same computer code package as for design evaluations. Some of the following capabilities are, however, not absolutely necessary for this particular application.

- Calculation of importance measures is optional but advisable.
- Long response times (many hours) are acceptable (although not practical).
- Success states can be ignored in quantification.
- Variety and user friendliness of editing and information retrieval functions are not critical factors for this application.

Presentation of results

The requirements presented in Section 3.2.1 can be significantly relaxed. Although the PSA still will need to calculate the same type of results, the presentation of the results can be limited. There are no requirements to present the engineering insights in detail. However, for safety goals, the results are seldom viewed only from a purely numerical perspective, i.e. in relation to a single number. The basis for acceptance will be a demonstration that adequate provisions have been incorporated into the design of the plant, and that adequate operating and maintenance procedures to prevent the occurrence of severe core damage are available. Thus, there still is a need to group and prioritize the important contributors, which leads to the following specific requirements:

- A discussion on which design and operational features are the principal controlling features for the criteria must be included.

- There is a need to demonstrate robustness of the PSA estimates and to clearly identify the driving factors. Results of sensitivity and uncertainty analyses are central for achieving this goal.

3.2.3. Decisions on design modifications/backfitting [12]

Many PSAs have been and are being successfully used to identify and optimize plant improvements. Consideration of design modifications is an integral part of the design process. Proposed design backfits of plants and systems generally emanate from either of two distinct sources. Regulatory bodies may propose design backfits, which are intended to enhance plant safety by

improving equipment operability. Backfits of this type are often proposed in response to safety issues which have become newly recognized, or which are believed to have recently become better understood and can, thus, be addressed more effectively. The second major source of proposed design backfits is the utilities which own and operate nuclear power plants. Backfits proposed by the operating utilities may be intended to address specific safety concerns, to achieve better cost or operating efficiency, or, in some cases, may be developed as alternatives to more costly backfits proposed by regulatory bodies.

Design modifications and backfitting applications are natural extensions of a basic PSA, having the features described in Section 3.2.1. Thus, the initial requirements are identical with those specified for evaluating design features and procedures. Some requirements, however, deserve special attention.

The process of developing alternative designs is supported by using PSA techniques, because this analysis will identify which features of the design contribute the most to system/plant failure. By concentrating on design solutions which 'fix' these problems, alternative designs are often suggested.

Alternatives, when evaluated, may be categorized as follows:

(a) No action, the proposed change will not improve the design.
(b) Improve personnel training requirements or discipline.
(c) Change the operational and/or maintenance procedures.
(d) Change the operational envelope of some systems or of the whole plant.
(e) Change component suppliers.
(f) Modify the application of some components.
(g) Modify some system design (added redundancy, new components, changed actuation principles, separation).
(h) Add a totally new system (including removing an old system as needed).
(i) Remove, replace, rearrange or redesign groups of systems.

It is important to emphasize that PSA is only one input to the decision making process which may result in design changes.

Any proposed design solution must comply with the applicable qualitative design criteria, including, for example, industry standards, as well as solutions dictating design directions (suitable redundancy, adequate isolation capability, diversity, sufficient independence, and appropriate margins). A basic assumption of the design modification/backfit assessment process is that existing design criteria provide valid limits of acceptable design practices. Each alternative must at least meet applicable functional and operability requirements and display features to satisfy existing safety and reliability requirements to some degree.

Once the functional and operability requirements are met, the proposed change becomes a candidate for implementation and will usually be subject to the cost/benefit evaluation, which is a part of the methodology for deciding on the design. Cost/benefit evaluation is particularly important when several alternatives are being compared. Factors which are outside of the PSA scope, although fundamental for the selection process, are not addressed in detail for the requirements presented here. They are, however, mentioned to stress the interactions between the PSA and other tools used by the decision makers. The process for evaluating the alternatives is iterative and has the following essential ingredients:

(1) Quantification of the level of safety for the existing design;
(2) Quantification of the level of safety for the backfit/design modification alternatives;
(3) Estimated cost of the backfit/design modification alternatives;
(4) Optimization of cost and safety considerations; and
(5) Development of the above information in a timely fashion concurrent with the design process to support decision making.

Decisions on design modifications and backfitting need identical requirements on PSA models, data, calculational capabilities, and presentation of results. However, backfits always concern operating plants, which implies availability of plant specific operational data. Design modifications, on the other hand, are implemented in the design process. Thus, the remarks with regard to constraints associated with limited information available during pre-operational phases in the plant life cycle, outlined in Section 3.2.1, also are valid for the applications covered in this section.

If the backfit or design modification is to improve system availability, then system unavailability is the safety measure of interest. However, when core damage frequency is to be reduced, a Level 1 PSA, which allows us to determine the relative importance of each safety system with respect to core damage frequency, is needed. This type of more extensive applications is considered here.

Objectives

The objectives of PSA applications to design modifications is to use PSA results at the design stage to evaluate various proposed design modifications. The objective of PSA applications to backfit decisions is to use PSA to quantify the impact of backfitting options in operating plants. This evaluation should not only rank the possible backfitting options in terms of their safety improvement potential but can also provide a cost effective way of deciding which modifications should be made.

PSA model requirements

The requirements defined in Section 3.2.1 are applicable here. Special attention should be paid to the following features:

- *Using conservative/bounding assumptions should be avoided to the extent possible.*

- The systems operating modes must be defined within a specific environment or set of environments, which includes the normal (or ambient) environment and the environment during the accident that the safety systems are designed to protect. Other environments may be included as dictated by the special needs of a particular backfit.

- All pertinent functions of the systems must be identified, because a particular system may perform more than one safety function, especially under different postulated accident conditions. Consideration should be given to the impact of the various alternatives for the system design backfit/modification on each of these functions. Specifically, assurance is needed that a proposed change will not unintentionally result in the degradation of some other function of the system.

- Using modularized events in the base PSA model should be avoided. Using this approach makes it more difficult to maintain and update the models. When implementing the design changes into the models, preferably the original, fully developed trees should be used. Alternatively (although this is not the preferred solution), great care should be taken to assure that changes in the systems do not affect the assumed independence between the modules.

- Human error and common cause failure analyses should be revised to the extent required by the proposed design changes. Modification/backfits may lead to the need to introduce additional human error contributions that affect individual components as well as subsystem/system operation; alternatively, the set of human errors already included in the base model might have to be reevaluated. Also, there is a need to reexamine operator actions that are related to test and maintenance activities, and calibration, which may affect different systems, including the interfacing ones. Contributions of common cause failures also might need to be added or reevaluated. Using a PSA for backfit/design modification decisions reemphasizes the need to carefully analyze historical data and thoroughly study the defenses against common cause failures. In fact, the intent to strengthen these defenses might be the reason for introducing the design changes that are under consideration.

- The minimal cut sets should be recalculated after design changes are implemented into the plant model. Using pre-processed cut sets from the base case PSA is usually inadequate because the changes are likely to affect the structure of the cut sets and also may require modification of cut-off criteria.

Data requirements

The data requirements are the same as those defined in Section 3.2.1. The following aspects need special emphasis:

- Screening values should be avoided to the extent possible. Ideally, it would be most desirable to employ plant specific data derived from actual operation.

- Sources of data used for evaluating the PSA base case and for evaluating proposed alternatives should be consistent.

- Trade-off studies to optimize a series of choices in selecting the best design do not necessarily require that error bounds be determined accurately. As a result, simplifying assumptions and approximations can be used. In fact, varying the input variable failure rates using upper and lower bounds may provide a reasonable estimate of the uncertainty.

Calculational capabilities

The calculational capabilities required are the same as those defined in Section 3.2.1; some features of the computer code package (i.e. short response times, flexibility and user friendliness of the code package, ability to handle NOT logic automatically), are highly desirable.

Presentation of results

The requirements are very similar to those defined in Section 3.2.1, with substantial emphasis on grouping and prioritizing of contributors. Specific additional requirements include the following:

- The results should compare the alternatives and should compare pre-determined criteria, or measures of merit. The solution representing the highest availability at the least cost and satisfying the deterministic design criteria is the 'best' choice. Because, in many cases, the outcome is not that clear, i.e. it is rare that one specific candidate is superior from all points of view, a discussion of the trade-offs involved in optimizing a series of choices is necessary.

- If the uncertainties are larger than the base case uncertainty, some effort may be worthwhile to identify the main contributors to the uncertainty and to make the input data more accurate.

3.2.4. Important procedure requirements and operator training [9, 13, 14]

PSA results are increasingly being used for identifying operator actions which either call for developing of new procedures or strengthening the existing ones.

Objectives

(1) To identify risk important operator actions that may need new procedures or may need to be improved.

(2) To communicate PSA results to operators and use the associated insights as a framework for operator training.

PSA modelling requirements

The PSA modelling requirements are the same as those defined in Section 3.2.1. Some additional features could be considered even though they should be regarded as optional.

- If the base case PSA uses the 'small event tree/large fault tree' approach, it might be advantageous to generate large event trees to explicitly represent operator actions.

- Success paths to mitigate the event can be defined using the base PSA fault tree and event tree models. The different success paths are ranked according to operator requirements and likelihoods of success. The preferred success paths are then translated to accident procedures.

- Sensitivity evaluations of operator actions can be performed to highlight, for example, variation of risk parameters due to human error, burden on the plant management and operating staff when conducting several activities, sensitivity of dominant accident sequences, and the level of improvement in plant risk due to improvement in human performance.

Data requirements

The data requirements are the same as those defined in Section 3.2.1.

Calculational capabilities

The calculational capabilities are the same as those defined in Section 3.2.1. For generation of success paths, special software is needed.

Presentation of results

The requirements for presenting the results are similar to those given in Section 3.2.1. Some additional considerations are, however, recommended when using the PSA to help train operators.

- It is beneficial to organize the PSA in terms of courses or training packages including presenting the following:

  - basic PSA concepts;
  - dominant accident sequences;
  - dominant system contributors;
  - dominant component contributors;
  - dominant human error contributors.

- Results and operator actions, in particular, are prioritized as to their risk importance.
- Help menus describe the additional results; verbal descriptions are given for each contributor.
- Numerical results are rounded to one significant figure.
- Graphs (histograms) are used extensively to show relative sizes of contributions.
- Explanations are given with respect to significance of contributors.
- Definitions of terms and symbols are available.

