Safety Reports Series
No. 25

Review of Probabilistic Safety Assessments by Regulatory Bodies

Jointly sponsored by IAEA, OECD/NEA

International Atomic Energy Agency, Vienna, 2002

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www.iaea.org/ns/coordinet

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series,** the **INSAG Series, the TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

REVIEW OF PROBABILISTIC SAFETY ASSESSMENTS BY REGULATORY BODIES

SAFETY REPORTS SERIES No. 25

REVIEW OF PROBABILISTIC SAFETY ASSESSMENTS BY REGULATORY BODIES

JOINTLY SPONSORED BY
THE INTERNATIONAL ATOMIC ENERGY AGENCY
AND THE
OECD NUCLEAR ENERGY AGENCY

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2002

IAEA Library Cataloguing in Publication Data

Review of probabilistic safety assessments by regulatory bodies / jointly sponsored by the International Atomic Energy Agency and the OECD Nuclear Energy Agency. — Vienna : International Atomic Energy Agency, 2002.

p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 25)

STI/PUB/1139

ISBN 92–0–117502–7

Includes bibliographical references.

1. Nuclear power plants—Risk assessment. 2. Reliability (Engineering) 3. Nuclear power plants—Safety measures. I. International Atomic Energy Agency. II. OECD Nuclear Energy Agency. III. Series.

IAEAL 02–00301

Printed by the IAEA in Austria
November 2002
STI/PUB/1139

FOREWORD

Probabilistic safety assessment (PSA) is increasingly being used as part of the decision making process to assess the level of safety of nuclear power plants. The methodologies in use are maturing and the insights gained from PSAs are being used together with those from deterministic analysis.

Many regulatory bodies consider that PSA is sufficiently well developed for results to be used centrally in the regulatory decision making process — referred to as *risk informed regulation*.

For these applications to be successful, it will be necessary for regulatory bodies to have a high degree of confidence in PSA. However, at the IAEA Technical Committee Meeting on the Use of PSA in the Regulatory Process in 1994 and at the OECD Nuclear Energy Agency Committee for Nuclear Regulatory Activities (CNRA) 'Special Issues' meeting in 1997 on Review Procedures and Criteria for Different Regulatory Applications of PSA, it was recognized that there was no formal guidance on regulatory review for PSAs. The senior regulators noted that there was a need to produce international guidance for reviewing PSAs to establish an agreed basis for assessing whether important technological and methodological issues in PSAs are treated adequately and to verify that conclusions reached are appropriate.

In 1997 the IAEA and OECD Nuclear Energy Agency agreed to produce in co-operation a guidance document on the regulatory review of PSAs. This led to the publication of IAEA-TECDOCs 1135 and 1229 on the Regulatory Review of Level 1 PSA and the Regulatory Review of Level 2 PSA. The present Safety Report is based on the information provided in these two TECDOCs. The scope of the work has been extended to cover PSA for low power and shutdown conditions, and Level 3 PSA.

This publication is intended to provide guidance to regulatory bodies on how to review the PSA for a nuclear power plant, to gain confidence that it has been carried out to an acceptable standard so that it can be used as the basis for taking risk informed decisions within a regulatory decision making process. The report gives guidance on how to set about reviewing a PSA and on the technical issues that need to be addressed.

The IAEA acknowledges the work performed by all the participating experts and wishes to thank them for their valuable contribution to the preparation of this report. The IAEA officer responsible for this publication was V. Ranguelova of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

An appendix, when included, is considered to form an integral part of the report and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

A probabilistic safety assessment (PSA) of a nuclear power plant provides a comprehensive, structured approach to identifying failure scenarios and deriving numerical estimates of the risks to workers and members of the public. PSAs are normally performed at three levels as follows:

(a) *Level 1 PSA*, which identifies the sequences of events that can lead to core damage, estimates core damage frequency and provides insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage.
(b) *Level 2 PSA*, which identifies the ways in which radioactive releases from plants can occur and estimates their magnitudes and frequencies. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures such as reactor containment.
(c) *Level 3 PSA*, which estimates public health and other societal risks such as contamination of land or food.

PSA provides a systematic approach to determining whether safety systems are adequate, the plant design balanced, the defence in depth requirement been realized and the risk as low as reasonably achievable. These are characteristics of the probabilistic approach which distinguish it from the deterministic approach.

Over 200 PSAs have been conducted around the world. All of them have been done to Level 1 to provide an estimate of the core damage frequency for initiating events occurring during full power operation. Many of them also estimate the contribution to the risk which would arise during low power and shutdown conditions.

In some cases, the analysis has been extended to consider how the sequences would progress after core damage has occurred. This is often termed a Level 1+ (Level 1 plus) PSA, although the exact meaning of this varies from country to country. However, the emerging standard in the past few years is for Level 2 PSAs to be carried out. A review of the state of the art carried out by the OECD Committee on the Safety of Nuclear Installations (CSNI) in 1997 [1] provided details of 19 such analyses that have been carried out for PWRs and 8 for BWRs. To date, relatively few Level 3 PSAs have been carried out.

These PSAs have been conceived for a wide variety of reasons, which include the following:

(a) To provide insights from risk analyses to supplement those obtained from deterministic safety assessments,
(b) To identify weaknesses in the design and operation of plants,
(c) To estimate the risk from plants for comparison with the risk criteria,
(d) To provide an input into plant specific applications such as the optimization of technical specifications and into operational uses such as maintenance planning,
(e) To address the phenomena that would occur during core damage and provide insights into how a plant would behave during a severe accident,
(f) To identify weaknesses in the level of protection provided for severe accidents,
(g) To identify additional safety systems and accident management measures that would provide further protection against severe accidents,
(h) To provide an input into emergency preparedness.

The scopes of the PSAs that have been carried out also vary. They have all addressed initiating events occurring at full power and, in some cases, been extended to address low power and shutdown states. In addition, they have all addressed internal events and, in some cases, been extended to address internal hazards such as fires and flooding, and external hazards such as earthquakes and aircraft impacts.

PSA is increasingly being used as part of the decision making process to assess the level of safety of nuclear power plants. The methodologies have matured over the past decade or so and, while they are continuing to develop, PSA is now seen as a very useful and often essential tool to support the deterministic analyses which have traditionally been carried out. The insights gained from PSA are being considered along with those from deterministic analysis to make decisions about the safety of plants. Additionally, many regulatory bodies consider that PSA (especially Level 1 PSA) is sufficiently well developed that it can be used centrally in the regulatory decision making process — referred to as *risk informed regulation*. For these applications to be successful, it will be necessary for the regulatory body (and the utility) to have a high degree of confidence in the PSA.

The use of PSA in the regulatory process was the subject of several IAEA consultant and technical committee meetings and two OECD Nuclear Energy Agency (NEA) Committee for Nuclear Regulatory Activities (CNRA) 'Special Issues' meetings [1, 2]. At these meetings, the senior regulators agreed that the use of PSA as a tool in the regulatory decision making process is increasing and it is now becoming acceptable to use PSA as a complement to the deterministic approaches to address plant safety concerns.

Although the current trend is for regulatory bodies to move towards a more risk informed approach to their activities, it was found that there is a considerable variation in the way they carry out their assessments of PSAs. While many countries have already drawn up, or are planning to draw up, guidance for reviewing PSAs, it

is often not a formalized or standard type of practice. Some international guidance is available but this is applicable only for specific purposes: for example, the international guidelines [3] produced by the IAEA as the basis for the service it provides to its Member States in the peer review of PSAs. However, no general guidance is available for the review of PSAs.

The senior regulators concluded that there is a need to produce some international guidance for reviewing PSAs. The main objective of this guidance would be to establish an agreed basis for assessing whether important technological and methodological issues in PSAs are treated adequately and to verify that the conclusions reached are appropriate.

This co-operative effort led to the publication by the IAEA of TECDOCs 1135 [4] and 1229 [5] on the Regulatory Review of Probabilistic Safety Assessment (PSA) Levels 1 and 2, respectively. The present document is based on this work and has extended the scope to include Level 3 PSA and initiating events occurring during low power and shutdown modes.

1.2. OBJECTIVE

This report provides guidance to assist regulatory bodies in carrying out reviews of the PSAs produced by utilities. In following this guidance, it is important that the regulatory body is able to satisfy itself that the PSA has been carried out to an acceptable standard and that it can be used for its intended applications. The review process becomes an important phase in determining the acceptability of the PSA since this provides a degree of assurance of the PSA's scope, validity and limitations, as well as a better understanding of plants themselves. This report is also intended to assist technical experts managing or performing PSA reviews. A particular aim is to promote a standardized framework, terminology and form of documentation for the results of PSA reviews.

The information presented in this report supports IAEA Safety Guide No. GS-G-1.2 [6]. Recommendations on the scope and methods to be used by the utility in the preparation of a PSA study is provided in IAEA Safety Guide No. NS-G-1.2 [7]. Information on these Safety Guides and other IAEA safety standards for nuclear power plants can be found on the following Internet site: http://www.iaea.org/ns/coordinet.

1.3. SCOPE

The scope of this report covers the review of Level 1, 2 and 3 PSAs for event sequences occurring in all modes of plant operation (including full power, low power

and shutdown). Where the scope of the analysis is narrower than this, a subset of the guidance can be identified and used.

Information is provided on carrying out the review of a PSA throughout the PSA production process, i.e. from the initial decision to carry out the PSA through to the completion of the study and the production of the final PSA report. However, the same procedure can be applied to a completed PSA or to one already in progress.