3.3. REQUIREMENTS FOR PSA APPLICATIONS FOR EVALUATING OPERATIONAL ACTIVITIES

3.3.1. Evaluation of surveillance and maintenance activities [15, 16]

During operation of a nuclear power plant, several surveillances and maintenances (preventive and corrective) are performed on standby safety system components to assure their availability in case

of an accident. The basic purpose of such activities is the early detection of any failure and degradations, and the timely correction of the deteriorations. In almost all cases, such requirements are guided by Technical Specifications or by similar documents. However, because of the large number of such activities, emphasis on plant safety and allocation of resources become difficult. The purpose of a PSA application in this area will be to obtain a risk significance of these activities so that the needed areas can be emphasized.

Objectives

The objectives of this application can be summarized as follows:

(1) To obtain an evaluation of risk significance of surveillance and maintenance activities in a plant.
(2) To identify areas of emphasis for maintenance and test personnel.
(3) To identify areas where regulatory requirements can be modified without compromising plant safety (refer to Section 3.4).

PSA modelling requirements

- Level 1 PSA event trees for all internal initiating events are required; to evaluate containment system surveillance and maintenance activities, a Level 2 PSA is required. To evaluate surveillances and maintenances relating to external events, external event initiators shall be included.

- System fault trees should be detailed enough to specifically include all the components for which surveillances and maintenances are performed and must be evaluated.

- In addition to the dominant accident sequences identified in the basic PSA, additional accident sequences will need to be considered. This additional requirement will assure that quantifications of core damage frequency for different test and maintenance activities are realistic, and also will increase the number of surveillance and maintenance activities included in the evaluation.

- A computer package must be available, which can regenerate accident sequence minimal cut sets when components are assumed to be unavailable (i.e. down) for surveillance or maintenance. Using pre-processed minimal cut sets from the base case PSA may not suffice, because the cut sets important for the surveillance/maintenance condition may already be truncated.

- System train level models are adequate for evaluating maintenance activities as long as all components belonging to the train (i.e., the failure of all those components that cause train failure) are clearly identified. Dependency failure considerations should not be compromised.

- Individual component level models are necessary for evaluating surveillance activities.

- A component unavailability model that includes random failure contribution, test downtime contribution, and maintenance downtime contribution is adequate for this evaluation. Additional modelling details on separating demand and standby time related contribution can be used for refining the evaluation.

Data requirements

- A list of any requirements of reconfiguration during test and maintenance should be prepared for convenient use.

- Surveillances, which require components to be aligned away from the emergency safety position, should be identified.

- Plant specific data on repair times, maintenance durations, test durations, and test intervals should be available. In case of non-availability of plant specific data, generic data may be used once an assessment about the applicability of the data to the plant has been made.

- Surveillances that have the potential for negative effects, i.e., may cause transients, or may cause unnecessary wear of the equipment, should be identified. Also, those that require reducing power for the tests and those that cause occupational exposure should be identified. These aspects can be treated qualitatively for use with quantitative results.

- The components tested by each of the surveillances and the failure modes detected should be listed.

- Data on common cause failures and human errors in the PSA quantification should be realistic, and not overly conservative. Overconservative estimates may mask the effects of the surveillances and maintenances.

Calculational capabilities

- The primary capability is the ability to calculate effects of accident sequence frequencies and core damage frequency impacts for components being unavailable (down) and available (up). There should be negligible error due to truncation of minimal cut sets.

- In calculating the risk level for a component that is down, the reconfiguration of other components should be accounted for.

- For maintenance evaluations, the effect due to a given maintenance and that due to several maintenances in a given period, e.g., one year, should be calculated.

Presentation of results

- The results should include a quantitative assessment of the risk impact of each of the maintenance and surveillance activities. For maintenance, the risk measures should include an assessment of risk impact over the duration of the maintenance and over a period of one year. For surveillance, risk measure assessing the benefit of surveillance will be adequate.

- The results should present a prioritization of surveillance and maintenance activities in 4 to 5 groups, clearly delineating the significance of the activities to the plant personnel. Such groupings should primarily be based on quantitative results, but can be adjusted to include qualitative considerations discussed in the data requirements section above.

- The results should be used to identify surveillance and maintenance activities that may need improvements to improve plant safety.

- The results should identify candidate areas for regulatory improvements in terms of modifications to allowed outage time (AOT) and surveillance test interval (STI) requirements.

3.3.2. Configuration management activities [17–19]

During the operation of a nuclear power plant, the status of safety system components change due to failure, maintenance, or test. Changes in status result in changes in the plant configuration, which affects the risk level of a plant. Configurations of particular interest involve components that are unavailable (or down) at the same time.

PSAs can be effectively used to control risk from configuration occurrences. The principal benefit of managing configuration occurrences, i.e. configuration management, is the control of risk and assurance of safety. The added benefit is the effective use of plant resources. If configurations were managed so that critical, high risk configurations did not occur, then many risk significant events would be avoided, and the risk from operation would be small. Also, more operational flexibility can be provided for areas where risk implications are minimal. Thus, the purpose of PSA based or risk based configuration control is to detect and control plant configurations from a risk perspective. The achievement of this objective is difficult because the status of a standby component is often not apparent unless it is tested.

Configuration management can be started through an off-line application of PSAs, and it can be effectively implemented through an on-line system, which may require near-real time risk quantification. The requirements and capabilities presented here are intended to address both types of applications. For on-line applications, there are similarities with the application defined in Section 3.5.2.

Objectives

The basic objectives of PSA based application of configuration management activities can be summarized as follows:

(1) To prevent occurrences to the extent possible, of configurations of risk significant component outages due to test, maintenance, or failures.

(2) To identify risk significant configurations and provide guidelines for moving to safer risk levels when such configurations are realized.

(3) To provide flexibility in plant operation when risk implications are minimal.

PSA modelling requirements

PSA modelling requirements defined in Section 3.3.1 are all applicable. Additional requirements are explained below.

- A computer code must be available to quantify accident sequences with several components being unavailable at the same time.

- System models should be built in such a manner that reconfigurations during testing and maintenance can be taken into account efficiently in computations.

- Component unavailability models must have flexibility so that test and maintenance downtime contributions can be neglected (i.e. made equal to zero), because average downtime contributors used in PSAs are not applicable in conditional risk calculations for a given occurrence of a configuration.

- Component unavailability models should maintain flexibility for modelling demand and standby time contributions.

- Common cause failure modelling should be such that it retains the component designator so that dependency is accounted for different plant configurations. Dependency modelling may need to retain specific component designators for conditional risk calculation.

- Operator recovery errors modelled in accident sequences need to be reviewed to assure their applicability in different plant configurations.

- Systems should be modelled using a fault tree; the use of plant specific databases to obtain direct estimates of system unavailability should be avoided.

- For an on-line configuration management system with real time or near-real time risk capability features, a time dependent component unavailability model will be a useful feature. This model will allow the effect of specific times at which tests are performed to be directly incorporated in the risk calculation.

- For an on-line configuration management system, component unavailability models and initiating event frequencies should allow updating the parameters when experience data accumulated in the system show that such updating is necessary or at specific intervals, as desired by the user.

Data requirements

The data requirements defined in Section 3.3.1 also are applicable here. Additional data requirements are discussed below. Data requirements for an on-line system can be significantly higher than for the off-line system.

- Separating of demand and standby time related contributions to component unavailability, at least for the components whose surveillance test benefits are significant, is useful in deciding which components should be tested for a given configuration with high risk level.

- Present technical specification requirements, and any additional requirements, should be collected and maintained for use as a comparison. Cases where these requirements supersede other choices should be identified.

The following requirements apply specifically to an on-line configuration management system.

- Every time one or more components is detected to be in a failed condition or will be disabled for testing or maintenance, the status of other components should be known. The status should be entered into the computer.

- The duration of each configuration occurrence and the frequency of different configuration occurrences over a given period, e.g., one year, should be available.

- An on-line system also is an excellent tool for collecting plant specific data for the input parameters in the PSA. This collection includes hardware data, human error data, dependent failure data, and initiating event occurrence data. The data should be stored and assimilated in a manner that makes updating input parameters easier.

- Generic data, in the absence of plant specific data, can be the starting point of a configuration management system, where experience is used to update the input parameters.

Calculational capabilities

- PSA models should be able to quantify plant risk levels (e.g., core damage frequency) for different plant configurations where the status of components (available, unavailable, or reconfigured) are accounted for.

- There should be negligible error due to the truncation of minimal cut sets. Minimizing truncation error is important because several component statuses are changed to zero or one or to a different intermediate unavailability for a given configuration.

- Accumulated risk for a given duration of a configuration should be calculated. This calculation should also include the ability to calculate the risk due to configuration occurrences over a given period of operation.

- For a given configuration, priorities for checking alternate success paths (by checking other components to assure they are operable) should be provided.

- For an on-line system and real-time evaluations, risk levels and other information should be calculated in a timely fashion, i.e., in less than several minutes (3 to 5 minutes).

- Calculation of risk levels, other information, and operational decisions achieved through the system should be stored so that auditing can be performed effectively.

- Risk calculation features should be capable of performing time dependent evaluations, incorporating the last test times of components that can significantly affect the risk level.

Presentation of results

- The results will have different users. For the operating personnel, information is provided on when to take actions and what risk effective actions can be taken. For engineering personnel, information is provided on the calculated risk and the risk contributors.

- One effective way to present the risk information is a time-line, where the risk levels due to occurrences of different configurations are plotted.

- The frequency of occurrences of different configurations (in numbers) grouped into various risk levels should be catalogued to provide feedback to plant operating personnel.

- The critical configurations (i.e., combination of components) to avoid during operation should be listed. This list should be updated when any design and operational changes are made in the plant and incorporated into the PSA model.

- A list of functional alternate components, i.e. those components which can be tested to assure availability of alternate success paths, should be identified for critical risk significant configurations. Cases where additional testing is not expected to be beneficial and can only be burdensome also should be identified.

- A list of allowed downtime durations for different critical configurations also can be developed. In developing this list, care should be taken that the durations remain flexible and implementable, i.e. they are preferably grouped into three to four intervals. For example, allowed outage times (AOTs) of one, three, seven, and thirty days may be proposed, depending on the associated risk level.