As a result of the performance of a PSA, changes to the design or operation of the plant are often identified that would increase the level of safety. This might include the addition of further safety systems or accident management measures. In reaching decisions on which improvements will actually be made, the insights gained from the PSA are combined with those gained from a deterministic analysis and with other factors (such as the cost and the remaining lifetime of the plant). The review of this decision making process is not within the scope of this publication.

1.4. STRUCTURE

Section 2 gives guidance on how regulatory bodies should carry out reviews of PSAs. It addresses issues such as when a review is carried out, the extent of the review, the review of the aims and objectives of the PSA, the review/audit of the utility's PSA production process and the documentation of the findings of the review.

Section 3 gives guidance on the technical issues that need to be addressed in carrying out reviews of Level 1 PSAs for initiating events occurring during full power operation. This addresses:

- Identification and grouping of initiating events;
- Accident sequence analysis;
- Systems analysis;
- Analysis of dependent failures;
- Analysis of passive systems, components and structures;
- Human reliability assessment;
- Data required for a PSA;
- Analysis of computer based systems;
- Analysis of internal and external hazards;
- Quantification of accident sequences;
- Sensitivity analysis, uncertainty analysis and importance analysis;
- Interpretation of the results of a PSA;
- Audit of the PSA quality assurance (QA).

Section 4 extends this to cover Level 1 PSAs for initiating events occurring during low power and shutdown conditions. In particular, this covers:

- Plant operating states (POSs);
- Identification and grouping of initiating events;
- Accident sequence analysis;
- Systems analysis;
- Analysis of dependent failures;
- Human reliability assessment (HRA);
- Data required for a shutdown PSA (SPSA);
- Analysis of internal and external hazards;
- Quantification of accident sequences;
- Sensitivity analysis, uncertainty analysis and importance analysis;
- Interpretation of the results of an SPSA.

Section 5 gives guidance on the technical issues that need to be addressed in carrying out reviews of Level 2 PSAs. This addresses:

- Familiarization with plant data and systems;
- The interface between Level 1 and Level 2 PSAs;
- Accident progression modelling;
- Containment performance analysis;
- Probabilistic modelling framework;
- Quantification of the containment event tree analysis;
- Characterization of the radiological source terms;
- Results of Level 2 PSAs;
- Audits of Level 2 PSA QAs.

Section 6 gives guidance on the technical issues that need to be addressed in carrying out reviews of Level 3 PSAs. This addresses:

- The aims of Level 3 PSAs;
- Source term characterization and grouping;
- The choice of a consequence analysis code;
- Data requirements for the consequence analysis;
- Atmospheric dispersion modelling;
- Identification and modelling of emergency planning and countermeasures;
- Quantification and use of the results of Level 3 PSAs.

A list of references, which provide more detailed guidance on many of the PSA issues, is provided at the end of this report. The abbreviations used and the names of contributors to drafting and review are also given at the end.

In preparing this Safety Report, it has been recognized that there are differences in the terminologies used in different countries and, whilst every attempt has been made to use consistent terminology throughout, it is important that readers take these differences into account in applying the guidance given.

In this report, the term PSA is used throughout. This is taken to be the same as probabilistic risk analysis/assessment (PRA) and the two are considered to be interchangeable. In addition, it is recognized that there are differences in the way that the industry is organized and that terms such as 'utility', 'plant operator' and 'licensee' may mean different things in different countries. In producing this report for regulatory guidance, these terms are considered to be interchangeable, with 'utility' being used throughout. In addition, there are differences in who actually carries out PSAs. In this report, the view is taken that PSAs are carried out by the 'utilities', since it is their responsibility, although they are often carried out by the plant designers or sometimes by consultants.

2. THE REVIEW PROCESS

2.1. INTRODUCTION

This section gives guidance on the way a regulatory body needs to set about reviewing a PSA for a nuclear power plant to gain confidence that it has been carried out to an acceptable standard.

In providing this information, it is recognized that the approach to the regulation of nuclear power plants in general and to the regulatory review of PSAs in particular may be different in different countries. In addition, the approach may also be different depending on the purpose of the review; for example, a review that is carried out on the PSA for a new reactor design may be different from that for an existing reactor carried out as part of a periodic safety review.

Guidance is given on:

- The approach to the review;
- The aims, objectives and scope of PSAs;
- The methods and assumptions used in PSAs;
- Auditing the utility's PSA production process.

2.2. APPROACH TO REVIEWS

2.2.1. Timing of reviews

Reviews carried out by regulatory bodies can be on-line or off-line, depending on the time when the review is carried out. An *on-line review* is one which is carried out immediately after the PSA team has finished one particular task. The advantage of this approach is that many of the findings of the review can be incorporated into the PSA, which will significantly reduce the amount of reworking needed. The disadvantage is that the review may have been based on reports that are changed significantly as the analysis proceeds and may need to be reviewed again. An *off-line review* is when the review is started after the PSA team has presented the final report to the regulatory body. The advantage of this approach is that the PSA documents are reviewed only once (if no major reworking is required). The disadvantage is that the review may find significant problems that could have been identified and corrected more easily at an early stage of the analysis.

It is considered that the most efficient approach is for the regulatory body to carry out an on-line review of a PSA whenever possible so that specific tasks are reviewed as they are completed rather than waiting for the whole of the analysis to be completed. This allows the regulatory body to determine whether the analysis is being carried out in an acceptable way and, if not, ensure that any deficiencies are rectified at an early stage. This will also usually result in an earlier date for regulatory acceptance of the PSA. However, it is recognized that there are situations where an off-line review may be chosen for particular reasons.

Having agreed on the timing of the review, it is advisable that a schedule of work be drawn up with the utility's PSA team that fits the needs of both organizations, ensures that the review process is conducted efficiently and that minimizes any delays in completing the PSA or the review. This schedule has to allow for sufficient time and effort to be given to the review of the results of the PSA, including taking an overall view on their correctness and credibility. Since this important step comes near the end of the review process, it is liable to be done without unnecessary delays, owing to the effort already allocated to the review, but it is an essential step in confirming that the aims and objectives of the PSA have been met, and in providing the level of confidence that the regulatory body is seeking.

The detailed review of the PSA would normally start with a Level 1 analysis then proceed to a Level 2 analysis and finally to a Level 3 analysis. This is important to ensure that deficiencies in the preceding parts of the analysis are identified and hence are not taken forward so that they lead to incorrect conclusions.

2.2.2. Extent of reviews

The extent of a review to be carried out by a regulatory body needs to be decided at the start of the review process. This can range from an extensive review to a much more limited review, depending on national practices and other factors.

In an *extensive review*, the PSA would be reviewed in considerable detail to ensure that the models and data used are good representations of the actual design and operation of the plant. This approach has significant advantages in terms of learning, building confidence in the PSA and reducing the effort required for reviewing PSA applications. It has the disadvantage that the cost to the regulatory body will be high. This approach may not be feasible if the number of different plant designs to be reviewed is high or the PSA resources available to the regulatory body are limited.

In a *limited review*, the aim would be to ensure that all aspects of the event sequences leading to core damage, a large (early) release or particular off-site consequences are modelled adequately and the data used to determine the frequencies of the event sequences are representative of the plant. In doing this, the review would focus on those aspects of the PSA which have the highest impact on the results. The advantage of this approach is that it is less intensive in resources for the regulatory body, the disadvantage that it leads to less being learnt and lower levels of confidence in the results. It also increases the effort required for reviewing later applications. Limited reviews use a combination of an overall review with spot checks using a detailed review as defined below. One example of this approach is that adopted by the International Peer Review Service (IPERS) of the IAEA — see Ref. [3], which needs to be of limited scope due to time constraints.

In a limited review there is a possibility that some significant aspect may be missed by the reviewers if it has not been addressed in the PSA, and so it is important for the reviewers to pay attention to the question of completeness in their high level review. This is particularly the case in an on-line review, where the numerical results are not available in the early stages and the reviewers have to rely on their judgement and knowledge of other PSAs to choose the aspects of highest impact.

It is recognized that practices will be different in different countries. However, it is advisable that the extent of the review be comprehensive enough to provide the regulatory body with the level of confidence it is seeking. In particular, it will need to provide confidence that the analysis is consistent with the current state of the art. This is particularly important in PSA areas which are still developing. This includes areas such as Level 2 PSA, human reliability analysis and the PSA for low power and shutdown conditions.

The reviewers should consider whether the scope of the PSA is adequate from the point of view of addressing an adequate range of internal and external initiating events, and operating modes of the plant.

The reviewers also need to focus on those issues which are important in determining the risk from the plant and any areas of the PSA which are found to be relatively weak. Even in the case of an extensive review, it is not necessary to independently verify every detail.

Although the extent of the review will depend on national practices and other factors, it will need to be sufficient to provide the regulatory body with the level of

confidence it is seeking. The factors which influence the scope of the review include the level of risk from the plant, the experience with that reactor system and whether it is intended to use the PSA as a basis for risk informed decision making.

The review to be carried out may take into consideration whether an independent peer review of the PSA funded by the utility has been carried out. If this is the case, the regulatory body may decide to reduce the extent of the review they would carry out, to avoid duplication. However, for many regulatory bodies, the review of the PSA is an excellent source of additional knowledge about the plant design, operation, and safety strengths and weaknesses that, in itself, may justify an extensive review in any case. An extensive review would probably be required if the regulatory body intended to use the PSA as a basis for risk informed regulation.

It is considered to be good practice whenever possible for an extensive review be carried out in the following cases:

(a) Where the level of risk from a plant is relatively high,
(b) For the first PSA from a utility,
(c) For the PSA for a new reactor system,
(d) For PSAs where the design and/or the operational practices are significantly different from previous experience.