3.3.3. Maintenance planning [18–23]

Planning preventive maintenance (PM), along with needed corrective maintenances, during normal power operation of a nuclear power plant is a substantial task for engineering and maintenance personnel. In many countries, preventive maintenances are allowed during power operation as long as technical specification limitations are followed; in some countries, separate requirements are provided for such maintenance. Realizing the potential benefit of preventive maintenance in preventing component failures, effective planning and execution of maintenance can result in significant risk improvements. PSAs can provide the basis for planning the activities to minimize any negative affect due to the unavailability of the maintained component for the duration of the maintenance. Methodology for reliability benefits of preventive maintenance, being developed by US NRC, can provide more refined planning and scheduling options.

Objectives

The objectives of maintenance planning activities can be summarized as follows:

(1) To develop master scheduling of maintenances of components using risk insights.
(2) To avoid any unnecessary increase in the risk level due to preventive maintenance activities.
(3) To allow flexibility in carrying out PM activities, where feasible.

PSA modelling requirements

The PSA modelling requirements are the same as those defined in Section 3.3.1. The additional requirements are as follows:

- The component unavailability model must have the flexibility to separate test and maintenance downtime contributions so that they can be equated to zero.

- The common cause failure contributions should be modelled in a manner so that they can be modified as needed for calculating of risk impacts of PM. If one of the components in the common cause component group is unavailable, then the common cause failure contribution will be different, and should be modelled for quantification. In many cases, common cause failure contribution may have to be neglected because when a component is taken down for PM it may be evident that common cause failure does not exist.

Data requirements

The data requirements are similar to Section 3.3.1. The additional requirement is as follows:

- A list of all the required PM activities and those activities that must be carried out together should be defined. The reasons for carrying out the activities together could be that the activities need the same personnel, or the same location, or that they use the same type of equipment, or the equipment belonging to the same division, or the same division or channel of different systems.

Calculational capabilities

- The average levels of core damage frequency need to be calculated for different options of PM activities.

- If PM activities are expected to repeat in cycle, then the calculations should be adequate for one cycle of PM activities.

- The calculation should be accomplished in a short time (within a half an hour) when it is to be used in planning daily activities. For longer range planning (e.g., for 12 weeks), the calculation time is not crucial, although faster calculation is convenient.

Presentation of results

- The level of the core damage frequency for different planned maintenance activities showing acceptable variation in the risk level should be plotted.

- A timeline plot of the conditional core damage frequency levels for different PM activities planned in the period should be calculated. The peaks in the levels, and the associated PM activities should be labeled.

- The PM activities that need to be modified to reduce the risk contribution should be identified.

- PM activities that are associated with higher risk levels should be identified for pre-determination and plant personnel should be notified when higher risk levels can not be avoided. Such activities should be implemented during operation only when other options have been determined to be unavailable or not feasible.

3.3.4. Surveillance test arrangements [24–26]

The objective of a surveillance test is to detect failure and degradation of components to assure their availability. If surveillance tests are performed in a defined order, i.e., they are placed in order in relation to each other, their benefit can be increased. PSAs can effectively aid in determining placement of the surveillance tests. However, the PSA based application must be tempered with the practical considerations involved in carrying out these surveillance activities. The implementation of such practices should not disrupt plant operation.

Objectives

The basic objectives in PSA application for surveillance tests arrangements are as follows:

(1) To obtain the risk-benefits that can be achieved through the placement of surveillance tests.
(2) To achieve early detection of dependent failures and plant configuration with significant risk implications.
(3) To minimize human error dependency in testing, maintenance, and calibration activities.

PSA modelling requirements

- Evaluations of system levels and function levels can be used to decide arrangements for surveillance tests. In a system level application, surveillance test placements within the system are optimized, and then accident sequence frequency level applications can be performed to make necessary adjustments.

- Time dependent models and evaluations are needed to quantify the effects of surveillance test placements.

Data requirements

- Component models identifying the standby failure rate of the component must be available. The effect of the assumption that component hardware unavailability is due to standby time related failure only, should be understood.

- Contributions of common cause failures contributions for hardware failures and for human errors should be realistically estimated.

Calculational capabilities

- Time dependent evaluations of alternate surveillance test placements should be performed to obtain average system, function, and plant level contributions. PSA averaged evaluation will not distinguish among different strategies for test placements, justifying the time dependent evaluations.

- Because of the burden associated with time dependent evaluations, it may be preferable to carry out system level calculations, and then perform accident sequence level evaluations.

- Sensitivity analyses should be performed assuming variations in common cause factors and in common cause contributions for human errors.

Presentation of results

- For each of the different strategies for surveillance test placements, both the peak and average unavailability contributions should be identified.

- Assumptions associated with the quantitative results should be clearly stated; common cause contributions for human errors eliminated due to staggered testing, and additional testing performed when a failure is detected should be used in decision making.

- A plot of average unavailability as a function of different test intervals should be presented for the different options studied.

3.4. REQUIREMENTS FOR EVALUATION OF REGULATORY AND INSPECTION APPLICATIONS

3.4.1. Guidance for inspection applications [27–29]

In many countries, nuclear power plants are routinely inspected by designated representatives (inspectors) of regulatory authorities to assure that the plant is operated within the limits and conditions set by the authorities, and that it maintains a ready status to respond to an accident condition. Typically, a wide variety of inspections are conducted. For example, the US NRC inspection manual requires specific daily, weekly, monthly, and longer inspection activities. Starting from daily tours of control rooms and walking down a plant, intensive examination of a plant's maintenance programme and a detailed review of the plant's ability to respond to accidents are covered. During these inspections, it is important that activities or aspects that are significant contributors to risk are focused upon. PSAs can be used to focus the inspection resources on most risk important areas. PSA based insights can be used to guide the inspector's effort once an inspection programme has been selected. Risk based inspection guidance developed for a plant can be used alongside the existing inspection manual.

Objectives

The objectives of PSA based guidance for inspection applications can be summarized as follows:

(1) To provide an information base to the inspectors, based on PSA insights, for effectively carrying out inspections.

(2) To prioritize the activities within each of the inspection procedures, i.e., for example, to prioritize the safety systems to be inspected, or the system failure modes of a specific system for inspection.

(3) To list in detail the dominant risk contributors at system, accident sequence, and core damage frequency levels.

PSA modelling requirements

- A Level 1 PSA that includes internal initiating events and detailed system fault trees is desired. External Event PSAs will help identify inspection activities relating to occurrences of fire, flood, and earthquake.

- The PSA should include important systems, i.e. front line systems and support systems. These system models should be distinct so that dominant contributors for system unavailability can be evaluated.

- The system models should be detailed such that various contributors affecting a train unavailability are identified.

- Human errors, including errors of operation, recovery errors during test, maintenance, and calibration, and any dependency for these errors should be adequately modelled.

- Common cause failures should be adequately modelled. Realistic estimates should be used both for common cause failures, and human errors, mentioned above; otherwise, other contributors may be masked.

- Human and common cause contributors estimated to be negligible at the accident sequence level should be retained in the model because they may be important at the system level. Also, this will allow sensibility evaluations for updating.

Data requirements

- Data requirements are the same as that for the basic PSA.

- Locations in the control room of the various equipment identified in the system walkdown list, and the important line-up errors, should be available.

Calculational capabilities

- The primary capability is the ability to calculate importance measures associated with various basic events in PSA, i.e. equipment failures, human errors, and common cause failures. There should be negligible errors due to the truncation of minimal cut sets in deriving these importance measures.

- The PSA should be capable of evaluations at the system level. This capability should allow system importances to be evaluated and the dominant failure modes for the system to be identified.

Presentation of results

- A brief summary of the dominant accident sequences for the plant and a description of the individual accident sequences in a language that is understood by the inspectors (avoiding jargon) should be provided.

- The systems should be ranked in order of priority for inspections. Ranking for general inspections when no knowledge of a specific system problem is available (using Fussel–Vesely importance measure), and the ranking of systems when specific system problems are known (using Birnbaum importance measure) should be provided.

- Matrices of system dependency, including interactions between front line and support systems, and support–support system interactions should be presented.

- For each system, the success criteria and important failure modes should be identified. For a system walkdown, a list of risk important components, their desired positions during operation, and the locations in the control room should be presented.

- A list of equipment and their important failure modes should be provided, for detailed maintenance inspections.

- A list of risk significant surveillance and calibration activities should be included for guidance in inspection of surveillance and calibration at the plant.

- For plant operations inspections, important human errors associated with normal system line-ups should be listed.

- Important common cause contributors to the plant should be gleaned from the PSA and presented for the inspectors.

- Important human errors should be identified for the inspectors. These errors should be categorized into various groups for convenient use: post-accident errors vs pre-accident errors; errors of operation, calibration, restoration in test and maintenance, and recovery; and others, as appropriate.

3.4.2. Modification of allowed outage times (AOTs) and surveillance test intervals (STIs) [15, 30–33]

The allowed outage time (AOT) of a component is the period during plant operation in which the component may be inoperable, i.e., if a component is found failed, it should be repaired within the defined AOT, or the plant must be shutdown. The basic philosophy behind the AOT is that component unavailability due to repair of failures is minimized and that the readiness of a plant to respond to an accident is assured. However, the difficulty with individual component AOT is that in many cases these AOTs are unnecessarily restrictive, resulting in incomplete repairs and undesirable plant mode changes. The AOTs were originally defined based on available engineering judgements, and as a plant accumulates operating experience, it may identify AOTs whose modifications are desirable both from safety and operational viewpoints.

A plant may seek modification to one or more of the AOTs because of any one or more of the following reasons:

(a) The AOT is unnecessarily restrictive, and failures experienced during operation required longer time for orderly repair.

(b) The AOT for the component is not clearly defined in the technical specifications, and creates ambiguity between operating personnel and regulatory representatives.

(c) The current AOT requirements are unnecessary from a risk perspective, and impose undue burden on the operating staff.