2.2.3. Documentation required for reviews

The documentation required for a review comprises the documentation which describes the design and operation of the nuclear power plant and the documentation of the PSA itself. This information is vitally important since it is normally submitted formally by the utility to the regulatory body and is the basis for the regulatory review and any uses made of the PSA.

The starting point for the production and review of a PSA is a clear definition of the design of the plant and of how it will be operated. This will normally be the design as of an agreed date for a plant during the design stage or the actual design and operation for an existing plant, again as of a specified date. A PSA for an existing plant is often part of a more general review of its safety, leading to a programme of modifications to the plant. The PSA may then relate to the state of the plant after the modifications have been completed. In such cases, it is advisable that a PSA be performed for both the states, i.e. before and after the changes, so that the reduction in risk can be evaluated. It is essential for sufficient information to be provided to allow the reviewers to become familiar with the design and operation of the plant. This would include systems descriptions, operating procedures, test and maintenance procedures, accident management procedures, etc. This is usually combined with plant visits as required.

Sufficient documentation needs to be provided/made available to the reviewers to characterize the PSA. This needs to include the PSA methods and data and all supporting analysis such as the transient analysis to support the safety system success criteria. It is important that sufficient detail is provided to allow the analysis to be traced (or repeated, if necessary).

The regulatory body should agree with the utility on the format and content of the documentation before the start of the PSA. This will ensure that the QA, peer review and regulatory review processes can be carried out much more efficiently. Extensive documentation of the PSA is even more important when it will be updated regularly/maintained as a living PSA or will be used for a number of applications.

The first task of the review team is to check that the PSA documentation submitted generally corresponds to that described above. If this is not the case, the reviewers have to indicate to the utility what additional documentation is required at an early stage in the review process so that it can be supplied in a timely manner.

This would include checks to ensure that:

(a) The information on the design and operation of the plant has been clearly documented.
(b) The methodologies used for performing the different PSA tasks have been clearly documented and would allow the analysis to be repeated without additional information from the PSA team.
(c) The supporting analyses (including, e.g., thermohydraulic analyses for justifying system success criteria) are either included in the PSA documentation or are available for consultation by the reviewers.
(d) All tables, figures and appendices have been provided.
(e) There are adequate references to supporting literature.
(f) All the information provided is consistent with the PSA 'freeze' date.

In addition, for Level 2 and 3 PSAs, the reviewers need to check that the preceding parts of the analysis have been documented fully. In particular, the documentation should describe how the information in the Level 1 PSA which is necessary to evaluate the containment performance and the transport of radionuclides has been transferred to the Level 2 PSA and how the information in the Level 2 PSA which relates to off-site consequences has been transferred to the Level 3 PSA. The reviewers need to confirm that the utility has documented the PSA in a manner that helps in understanding and reviewing it.

It is considered good practice that the reviewers obtain and use the electronic version of the PSA model rather than rely on paper copies of the event/fault tree analysis. This allows the reviewers:

(1) To search for specific information in the model,

(2) To perform spot checks on the model and its quantification,
(3) To carry out an analysis to identify the areas of the PSA on which the review needs to focus,
(4) To carry out their own sensitivity studies to determine how changes in assumptions can affect the results of the PSA,
(5) To use the PSA as a basis for risk informed regulation.

However, it is recognized that this may not be possible for some regulatory bodies.

2.2.4. Setting up the review team

The size of the review team has to be sufficient to carry out a review of the extent intended by the regulatory body, as discussed above.

It is important that the review team be experienced in the techniques necessary for carrying out state of the art PSAs. The range of expertise needs to be sufficient to address all the issues which are likely to arise during the review of the PSA. This could involve the use of external consultants to support the work carried out by the regulatory body. Where necessary, additional training may be required and provided.

The range of expertise of the reviewers should be sufficient to address all the issues that are likely to arise during the review and those involved would typically include the following:

(a) *Systems analysts* who are familiar with the design of reactor safety systems (Level 1 PSAs), containment systems (Level 1 and Level 2 PSAs) and the interface between Level 1 and Level 2 PSAs.
(b) *Staff with an operating background* who are familiar with the emergency operating procedures (EOPs) (Level 1 PSA), the accident management measures for severe accidents (Level 2 PSA) and the off-site emergency arrangements (Level 3 PSA).
(c) *Experts in the severe accident phenomena* that could occur during and following core melt. These include the physical and chemical processes that govern accident progression and determine the loads on the containment, and the way that radioactive material is transported from the molten fuel to the environment. Expertise is also required in the computer codes which are used to model severe accidents.
(d) *Structural specialists* to address the performance of the containment following the loadings imposed by a severe accident and the failure modes that could occur.
(e) *PSA specialists* to address the modelling and quantification of the analysis and the associated uncertainties.

It is good practice that the review team includes experts with experience of deterministic analysis. This offers the advantage of aiding the regulatory body in understanding the PSA, increases PSA credibility and helps in the review of applications combining deterministic and probabilistic analyses.