Surveillances are performed on standby safety system components to detect any failures that may have occurred and would have otherwise gone undetected. The basic intent of surveillances is to promptly detect failures so that repairs can be performed to assure successful operation in case of a demand in accident conditions. Like AOTs, these requirements also are based on engineering judgements, and component performance indicates that in many cases, the required frequencies of surveillance are unnecessarily high. At the same time, many adverse effects of surveillances, e.g., test caused transients, test caused wear of equipment, test caused unavailability, also were observed to become significant contributors. At the least, unnecessary surveillances divert attention away from other risk important activities.

A plant may seek modification to one or more of the STIs because of one or more of the following reasons:

(a) The burden of surveillances is too high and the reduction in surveillances will not result in any significant increase in risk.

(b) The adverse effects of surveillances are judged to be substantial, and the benefit of the current surveillance interval is not significant.

(c) The risk-benefit of surveillance is very small, and resources can be better spent in other activities.

This application is similar to the applications defined in Section 3.3.1. As mentioned in Section 3.3.1, areas of modifications can be defined using risk based evaluation of surveillance and maintenance activities. In fact, AOT/STI modifications are a natural follow-on to the applications defined in Section 3.3.1, because the additional resources required are minimal.

Objectives

The objectives of this application can be summarized as follows:

(1) To provide risk based evaluation and justification for modifying AOT/STI requirements.

(2) To bring more risk perspective to AOT/STI requirements in the nuclear power plant technical specifications.

(3) To reduce the burden of regulatory requirements without compromising safety during the operation of a nuclear power plant.

PSA modelling requirements

PSA modelling requirements are the same as those defined in Section 3.3.1.

Data requirements

The data requirements include those defined in Section 3.3.1. Additional requirements are defined as follows:

- For AOT modifications, any repair data or engineering evaluation showing that repair time longer than AOT may be needed, should be presented.
- For extending AOTs, data estimation of repair times for the new AOTs should be presented.
- For STI modifications, test intervals recommended by manufacturers should be obtained.

Calculational capabilities

- The primary capability is the ability to calculate accident sequence frequencies and core damage frequency for components being unavailable (down) and available (up) with negligible error due to the truncation of minimal cut sets.
- In quantifying the risk level for a component being down, the reconfiguration of other components should be accounted for.
- In quantifying the effect of a modification being proposed, the PSA model and input data should be updated, incorporating prior changes to AOTs and STIs.
- In quantifying the risk impact of several changes of surveillance test intervals, the individual effects obtained separately cannot be added to obtain the total effect, because the interaction effects due to several changes are neglected in this approach. Updated models incorporating the changes should be used to obtain the total effect.

Presentation of results

- The results should present a quantitative assessment of the modification being proposed, including the quantification of the increased (or decreased) risk, if any, due to the changes and the estimated risk level (e.g., CDF) with the changes.

- For AOT modifications, both the single AOT contribution, i.e. the risk impact given a component failure, where the entire AOT is used, and the expected or projected yearly AOT contribution, i.e. the risk impact for the expected number of component outages in a year assuming the entire AOT is used for all occurrences, should be evaluated. The risk impact evaluated in this manner is conservative, because typically repairs are completed in shorter periods compared to the AOT.

- For STI extensions, an assessment of the benefit of testing, i.e., risk averted due to detecting failures by the test, should suffice. Where quantification of risk benefit of test does not justify the extension, quantification of adverse effects may be necessary.

- For STI extensions, impact on common cause failures, if dominant, should be assessed and presented.

- Results should clearly state the assumptions made in the model to quantify the effect under the changed requirements being proposed. For example, if the same repair distribution is being used to obtain the mean repair time for the proposed extended AOT, then it should be clearly stated.

- Sensitivity analyses should be presented for, at least, the important assumptions in the evaluations.

- Qualitative assessments and justifications should be presented for important non-quantified aspects.

- Any reliability programme activities or operational activities being proposed, along with the modification, should be stated and the implementation plan provided.

3.4.3. Limiting conditions of operation (LCOs) action statements [26, 34]

The limiting conditions of operation (LCOs) in nuclear power plant technical specifications define the conditions set by the regulatory authorities for operating the plant. Typically, if these conditions are violated, the plant is required to change its operational mode, i.e. transfer to a shutdown state from a full power operational state. The intent of such action requirements is to move to a safer mode of operation. For example, if a safety system component is found failed and is not repaired within the specified AOT, then the action statement would require that the plant be transferred to a shutdown state.

In case of failure(s) in systems that are required to shut the plant down, the risk of shutting down may be significant in comparison to the risk of continued operation. This is particularly true in the case of several failures in these system, where the choice from risk consideration may be to continue operation with precautions. Using the basic PSA of the plant, methodologies are being developed to address such situations whereby action statements can be redefined based on risk comparison of the available alternatives. Failures in residual heat removal (RHR) and standby service water (SSW) systems require this type of application. In case studies conducted so far, in rare, multiple failure situations in RHR and SSW systems, the shutdown constitutes higher risk compared to continued operation, and the current action requirement for immediate shutdown is inappropriate and should be modified.

Carrying out this type of application requires significant additional effort and extensions of the basic PSA. As explained in the requirements presented below, information relating to transfer to shutdown state and associated data are required, which is expected to be collected as part of a shutdown PSA, and not in the basic PSA.

Objectives

The objectives of this type of application can be summarized as follows:

(1) To evaluate action statements requiring shutdown in standby safety systems needed for shutdown.

(2) To provide risk effective alternatives to existing action statements and avoid shutdowns, if shutdowns constitute greater risk.

(3) To modify technical specifications and to present guidance for operators to follow in failure situations where risk of shutdown is higher.

PSA modelling requirements

The PSA modelling requirements include those identified in Section 3.3.1. Additional requirements are presented below.

- Modelling of various stages of the shutdown cooling phases incorporating the support system and the operator interactions are required.

- Any initiating event not modelled in the basic PSA, but having greater importance during the shutdown phases should be identified and modelled. Specific examples are those events that challenge RHR and render part of the RHR system unavailable.

- Different recovery paths applicable at various stages of shutdown in defining successful near-mission failure and failure scenarios should be modelled. Event sequence diagrams (ESDs) were used in the case studies conducted so far.

- Modelling of available time margins for scenarios of suppression pool heatup under different conditions are required. Both total and partial loss of pool cooling under loss of coolant accident (LOCA) and transient conditions may need to be evaluated.

Data requirements

- Detailed data on the failure events of the systems whose action statements are being evaluated are required.

- Specific test arrangements followed and/or required for the systems and components during normal operation and in case of accidents are required.

- Initiating event data during the shutdown phases of the plant should be compiled. Data from the plant being evaluated are not expected to be sufficient, thus data from similar plants must be collected.

- Data are required on operator actions during these transient phases where different recovery paths are modelled. Due to lack of actual data, databased on human reliability analyses of similar scenarios may be used.

- Data for developing the behavior of suppression pool temperature are required. In the case studies available, a crude heat transfer model for the suppression pool was used. Such data are available from the plant safety analysis report.

- Data are required on the repair time distributions for major components in the systems.

- Plant specific common cause data for these components will be useful, because these data may play an important role in defining additional testing requirements in failure situations.

Calculational capabilities

- Basic PSA computational tool, which can quantify the risk of continued operation for failure situations in safety systems should be available. This is similar to the capabilities defined in Section 3.4.2.

- Capability to quantify risk associated with transition states during shutdown is required.

- In quantifying the risk associated with shutting down, time dependencies should be considered because the risk level can vary significantly during this period. At least, the shutdown period should be divided into several discrete phases as may be necessary to effectively represent the associated risk.

- Capabilities should be available to perform sensitivity studies for various alternative action requirements that may be studied to resolve the issue. Sensitivity analyses for timing different actions, data uncertainties, and modelling uncertainties should be performed.

- Capabilities to evaluate core damage frequency level for continued operation and for shutting down will be required to satisfy the requirements.

Presentation of results

- A comparison of risks for continued operations versus shutting down in different LCO conditions (single and multiple failures) including both the risk frequency as a function of time and the accumulated risk as the time progresses, should be presented.

- Risk quantification should be presented for the alternatives. This quantification should present the risk, comparing the alternatives, given that the LCO condition has taken place.

- Sensitivity analyses should be presented for the important assumptions and data variabilities. Effects of such variabilities on the alternative also should be discussed.

- Procedures for implementing the chosen alternatives also should be presented. Conceivably, the changes to the Technical Specification can be minimal and detailed guidance may be provided for operational use.

3.4.4. Applications to determine quality assurance requirements [35, 36]

Quality assurance (QA) requirements are an integral part of regulatory requirements to assure that equipment installed in nuclear power plants are of proper quality and will perform the desired functions, as defined. Both for safety and availability reasons, equipment used in nuclear power plants should be quality assured. However, because of the large amount of equipment involved, the cost of QA can be very high where safety improvement due to the requirements is not clearly known. Many argue that the quality assurance process rarely rejects equipment; thus, the actual safety benefit is, at most, marginal.

One effective way to bring a balance between the plant burden in abiding by QA requirements and assuring proper quality of equipment is to focus QA requirements for equipment important to safety. PSAs can be used to determine list of components which should remain under QA, and also define where such requirements can be relaxed. There is no PSA application for defining QA requirements and practical and implementation problems associated with QA are not clearly known. Guidelines are given here for starting such an application.

Objectives

The objectives in PSA applications to define QA requirements are as follows:

(1) To define the QA requirements for nuclear power plant equipment using probabilistic and risk based arguments.

(2) To remove equipment from the QA list where safety implications are minimal and cost savings are high.

PSA modelling requirements

PSA modelling requirements are same as those defined in Section 3.4.1.

Data requirements

In addition to the basic PSA data, the following requirements should be considered:

- Any available data comparing the performance of similar equipment installed, with and without QA should be required.

- Any engineering data showing that newly available equipment, not quality assured, will have improved reliability compared to currently used equipment, due to advances in technology, are required.

- An estimation of increase in the failure rate of an equipment, if QA is removed should be provided.

Calculational capabilities

- The primary capability is the ability to calculate importance measures associated with various equipment failures in the PSA. This capability implies that conditional core damage frequency, accident sequence frequency, and system unavailability are calculated for equipment being unavailable (down) and available (up). Error due to the truncation of minimal cut sets should be negligible.

- The PSA tool should be capable of performing sensitivity analyses, i.e. increase in CDF or other measures for increase in the failure rates, for one or a group of equipment.

Presentation of results

- Quantification of the effect of increased failure rate of the equipment, if the QA is proposed to be removed, on the risk parameters, e.g., core damage frequency, accident sequence frequency, and system unavailability, should be presented.

- When a group of equipment is being considered for removal of QA requirements, the combined effect of changing the requirements should be provided.

- Sensitivity analyses showing the effect of increased failure rates of the equipment to be removed from QA list should be presented.

- If the increase in the failure rate of the equipment due to the removal of QA requirements is judged to be limited, then analyses should be carried out to justify such an argument.

- The time at which any design defects present in the equipment removed from the QA list will be detected by the normal plant test and maintenance policy should be identified.

3.5. REQUIREMENTS FOR OPERATIONAL EXPERIENCE ASSESSMENT APPLICATIONS

3.5.1. Incident analyses (off-line evaluations) [37-39]

Feedback from analyzing events occurring during the operation of a nuclear power plant is an essential element in assessing and assuring continued safety at the plant. The incidents reported by the plant are of varying significance. PSAs can be an important tool in obtaining a quantitative assessment of the risk significance of the events or incidents occurring at a plant site.

All incidents reported by a plant are not necessarily candidates for evaluation by a plant specific PSA. Some qualitative screening of the incidents are necessary to identify potentially significant ones. Those incidents which involve a portion of the accident sequences defined in PSA, i.e. where a challenge to safety systems occurred with partial failure of such responses, or where partial failures are observed which would have resulted in an inadequate response to unexpected or significant challenges, are candidates for this type of evaluation.

Objectives

The objectives of this application can be summarized as follows:

(1) To obtain a quantitative estimate of the risk significance of the events occurring at a plant site.

(2) To detect any design or procedural deficiency using PSA insights for instituting improvements, as necessary.

(3) To obtain any trends or patterns of operation related problems at the plant site for corrective actions.

PSA modelling requirements

- A Level 1 internal event PSA will be an adequate starting point for this type of analysis. An external event PSA can be a useful addition in the analysis as experiences with internal event PSA are gained.

- Detailed extensive models of the systems and accident sequences are required to accurately estimate the likelihood of an accident. However, because the focus will be on more significant events, typical PSA models are adequate to obtain estimates of magnitude of the accident likelihood, given that the event has occurred.

- Modelling and interactions of support systems with front line and other support systems are needed to address many risk significant events and to obtain realistic estimates.

- Detailed system train level models incorporating system interactions and common cause failures, where components belonging to the trains are identified, can be effectively used to start this type of evaluation.

- Operator recovery actions should be adequately modeled to obtain realistic estimates. This model includes assessing recovery actions, given an event has taken place, i.e., reviewing the recovery actions credited in the PSA for their applicability, and assessing the need for incorporating any new ones may be necessary.

- Modelling of additional common cause failures that are experienced in the operational event, but are not included in the basic PSA model may be required.

- Accident sequences considered to be non-dominant in the base case PSA are expected to be required and should be retained for incident analyses.

Data requirements

- A detailed description of the operational event to be evaluated, which can be used to relate the incident to the PSA in terms of the accident sequences affected, the hardware failures and operation errors occurred, and the recovery actions successfully completed or could have been completed, will be needed.

- A review of the human errors rates and an estimation of new human error rates assessed that are likely based on the evaluation of the operational events experienced at the plant, including recovery actions, may be necessary.

- An estimation of common cause failures indicated by the event, but not modelled in the PSA, requiring common cause failure data for such failures from other sources is required.

Calculational capabilities

- The PSA model should be available in a computer code so that the operational event or incident can be easily manipulated and evaluated.

- A commonly available PSA code that allows the regeneration of system and sequence minimal cut sets, and requantifies accident sequence frequencies, where basic event probabilities are modified, will be adequate.

- A PSA model must be capable of requantifying the accident sequences considered negligible in the base case analysis. To perform the requantifcation, the code, at least, should maintain the logic of a large number of accident sequences originally modelled in the PSA.

Presentation of results

- The accident sequences that were affected or could have been affected by the operational event or incident being analyzed should be presented as graphs. Typically, this will involve identifying the PSA event trees for various initiating events and highlighting the affected sequences.

- The basic events in the PSA affected by the incident and the PSA assumed probability for the events should be summarized. This summary should include the human errors, including recovery actions and the common cause failures assessed in the evaluation of the incident.

- A list of the conditional accident sequence frequencies and the core damage frequency also should be compiled.

- The assumptions made in quantifying the incident should be identified, and any sensitivity analyses performed to address the issue should be presented.

- Key contributors to the accident sequences also should be identified. This will require reevaluating risk importances of basic events.

- Key features that have prevented the incident from becoming serious also should be identified. This will require using risk importance measures, if quantitative assessments are desired.

- A summary of the lessons learned focussing on any modifications or procedural changes that may be desired should be compiled. This summary should be prepared in a language that can be understood by personnel who are not involved in PSA, i.e. jargon must be avoided.

3.5.2. On-line real time assessment of operational events [40]

With the availability of powerful microcomputers, the use of PSA as an on-line risk monitoring device is increasingly being suggested and discussed. For an on-line system, a fast running PSA tool with the capability to quickly quantify accident sequence frequencies through the regeneration of cut sets for a given input and to be fed with the status of component and other relevant conditions, is envisioned. Such a system can be used to obtain a quantitative assessment of the risk significance of the events happening at the plant.

Although there are several promising PSA codes, there is no on-line PSA tool for assessing operational events. (The Essential Safety Status Monitoring System at the Heysham plant in the United Kingdom is directed towards maintenance planning and defining maintenance durations). Perhaps developing the computer code is feasible, but integrating such a tool with plant activities and a database for assessing operational events is the difficult part.

Recognizing that such an application of PSAs is further away than the others being discussed, we present PSA requirements and capabilities as we envision them now. The discussions below have similarities with those presented in Section 3.3.2 for on-line application of plant configuration management activities.

On-line analyses of operational events have merits, but they do not replace off-line incident analyses.

Objectives

The objectives of the on-line assessment of operational events can be summarized as follows:

(1) To obtain an immediate assessment of the risk significance of an operational event at a plant.

(2) To identify actions that may help prevent a relatively unimportant event from becoming a significant one.

(3) To screen and provide input to detailed operational event analyses that are necessary for preventing future occurrences.

PSA modelling requirements

Many of the modelling requirements are the same as those discussed in Section 3.5.1. The first five requirements, are applicable here. The last two requirements should be neglected, because revised modelling of operator recovery errors and common cause failures are not feasible in an on-line system for timely incorporation into the analysis. Events requiring such evaluations should be screened for future off-line analysis, as defined previously in Section 3.5.1.

The additional requirements are presented below:

- Component unavailability models should be modified and presented as a function of time from the last test, when it was detected to be operational or repaired to an operational state. This also requires separating demand stress and stand-by time related contributions.

- Component unavailability models and initiating event frequencies should be updated using experiences being collected by the on-line system. These models and frequencies can be updated when sufficient experiences are accumulated to indicate that a revised estimate is necessary, or at specific intervals, as desired by the user.

Data requirements

- Data requirements are the basic data used in the PSA and the experiences accumulated in the system for updating the parameters.

- If a time dependent component unavailability model is used, then one set of test times for the components reflecting the last test time should be retained.

- The status of components and occurrences of initiating event frequencies identified by plant parameters or by the operator should be available. This information should be entered, on line, into the computer.

Calculational capabilities

The calculational capabilities include those defined in the Section 3.5.1. The additional capabilities are defined below:

- The risk level and other information to advise operators should be calculated in a timely fashion, i.e., in less than three to five minutes.

- Key features useful in preventing the condition from deteriorating further, within the limits of the PSA, should be identified and presented to the operator.

Presentation of results

- A quantitative evaluation of the risk level associated with the event should be presented, along with a qualitative representation (high, medium or low risk significance).

- The accident sequences that were affected and are the dominant contributors to the risk, should be delineated.

- From the key features that were useful in preventing the condition from deteriorating further, specific actions desired by the operator should listed.

- The events that require further detailed evaluations should be screened.

3.6. Requirements for applications in assessment and mitigation of ageing effects [41, 42]

As nuclear power plants age, it is important to assure that the safety level of the plant is maintained all through its operating life. Even as the plants approach the end of the currently designed operating life, decisions need to be made on whether the plants should be relicensed.

PSAs provide a useful basis for assuring the safety level of the plant with the age and for determining specific ageing mitigating activities that may be undertaken both to assure safe operation and as a justification for extending the useful life.

The recent IAEA report on The Use of Probabilistic Safety Assessment in the Relicensing of Nuclear Power Plants for Extended Lifetimes, IAEA-TECDOC-547 [42], provides useful guidance on PSA application in ageing and relicensing of nuclear power plants. In this section, we present an overview of requirements and the capabilities to assess and to prioritize mitigation activities for ageing plants, using a PSA. Detailed guidelines and information can be obtained from the IAEA report.

Two basic areas of PSA application are considered useful in studying ageing effects:

(1) Assessing plant level safety implications of ageing effects on components and structures.
(2) Risk based prioritization of ageing management.

Requirements and capabilities of a PSA are similar in both these applications; they are presented together. In defining these requirements, we recognize that the methodology is in a developmental stage in many cases.

Objectives

The objectives for assessing safety implications of ageing effects are as follows:

(1) To assess any changes in the plant safety level through estimating core damage frequency level with the age of the plant.

(2) To evaluate the impact of safety issues, relevant to ageing, associated with the plant.

(3) To obtain insights based on sensitivity evaluations of plant improvements to be considered for assuring safer operation in later life (more than 30 years of operation) of a plant.

The objectives in a risk based prioritization of ageing management activities are as follows:

(1) To identify specific test, maintenance, and renewal activities which can be performed to mitigate ageing effects and control the core damage frequency level.

(2) To identify areas resulting of large uncertainty in the PSA evaluations, that require additional data and evaluations.

(3) To obtain sensitivity on prioritizing ageing management activities due to different assumptions of ageing effects in the methodology.