Establishing good interfaces between the review team and the PSA team will allow free exchange of documentation and open discussions. However, in setting up and carrying out the review, care has to be taken to ensure that the independence of the regulatory body is not compromised.

After the review has been completed, it is advisable that the regulatory body retain a sufficient level of expertise to be able to review any of the uses being made of the PSA.

2.2.5. Agreement on methods

2.2.5.1. Level 1 PSA for full power

The methods that are available for performing the Level 1 PSA are discussed in detail in Section 3. This part of the analysis can be carried out using large event trees, large fault trees or a combination of event trees and fault trees and, although all three approaches are currently in use, the norm is to use a combination of event trees and fault trees. In addition, there are, for example, a number of possible approaches to modelling common cause failures and carrying out the HRA included in the PSA.

2.2.5.2. Level 1 PSA for low power and shutdown conditions

The methods that are available for performing level 2 PSAs are discussed in detail in Section 4. The first step in the analysis is to define the POSs that could occur during low power and shutdown conditions, which is generally a major task due to the great variety of conditions that could arise. Otherwise, the methodology generally follows that for a full power PSA. However, particular attention needs to be paid to some parts of the analysis, for example, the HRA where the timescales for operator actions are generally longer than those for the same initiating event occurring at full power.

2.2.5.3. Level 2 PSA

The methods that are available for performing Level 2 PSAs are discussed in detail in Section 5. The usual way to model the progression of a severe accident in a Level 2 PSA is to use some form of event tree analysis — referred to as containment event trees (CETs) or accident progression event trees (APETs). These vary significantly in terms of the number of nodes included in the model. These typically range

from small event trees that have branch points representing different time regimes and some intermediate events to complicated event trees that represent a large number of different time regimes, all major phenomena, system events and operator actions. Experience in carrying out Level 2 PSAs shows that both these approaches can be used to model accident progressions adequately.

The reviewers need to check that, in principle, the set of nodes chosen for the analysis is sufficient to model all the significant phenomena that could occur during a severe accident and to provide the insights required by the aims and objectives that have been agreed for the analysis.

Where several methodologies are available to perform any portion of an analysis, it is important that the regulatory body clearly point out to the PSA team which of these methodologies it would consider to be unacceptable. This will avoid resources being used for carrying out work that would later be considered inadequate.

2.2.5.4. Level 3 PSA

The methods that are available for performing Level 2 PSAs are discussed in detail in Section 6. The basis of Level 3 PSA is to determine the off-site consequences following a release of radioactivity. There are a number of computer codes that can do this.

2.2.6. Identification of/focus on important issues

The work of the reviewers needs to focus on the areas which have the most significant impact on the results of the PSA. This would include the PSA topics addressed in Section 3 and, for example, the initiating events and system/component failures which have the highest risk significance.

The reviewers need to identify the issues which have the highest risk significance. This may be done by using the importance functions, sensitivity studies, which address the assumptions made and the data used in the analysis, and uncertainty analysis. However, in doing this, the reviewers should recognize that the importance, sensitivity and uncertainty analyses are dependent on the quality of the PSA being reviewed and they cannot be considered as correct until the end of the review.

A preliminary review may be carried out to identify the risk significant areas which will need to be addressed in the more detailed review. This would usually generate a list of questions which can be addressed to the PSA team to initiate the more detailed review.

2.2.7. Comparison with other PSAs

It is often useful to carry out a comparison of the methods used in a PSA with those used in other PSAs for similar plants. It is the practice in many countries to use a previous, state of the art, PSA as a reference for carrying out/reviewing a new PSA.

In addition, it is often useful to compare the results of the PSA and the insights obtained from it with those from the PSAs of similar plants. However, if there are differences in design between the plants compared, neither the similarity nor the lack of similarity of the results is a clear indication of the correctness or incorrectness of the PSA, but such a comparison can stimulate the thinking about areas to be reviewed in more detail.

2.2.8. Reworking of an analysis by a regulatory body

The reviewers have to consider whether there is a need to carry out any independent calculations or to rework particular parts of the PSA to aid in the understanding of the PSA and of its sensitivities and uncertainties.

The practice varies between regulatory bodies in different countries from virtually no reworking of the analysis to carrying out whole PSAs themselves, either in-house or with the use of consultants. Where consultants are employed, it is important that they work in close consultation with regulators. Where some of the computer codes or particular techniques used in the PSA are unfamiliar to the reviewers, the reworking of parts of the analysis, for example the evaluation of a fault tree or an accident sequence using different codes or techniques, needs to be considered to give the reviewers confidence that the mechanics of the PSA have been correctly handled.

However, owing to the complexity of the PSA, this is not advisable unless the regulatory body (or its consultants) has a sufficient level of expertise and resources.

2.2.9. Documentation of the review findings

The findings of the review need to be documented in a PSA review report. The format, content and structure of this report will depend on the national practices and on the scope of the review. Generally, the contents of the report have to include the following items.