PSA modelling requirements

- PSA modelling requirements include the basic Level 1 PSA requirements in terms of initiating events, event trees, system fault trees, common cause/dependency modelling, quantification rules, and associated databases. External event initiators shall be included; however, for convenience, evaluations may be started with internal events.

- The system fault trees, both for front line and support systems, need to be developed in sufficient detail so that ageing effects of individual components can be modelled. Many components with negligible contributions in the basic PSA can be important contributors in an ageing PSA, and accordingly, care should be taken to include such components.

- Treatment of passive components in a basic PSA is generally inadequate for ageing assessments. Although, at this time, there are no approaches for handling the degradations of structures and materials in a PSA, the modelling of passive component failures in the system logic should be improved so that at least sensitivity evaluations can be performed.

- Component unavailability should include age dependent failure contributors, i.e. the modeling should be able to accommodate ageing effects in the failure rate, demand failure contribution, and maintenance duration.

- Component test and maintenance models should include the effects of test and maintenance in terms of 'good as old' and 'good as new' cases, and should include replacements and renewals of components. Because detailed models are not available, simplified models with conservative assumptions are acceptable.

- Systems interaction and dependency modelling in the basic PSA should be evaluated to determine if any additional dependency, due to age related degradation of components and structures, should be included.

- Computer packages that can handle models incorporating ageing effects in various aspects of quantification shall be used. This use should allow concomitant ageing effects on multiple components being evaluated. The Taylor series approximation method can be used.

Data requirements

- Plant specific data on component failures and initiating events over a sufficient period (e.g., 10–15 years) shall be available. If ageing assessment is being carried out for a plant with less than 10 years of operating life, then the available plant specific data can be combined with expert judgement, if needed. Data shall be used to determine parameter of age dependent component unavailability and initiating event frequency.

- Records of maintenances performed on components and the duration of maintenance should be available. The maintenance durations should be analyzed to determine any ageing effects (e.g., increased maintenance to mitigate ageing effects resulting in increased maintenance unavailability), to incorporate into the PSA evaluation.

- Any replacements and renewals of components should be clearly identified.

- Due to the lack of availability of ageing data, expert opinions may need to be used to obtain ageing parameters. Use of expert opinion, as a replacement of plant specific data, should be minimized to the extent possible. When such opinions are used, a structured process must be followed.

- Data requirements for passive components are not clearly defined due to the lack of well defined approaches. For the passive contributors included in the model, expert generated parameters or ranges of parameters for sensitivity evaluations should be developed.

- For the estimated parameters, uncertainty ranges shall be developed. These uncertainty ranges shall at least be used in the sensitivity evaluations.

- Common cause parameters (e.g. ß in the ß-factor model) should be evaluated to assess if they are influenced by ageing effects. Observed occurrences of common cause failures should be analyzed for ageing effects, if sufficient data are available; otherwise, constant common cause parameters are acceptable.

- Human reliability analysis should be revisited to assess if the ageing effect on component/structures changed any of the human error analyses.

Calculational capabilities

- The average core damage frequency should be calculated at intervals of 5 years using the age dependent parameters and models.

- Before truncating any cut sets in the quantification phase, an assessment must be made on whether the cut set with the incorporation of the ageing effect has the potential of being a significant contributor, i.e., care should be taken to minimize any underestimation due to the truncation.

- Risk significant contributors at different intervals should be identified through quantitative evaluations.

- Flexibility should be available for conducting relatively extensive sensitivity analyses with respect to changes in the input parameters, modelling parameters, and operational parameters (e.g., test interval, renewal intervals, effects of test and maintenance.)

- Effects on average core damage frequency for different options in test and maintenance activities, plant design features, and backfit considerations should be determined for comparison and implementation.

- Uncertainty analyses features that can incorporate ageing effects modelled in fault/event trees should be available for PSA quantification.

Presentation of results

- The assessment of core damage frequency for different intervals of the plant with associated uncertainties should be presented in tables or in graphs. Large uncertainties may be involved in these evaluations. Cautions should be provided that results are more useful as a relative measure and for sensitivity evaluations rather than their use as absolute values.

- Dominant contributors to ageing risk should be prioritized. Sensitivity analyses with respect to the prioritization also should be presented; any changes with prioritization due to variability in modelling and data, should be discussed.

- Clear delineation of different ageing mitigating features studied and their effects on the assessed core damage frequency levels, along with the associated uncertainty ranges, should be presented.

4. RECOMMENDATIONS FOR APPLICATION PRIORITIES

This section prioritizes the PSA applications discussed in this report. The applications are categorized into three groups. All the applications cannot be carried out together; such a large undertaking, even if the resources are available, is not desirable. Some of applications naturally follow others, and in other cases, valuable experiences can be gained from earlier applications, which can be effectively used to conduct later applications. Applications can be sequenced, resulting in cost savings. With these considerations and the resource constraints in mind, we present a qualitative grouping of different phases of applications in Table I. It is quite possible that because of a specific need of a particular plant, the order of applications will have to be altered.

TABLE I. RECOMMENDATIONS FOR PRIORITIZING PSA APPLICATIONS IN THREE PHASES

PSA applications	First phase	Second phase	Third phase
I. Design and procedure adequacy evaluations and improvements			
1. Evaluation of design features and procedures	F		
2. Consistency with safety goal(s)	F		
3. Decisions on design modifications	F[a]		
4. Decisions on backfits		S[a]	
5. Important procedures requirements and operator training		S	
II. Operational activities			
1. Evaluation of surveillance and maintenance activities	F		
2. Configuration management activities			
– Off-line evaluations		S	
– On-line system			T
3. Maintenance planning		S	
4. Surveillance test arrangements			T
III. Regulatory & inspection applications			
1. Inspection guidance		S	
2. Modification of allowed outage times/surveillance test intervals		S	
3. Limiting conditions of operations action statements			T
4. Quality assurance		S	
IV. Operational experience assessment			
1. Incident analyses	F		
2. On-line or real time monitoring			T
V. Ageing assessment			
1. Safety implication of ageing effects			T
2. Prioritization of ageing management activities			T

F: Recommended first phase application.
S: Recommended second phase application.
T: Recommended third phase application.

[a] PSA requirements and capabilities are similar for applications concerning decisions on design modifications and on backfits. However, in the case of design modifications, the available information is more limited, leading by necessity to somewhat more relaxed requirements. These two applications were assigned to different phases, because for a plant being designed or constructed a PSA should be carried out in parallel and the design related decisions should be made before the start of operation. PSA based decisions on backfits are, on the contrary, normally made using completed PSAs as a follow-up application.

Appendix

LESSONS LEARNED FROM INTERNATIONAL PEER REVIEWS OF PROBABILISTIC SAFETY ASSESSMENTS

Independent peer reviews of a PSA are an integral part of any PSA programme. Since 1989 the IAEA has been providing International Peer Review Service (IPERS) on request from Member States. The general objectives of the IPERS programme are to bring international experience into the review process and give guidance on what improvements should be made on the analytical approaches used. Specific objectives of the review can be adjusted to the needs of a particular Member State. The reviews are carried out in accordance with procedures developed by the IAEA [2], which, in turn, are consistent with the IAEA procedures for conducting PSAs [5].

The IPERS reviews have resulted in a large number of insights concerning the potential for improving modelling. A list of specific modelling problems that are frequently observed in the PSAs reviewed is presented below [3]. Because most of these deficiencies lead to limitations of the uses of PSAs, the list is reproduced here for the benefit of analysts who are responsible for defining PSA requirements, as well as the reviewers of PSA applications.

A.1. INITIATING EVENT ANALYSIS

(1) Incomplete list of initiating events.

Certain initiating events screened out without sufficient analysis. This applies, in particular, to common cause initiators caused by the loss of support systems. Such initiators have been identified as significant contributors to core damage frequency in many PSAs. Systematic approaches to assure that the initiating events list is completed (e.g. Master Logic Diagram) are regrettably seldom employed.

(2) Invalid grouping of initiating events.

Simplifications by grouping dissimilar events under a more conservative event and adding the frequencies. This approach might not be conservative for common cause initiators which have severe impacts on mitigating systems. Mismatches in identified LOCA sizes and associated mitigation systems flow requirements have been observed.

(3) Initiating event frequencies based on excessively optimistic assumptions.

Use of not directly applicable foreign experiences and/or censoring data on the basis of rectification (the problem has been fixed) may result in optimistic estimates. Loss of off-site power frequency has frequently been underestimated due to such approaches. Possible underestimation of large and medium LOCA frequencies due to taking unsupported credit for a leak before break postulate, also has been identified.

A.2. ACCIDENT SEQUENCE ANALYSIS

(1) Inadequate justification of success criteria.

Due to the lack of PSA specific thermal-hydraulic analyses for LOCAs and transients, best estimate success criteria are frequently not established in a convincing way. This inadequacy leads usually to overconservative estimates, but in some cases unjustified credit has been taken, and certain potentially significant functional dependencies have been ignored. Lack of deterministic best estimate analyses also compromises the grouping of initiating events on the basis of similar plant status.

(2) Lacking definitions of core damage categories.

Different core damage categories, as well as successful end states, also need to be defined in a Level 1 PSA to differentiate between different levels of severity of damage and consequences. For some plants core uncovery may not be an acceptable substitute for core damage; this applies to situations where there are relatively long recovery times to mitigate core damage after core uncovery starts.

(3) Exclusion of certain systems based on prejudged insignificant impact.

This exclusion can limit the usefulness of the PSA as a tool for operational support. Prioritizing training and upgrading procedures via the PSA become difficult. Specific examples for BWRs include the boron injection system, recovery of the main feedwater, and the use of the main condenser to depressurize the reactor.

(4) Shortcuts and simplifications in the development of event trees.

These shortcuts and simplifying assumptions are often conservative, but in some cases, could be non-conservative, because the paths of the event trees, which are neglected, could be important contributors, particularly for subsequent Level 2 evaluations and for 'living' PSA applications.

A.3. SYSTEMS ANALYSIS

(1) Insufficient degree of detail in fault tree models for support systems.

There is a danger that subtle but significant dependencies in electrical power supply systems (e.g., through breakers, overcurrent protection switches) or in reactor protection systems (e.g., actuating logic) might be missed if the logical models are not decomposed down to a sufficiently low level.