The report should contain background information including a brief description of the plant, the organizations involved in the PSA, the purpose/objectives/scope of the PSA and general information on the review process carried out. Where these topics have been discussed and agreed with the utility, this information could be summarized and the available documents referenced or attached as appendices.

It is important that the report also contains the conclusions of the review, which would address the accurate implementation of the methodologies chosen for each of

the PSA tasks, major concerns expressed by the reviewers, the responses provided and final resolutions achieved. Summary information on what was checked in detail also needs to be provided. This would include all lists of issues (questions, answers and resolutions) used in the review process and would highlight any issues still open.

The report should give the final conclusions reached on the adequacy of the PSA including the PSA, uncertainty and sensitivity study results. Problem areas need to be identified and explained.

The report may contain recommendations for further PSA work to improve its scope/methodology/quality, changes to be made in the way the PSA is applied, or changes to be made to the design or operation of the plant. It may also include recommendations regarding the revision of the PSA in order to keep it up to date and to ensure that it continues to meet the requirements originally agreed for the PSA.

It is good practice to attach to the report a list of the participants in the review team indicating the main responsibilities for each review area.

If an on-line review has been carried out, the reviewers will need to complete the review in a short time after the presentation of the PSA report. If the review process is off-line, this requirement would also apply in principle although it is recognized that the timescale will be much longer.

It is necessary to maintain control of all the documents and workbooks used in the review of the PSA. This needs to be done in accordance with the QA requirements.

2.2.10. Interactions with the utility

It is important that the reviewers agree with the utility on how to conduct the interactions between themselves and other parties such as designers and consultants during the process of reviewing the PSA. The optimization of this process deserves careful consideration, since it may have a significant impact on the time and effort required for the review. It involves a balance between free interaction, which can be productive and efficient, and the degree of formality appropriate to a regulatory process, with legal sanctions in the background. The reviewers, with their regulatory role in mind, need to avoid too close a relationship with the utility personnel, which might be perceived as compromising their independence, while endeavouring to maintain a friendly and professional relationship, in which there is a reasonably free flow of views and information. The utility personnel and designers will know about other options in the design, or in the PSA techniques, which they have considered and rejected. Information on these can be very helpful to the reviewers in reaching a view on the options chosen, but this is not normally part of the PSA documentation and the utility may be under no obligation to reveal it. It may, however, be possible to discuss such matters informally if a good relationship between reviewers and utility has been established. As a general rule, the reviewers also need to avoid

proposing specific means of resolving their concerns: that is a task of the utility and is part of the process whereby the utility is committed to the safety case for its plant. In some cases, however, the resolution may be implicit in the expression of the concern.

A good practice is to document the concerns expressed by the review team, the responses provided by the PSA team and the final resolution achieved. An example of this process is included in the IPERS procedures guide of the IAEA [3]. The time spent on such documentation will be reduced if it is agreed that informal contacts between the reviewers and the PSA team are used for the clarification of points in the PSA reports and for the resolution of minor issues. Any issues of sufficient substance to be mentioned in the review report need to be formally confirmed in writing.

The aim of all parties is a final PSA report for which the utility is content to take full responsibility and which the regulatory body and its reviewers find acceptable, and it is expected that some iterations will be needed to achieve this. Some of the review comments may require parts of the PSA to be reworked using different assumptions or methods, while others may only require the PSA documentation to be changed to provide clarification and further explanation and justification. Where a part of the PSA has been re-evaluated, the reviewers need to ensure that all the significant impacts of the change are reflected throughout the PSA and its documentation, so that consistency is retained throughout, even if this means repeating, for example, the whole of the numerical evaluation and the review of the dominant components and sequences. It is also necessary to ensure that all the points that required clarification, including those dealt with informally, have been satisfactorily incorporated into the final PSA report; it needs to be borne in mind that this report, or its future updates, will be used to support decision making in years to come when the authors are no longer available to explain it.

At the end of their review, it is good practice for the reviewers to communicate their consolidated findings to the utility's PSA team, although they may have passed them on during the course of the review. This would normally be done by sending a copy of the review report. Only the findings of the reviewers, extracted from the report, may be sent if there are special reasons for not sending the whole report, but this is to be regarded as exceptional. The main purpose is to allow the utility to point out any factual errors, although the utility would no doubt take the opportunity to raise objections to anything in the report which it regards as unreasonable or unfair.

The whole process of performing a PSA, its internal reviews, its independent verification and its regulatory review, will usually lead to a programme of work for improving the plant to remove any weaknesses uncovered by the PSA, where this is reasonably practicable. While members of the PSA review team may well be involved in the assessment and monitoring of such a programme of work, they need to be

careful to distinguish their role in these activities from that as PSA reviewers. It is the responsibility of the utility to formulate the programme of plant changes, to obtain regulatory approval and to implement the programme, ensuring that the changes have no negative impacts on the deterministic safety analysis. It is also necessary for the utility to evaluate the effects of the plant changes on the PSA, and to produce an updated PSA at an appropriate time, such as when the programme has been completed. The regulatory body then needs to review the utility's safety assessments of the changes, which will include reviewing the PSA aspects, and monitor their implementation.