(2) Neglect (or 'lumping' with failure to start contributions) of failure to run contributions and other spurious failure modes.

These contributions have been found significant in many PSAs and should be identified explicitly in the fault trees.

(3) 'Lumping' of components together to be analyzed as a single basic event.

'Lumping' of components has advantages in restricting the size of the analysis. However, the usefulness of the results can be inhibited; for example the study could not be used for optimizating maintenance and test intervals for individual components.

A.4. COMPONENT DATA

(1) Improper use of generic data.

This improper use leads often to excessively optimistic data, especially when experience originating form optimal conditions is directly transferred to a significantly different operating environment. In many cases, no attempts are made to update the generic experience using the actual plant records.

(2) Lack of clear definition of component boundaries.

It is frequently unclear what the component failure rate covers and does not cover. Generally, it should not cover separately modelled support system contributions and interfaces with other

components. Imprecise or a lack of definition of component boundaries leads to inconsistencies and either double counting or underestimation in the quantification of accident sequence frequencies.

(3) All failure rates given in per demand units.

This type of estimation of failure data does not explicitly take into account differing test intervals which can have significant effects. Also, when test intervals are not explicitly included, the PSA is not able to be used for applications involving modifications of Technical Specifications.

(4) Incorrect representation of component repair times, maintenance downtime and component test duration times.

The values used for these contributions should reflect actual conditions and be based on plant specific information. Thus, component restoration time includes not only the actual repair time, but also administrative time needed to initiate repair. The latter should reflect station policies, availability of personnel, and replacement parts.

A.5. TREATMENT OF DEPENDENCIES

(1) Modelling of functional and shared equipment dependencies.

This modelling is basically addressed in a conventional way, i.e. either by use of a large event tree/small fault tree approach or a small event tree/large fault tree approach. The first approach seems to be more prone to overlooking important dependencies, at least when the study is carried out by relatively inexperienced analysts. One of the studies reviewed used reliability block diagrams instead of fault trees for systems modelling. This approach creates major difficulties in the linking of system logics, representation of support system dependencies, and when modelling, e.g., reactor protection system. For other comments relevant for this category of dependencies, see points (1) and (3) in paragraph A.2 and points (1) and (3) in paragraph A.3.

(2) Coverage of common cause initiators.

Incompleteness in treating common cause initiators related to equipment are commented on in points (1) and (2) in paragraph A.1. Many of current PSAs do not include external events in the scope, in spite of their importance according to international experience.

(3) Use of bounding assumptions and conservative success criteria.

Such approaches have frequently masked the effect critical safety engineering insights obtainable from the PSA. This observation is applicable to all parts of a PSA, but has the most significant effect on the treatment of dependencies.

(4) Inadequate treatment of physical interaction dependencies.

These dependencies are partially covered by conventional analyses (e.g., component cooling fault trees) and also are reflected by failure rates. However, special treatment of dynamic effects (pipe whips, jets, secondary missiles) is seldom found in PSAs, which can lead to serious underestimation of accident sequence frequencies.

(5) Treatment of human interaction dependencies. See comments under points (3) and (9) in paragraph A.6.

(6) Modelling of common cause failures (CCFs).

There is a wide range of different approaches from non-consideration to relatively detailed treatment. While extensive procedures have been developed for modelling CCFs, they are regrettably seldom used consistently and comprehensively. Identified problems include use of generic data without proper specialization; use of very low CCF contributions with no or invalid supporting arguments; and insufficient analysis coverage with respect to component groups susceptible to CCFs.

A.6. TREATMENT OF HUMAN INTERACTIONS

(1) Categorization of human interactions.

Most PSAs differentiate clearly between pre-initiator errors and post-initiator errors, and also specify the subcategories involved (errors causing initiating events, reconfiguration errors after test or maintenance and miscalibration; errors of omission, commission and recovery). Lack of such a corresponding classification is a serious drawback and makes it difficult to assess completeness of a PSA.

(2) Representation of errors causing initiating events.

These errors are implicitly incorporated in the initiating event frequencies. Current PSAs do not employ any systematic methods for identifying, modelling, and quantifying these types of human interaction. This lack of methods might limit the ability to achieve the overall long term objectives of the PSA.

(3) Representation of reconfiguration errors and miscalibration.

These errors, found to be significant in some past PSAs, have sometimes been excluded; alternatively, the dependencies involved have been neglected or treated in an excessively optimistic way.

(4) Treatment of error of diagnosis.

Lack of clear distinction between errors during diagnosis and errors during carrying out of specific tasks after a correct diagnosis has been observed.

(5) Treatment of errors of commission.

Most PSAs neglect these contributions. However, examples have been found of incorporating such errors on the component level, which might lead to excessive conservatism. As a minimum, incorporating errors of commission on the system level has been recommended as a part of sensitivity studies.

(6) Inadequate background information.

Frequently little or no information on the actions required, the time windows, and the location of the action in available in the PSAs.

(7) Treatment of recoveries.

There are examples of either lack of recovery analyses or of excessively optimistic treatments. PSA results should be presented separately with and without recovery.

(8) Use of extremely low human error probabilities.

Probabilities lower than 10^{-4} per demand can seldom be supported.

(9) Treatment of human interaction dependencies.

This part is seldom subject to plant specific analysis which should be performed at least for dominant contributors.

A.7. ACCIDENT SEQUENCE QUANTIFICATION

(1) Integration of logic models.

In some cases, the approaches used are limited in their completeness and thoroughness. Thus, it is not explicitly shown how the support systems are integrated with the front line systems in the event trees to produce the final accident sequence minimal cut sets. Furthermore, shortcuts are taken in combining system success states and system failure states, and in eliminating minimal cut set inconsistencies. Sequence probabilities should be determined without mutually exclusive contributions arising from neglecting success branches within a sequence.

(2) Screening process to reduce the number of sequences selected for complete analysis.

The selection criteria based on qualitative reasoning may be arbitrary. The process should be validated to assure that important sequences are not lost.

(3) Quantification of component unavailabilities, and test and maintenance contributions.

The mission times should be clearly identified, which is critical for assuring that the quantifications are consistent with the definitions of system failure. Correct formulas should be used to quantify unavailabilities of standby components for monitored, testable, and non-repairable cases. Maintenance and test duration contributions should be accounted for comprehensively, reflecting plant specific conditions.

(4) Validity of unavailability estimators.

Simple (first moment) estimators seldom provide sufficient accuracy. For the global unavailability, estimation of higher order terms should be accounted for, especially in cases with high failure probabilities and the involvement of the same contributors in different cut sets.

(5) Importance, sensitivity, and uncertainty evaluations.

These evaluations are not always represented comprehensively in current PSAs, which should not be the case. Risk achievement worths (RAWs) and risk reduction worths (RRWs) should be calculated for each contribution, and sensitivity quantifications should be carried out for contributions with large RAWs and RRWs. Many PSAs lack extensive sensitivity analyses to provide perspective on the uncertainties involved and to indicate relative importance of issues. Also formal propagations of parametric uncertainties should be included at a later stage of a PSA, although these are relatively less important than sensitivity studies.

A.8. DOCUMENTATION AND RESULT PRESENTATION

(1) Structure of documentation.

In some cases, the documentation provided is not organized properly with a clear separation between a summary report, main report, and appendices providing the necessary background.

Improvements of traceability are generally desirable, which can be achieved by providing road maps and cross-references.

(2) Completeness of documentation.

Frequently the limitations and assumptions associated with each analysis are not accounted for. Such information is critical for review, for future use, and for extending a PSA.

(3) Result presentation.

This is one of most apparent weaknesses in current PSAs. The results should be organized to show the dominant sequences, event class (e.g. human errors, component, system) importance with respect to core damage frequency, and support system contributions. Different contributors should be prioritized with regard to their contributions or sensitivities. Graphs or bar charts should be used more extensively to show the insights and findings.

A.9. QUALITY ASSURANCE

(1) Analysis procedures.

Procedures for different parts of the analysis presently constitute a standard part of any PSA. They are usually well written, clear, and complete. Identified problems are to a higher extend associated with the failure to follow the developed procedures rather than with the quality of these procedures. Deficiencies in documentation control also have been identified.

(2) Internal review.

Many PSA weaknesses could have been avoided by implementing an effective internal review process. In particular, PSAs carried out by several organizations, especially when they are geographically separated, can significantly benefit from a comprehensive internal review. The technical quality assurance should be assigned to a permanent team comprising the most experienced personnel involved in the project.

(3) Software quality assurance.

Software used in PSAs should be subject to QA procedures covering specification, design, and testing. This recommendation is not always followed.

REFERENCES

[1] BONACA, M.V. (Ed.), Living Probabilistic Safety Assessment for Nuclear Power Plant Management, A Report by a Group of Experts of the NEA Committee on the Safety of Nuclear Installations, Nuclear Energy Agency, Organisation for Economic Co-operation and Development, Paris (1992).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, Guidelines for the International Peer Review Service (IPERS) Programme, IAEA-TECDOC-543, Vienna (1990).

[3] HIRSCHBERG, S., "Experiences from International Peer Reviews of Probabilistic Safety Assessment", The Use of Probabilistic Safety Assessment for Operational Safety, PSA' 91, (Proc. Int. Symp. Vienna, 1991), IAEA, Vienna (1992).

[4] Probabilistic Safety Assessment (PSA) Requirements for Use in Safety Management, IAEA Techn. Committee Mtg Stockholm, 1991.

[5] 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).

[6] US NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide, A Guide to Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Final Report, Vol. 1: Chapters 1–8, Vol. 2: Chapters 9–13 and Appendices A–G, NUREG/CR-2300, USNRC, Washington, DC (1983).

[7] US NUCLEAR REGULATORY COMMISSION, Probabilistic Safety Analysis Procedures Guide, Vol. 1: Sections 1–7, Vol. 2: Sections 8–12, NUREG/GR-2815, USNRC, Washington, DC (1985).

[8] BUDNITZ, R.J., JOKSIMOVICH, V., Content of PRA Submittals for Future LWRs, NUREG/CR-4812, USNRC, Washington, DC (1987).

[9] VESELY, W.E., "Case studies of PSA applications: Overview of US and international PSA applications", ANL/IAEA Interregional Training Course on Operational Safety in Nuclear Power Plant Operation: Prevention and Management of Accidents, Argonne, 1991, Lecture 50.2.12, Argonne National Laboratory, IL (1991).

[10] KNOCHENHAUER, M., HIRSCHBERG, S., Probabilistically based decision support, Reliab. Eng. Syst. Saf. **36** (1992) 23–28.

[11] 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).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Case Study on the Use of PSA Methods: Backfitting Decisions, IAEA-TECDOC-591, IAEA, Vienna (1991).

[13] HIRSCHBERG, S., (Ed.), NKA-project "Risk Analysis" (RAS-470): Summary Report on Reference Study on Human Interactions, Final Report NKA RAS-470(89)17 (ABB Atom Report RPC 89–112) (1989).

[14] SAMANTA, P.K., WONG, S.M., HIGGINS, J., HABER, S., LUCKAS, W., A Risk Methodology to Evaluate Sensitivity of Plant Risk to Human Errors, IEEE Fourth Conference on Human Factors and Power Plants, Monterey, CA (1988).

[15] SAMANTA, P.K., WONG, S.M., CARBONARO, J.C., Evaluation of Risks Associated with AOT and STI Requirements of the ANO-1 Nuclear Power Plant, NUREG/CR-5200, US Nuclear Regulatory Commission, Washington, DC (1988).

[16] VESELY, W.E., DAVIS, T.C., SALTOS, N., Measures of the Risk Impact of Testing and Maintenance Activities, NUREG/CR-3541, US Nuclear Regulatory Commission, Washington, DC (1983).

[17] SAMANTA, P.K., VESELY, W.E., KIM, I.S., Study of Operational Risk-Based Configuration Control, NUREG/CR-5641, US Nuclear Regulatory Commission, Washington, DC (1991).

[18] HORNE, B.E., "The use of probabilistic safety analysis methods for planning the maintenance and testing unavailabilities of essential plant at Heysham 2 AGR power station",

Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, Vienna (1991) 165–175.

[19] KNOCHENHAUER, M., Plant Level Probabilistic Evaluation of Preventive Maintenance during Power Operation in Forsmark 2, NKA/RAS-450S(87)4 (ABB Atom Report RPC 87-61) (1987).

[20] LAAKSO, K., KNOCHENHAURER, M., MANKAMO, T., PÖRN, K., Optimization of Technical Specifications by Use of Probabilistic Methods, A Nordic Perspective, Final Report of the NKA Project RAS-450, Nordic Liaison Committee for Atomic Energy (1990).

[21] SAMANTA, P.K., VESELY, W.E., Risk Impact and Effects of Maintenance Scheduling (in preparation).

[22] LOFGREN, E., et al., A Process for Risk-Focused Maintenance, NUREG/CR-5695, US Nuclear Regulatory Commission, Washington, DC (1991).

[23] Risk-based Optimization of Maintenance at NPPs, Report of an IAEA Consultants Mtg Vienna, 1991.

[24] ENGQVIST, A., MANKAMO, T., "Test scheme rearrangement for diesel generators at Forsmark 1/2", PSA' 89 (Proc. Int. Top. Mtg on Probability, Reliability and Safety Assessment, Pittsburgh, PA, 1989), American Nuclear Society, La Grange Park, IL (1989).

[25] SAMANTA, P.K., GINZBURG, T., VESELY, W.E., Consideration of Test Strategy in Defining Surveillance Test Intervals, Technical Report A-3859, Brookhaven National Laboratory, Upton, NY (1989).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants, IAEA-TECDOC-729, Vienna (1993).

[27] TAYLOR, J.T., et al., Development and Use of Risk-Based Inspection Guides, NUREG/CR-5371, US Nuclear Regulatory Commission, Washington, DC (1989).

[28] GORE, B.F., VO, T.V., HARIS, M.S., PRA Application Program for Inspection at Oconee Unit 3, NUREG/CR-5006, US Nuclear Regulatory Commission, Washington, DC (1987).

[29] US NUCLEAR REGULATORY COMMISSION, Risk-Based Inspection — Development of Guidelines, NUREG/GR-0005, USNRC, Washington, DC (1992).

[30] VESELY, W.E., Evaluation of Allowed Outage Times (AOTs) from a Risk and Reliability Standpoint, NUREG/CR-5425, US Nuclear Regulatory Commission, Washington, DC (1989).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, Vienna (1990).

[32] WAGNER, D.P., VESELY, W.E., MINTON, L.A., Risk-Based Evaluation of Technical Specifications, EPRI-NP-4317, Electric Power Research Institute, Palo Alto, CA (1987).

[33] SAMANTA, P.K. et al., Risk Methodology Guide for AOT and STI Modifications, BNL Technical Report A-3230-12-02-86, Brookhaven National Laboratory, Upton, NY (1986).

[34] MANKAMO, T., KIM, I.S., SAMANTA, P.K., Risk-Based Improvement of Technical Specification Action Statements Requiring Shutdown: Pilot Application to the RHR/SSW Systems of a BWR, BNL Draft Report, Brookhaven National Laboratory, Upton, NY (1992).

[35] GALLUP, D.R., WHITEHEAD, D.W., VANNONI, M.G., A Method for Using PRA to Establish Quality Assurance Program Applicability, NUREG/CR-4678, US Nuclear Regulatory Commission, Washington, DC (1986).

[36] SPECTER, H., Risk-Based Regulation, Draft Report for Comment, New York Power Authority, December 1991.

[37] MINARICK, J.W., The US NRC accident sequence precursor program: Present methods and findings, Reliab. Eng. Syst. Saf. **27** (1990) 23–51.

[38] HOERTNER, H., KAFKA, P., REICHART, G., The German precursor study — methodology and insights, Reliab. Eng. Syst. Saf. **27** (1990) 53–76.

[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Plant Specific PSA to Evaluate Incidents at Nuclear Power Plants, IAEA-TECDOC-611, Vienna (1991).

[40] JOHANSON, G., ERHARSSON, U.-K., HOLMBERG, J., LAAKSO, K., NIEMELÄ, I., SANDSTEDT, J., "Synopsis report: Use of living PSA for operational safety evaluation and

management. Part I of NKS/SIK-1 Project Reporting", Probabilistic Safety Assessment (PSA) Requirements for Use in Safety Management, IAEA Techn. Committee Mtg Stockholm, 1991.

[41] VESELY, W.E., et al., Evaluation of Core Melt Frequency Effects due to Component Ageing and Maintenance, NUREG/CR-5510, US Nuclear Regulatory Commission, Washington, DC (1990).

[42] INTERNATIONAL ATOMIC ENERGY AGENCY, The Use of Probabilistic Safety Assessment in the Relicensing of Nuclear Power Plants for Extended Lifetimes, IAEA-TECDOC-547, Vienna (1990).

CONTRIBUTORS TO DRAFTING AND REVIEW

Johanson, G. Swedish Nuclear Power Inspectorate, Sweden

Samanta, P.K. Department of Nuclear Energy, Risk and Reliability Analysis, Brookhaven National Laboratory, United States of America

Hirschberg, S. International Atomic Energy Agency

Technical Committee Meeting
Stockholm, Sweden, 16–20 September 1991

Consultants Meetings
Vienna, Austria, 2–6 December 1991, 9–13 March 1992

HOW TO ORDER IAEA PUBLICATIONS

☆ ☆ **In the United States of America and Canada**, the exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, is

UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

☆ ☆ **In the following countries** IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

ARGENTINA	Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires
AUSTRALIA	Hunter Publications, 58A Gipps Street, Collingwood, Victoria 3066
BELGIUM	Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels
CHILE	Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 95, Casilla 188-D, Santiago
CHINA	IAEA Publications in Chinese China Nuclear Energy Industry Corporation, Translation Section, P O Box 2103, Beijing IAEA Publications other than in Chinese China National Publications Import & Export Corporation, Deutsche Abteilung P O Box 88, Beijing
FRANCE	Office International de Documentation et Librairie, 48 rue Gay-Lussac, F-75240 Paris Cedex 05
GERMANY	UNO-Verlag, Vertriebs- und Verlags GmbH, Dag Hammarskjöld-Haus, Poppelsdorfer Allee 55 D-53115 Bonn
HUNGARY	Librotrade Ltd , Book Import P O Box 126, H-1656 Budapest
INDIA	Oxford Book and Stationery Co , Scindia House, New Delhi-110 001
ISRAEL	YOZMOT Literature Ltd , P O Box 56055, IL-61560 Tel Aviv
ITALY	Libreria Scientifica Dott Lucio di Biasio "AEIOU", Via Coronelli 6, I-20146 Milan
JAPAN	Maruzen Company, Ltd, P O Box 5050, 100-31 Tokyo International
NETHERLANDS	Martinus Nijhoff International, P O Box 269, NL-2501 AX The Hague Swets and Zeitlinger b v , P O Box 830, NL-2610 SZ Lisse
PAKISTAN	Mirza Book Agency, 65 Shahrah Quaid-e-Azam, P O Box 729, Lahore 3
POLAND	Ars Polona, Foreign Trade Enterprise, Krakowskie Przedmiescie 7, PL-00-068 Warsaw
ROMANIA	Ilexim, P O Box 136-137, Bucharest
RUSSIAN FEDERATION	Mezhdunarodnaya Kniga, Sovinkniga-EA, Dimitrova 39, SU-113 095 Moscow
SLOVAK REPUBLIC	Alfa Publishers, Hurbanovo námestie 3, SQ-815 89 Bratislava
SOUTH AFRICA	Van Schaik Bookstore (Pty) Ltd, P O Box 724, Pretoria 0001
SPAIN	Díaz de Santos, Lagasca 95, E-28006 Madrid Díaz de Santos, Balmes 417, E-08022 Barcelona
SWEDEN	Fritzes Information Centre, S-106 47 Stockholm
UNITED KINGDOM	HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR
YUGOSLAVIA	Jugoslovenska Knjiga, Terazije 27, P O Box 36, YU-11001 Belgrade

☆ ☆ Orders (except for customers in Canada and the USA) and requests for information may also be addressed directly to:

Sales and Promotion Unit
International Atomic Energy Agency
Wagramerstrasse 5, P O Box 100, A-1400 Vienna, Austria