The regulatory body usually encourages the utility to use the PSA as widely as possible during the operation of the plant, to maintain a PSA team which is capable of doing this and to keep the PSA up to date.

2.2.11. Research

Reviewers need to be aware of the extensive body of research which has been carried out in recent years that has provided a better understanding of the various phenomena that would occur during a severe accident. This has yielded experimental data and permitted computer code simulations of severe accident sequences and radiological releases and transportation.

In the course of the regulatory review, the reviewers may identify areas which they see as promising candidates for research to develop the state of the art in PSA further by, for example, reducing uncertainties, increasing confidence or being less conservative. This would include research to support the development of PSAs in general (e.g. to improve the modelling capabilities of the PSA) and research to investigate the issues which arise out of the review of a particular PSA (e.g. to provide better information on particular event sequences, which allows some of the conservatism to be removed from the PSA). For Level 2 PSA, this would include research to provide a better understanding of the development of severe accidents, increase confidence in the analyses and reduce uncertainties. The reviewers usually draw any such research topics to the attention of the regulatory body and/or the body which is best placed to take the work forward.

In some countries, there is a joint programme of research agreed between the regulatory body and the utility which aims to identify technical areas that may be controversial and fund research or pilot activities aimed at developing the criteria or methods to be used.

2.3. REVIEW OF THE AIMS, OBJECTIVES AND SCOPE OF PSAs

The starting point for the review process is ideally when a decision to perform a PSA is taken. The decision may be taken by the regulatory body, in terms of a

requirement or recommendation, it may be taken voluntarily by the utility or it may arise in some other way, for example, as a result of a government inquiry. However it arises if a PSA is going to be presented to the regulatory body for review, it is advisable that before the PSA is started both parties agree on aspects of the PSA such as its aims, objectives and scope.

2.3.1. Development of regulatory principles for the review of PSAs

It is advisable for the regulatory body to set the standards which will be used to assess the acceptability of a PSA and to make these clear to the utility.

It is considered very important that, before the start of a PSA, both the regulatory body and the utility are aware of the technical standards required for the PSA. Normally this will be done by reference to available national or international guidance. The IAEA has already issued Safety Practices covering the performance of Level 1, Level 2 and Level 3 PSAs [8–10] and documents covering specific aspects of PSA including the treatment of external events [11], seismic events [12], common cause failure analysis [13], definition of initiating events [14, 15] and HRA [16].

2.3.2. Aims and objectives of PSAs

The regulatory body may find it useful to formulate what it considers are the aims and objectives of a PSA. These criteria need to be compared with what the utility has proposed and an agreement reached. As a minimum, the PSA has to be adequate to allow plant weaknesses to be identified and decisions made on how to improve the level of safety of the plant.

Where risk targets or criteria have been specified (whether formal or informal) the PSA will need to address them adequately. Risk targets are typically set in terms of the core damage frequency which will require a Level 1 PSA, large (early) release frequency which will require a Level 2 PSA or societal risk criteria which will require a Level 3 PSA.

It is important to understand what the risk targets are since, as pointed out in Ref. [5], "the review of a Level 2 PSA that is intended only to show that a nuclear power plant fulfils quantitative safety goals will be different than the review of a Level 2 PSA in which the objective is to produce information about the relative importance of systems and phenomena for accident management decisions or other purposes".

In this Safety Report, it is assumed that the aim is to produce a state of the art Level 1 PSA which is extended into a Level 2 PSA and then into a Level 3 PSA.

2.3.3. Scope and applications of PSAs

The regulatory body and the utility need to agree on the scope and uses of a PSA and to ensure that these are sufficient to meet the overall aims and objectives of the analysis.

It is good practice for the regulatory body to specify the scope of the PSA that it would expect the utility to carry out. This can then be compared with what the utility has proposed and an agreement reached. If the scope of the PSA falls short of what would be expected, this needs to be brought to the attention of the utility so that the scope of the analysis can be changed at an early stage.

The specification for the scope of the PSA usually includes:

(a) The range of internal and external initiating events to be covered by the analysis (internal initiators such as transients and loss of coolant accidents (LOCAs), internal hazards such as fires and flooding, and external hazards such as earthquakes and aircraft crashes);
(b) The modes of operation of the plant to be covered by the analysis (full power operation, low power operation and shutdown states);
(c) The scope of the human reliability analysis, for example, whether modelling of cognitive errors is required;
(d) Whether post-trip repair and return to service of failed systems/components is to be taken into account;
(e) Whether recovery actions and accident management measures (to prevent core damage) are to be taken into account for accident situations beyond the design basis;
(f) Whether operation of the plant outside its operating rules or technical specifications is to be taken into account, so that initiating events occurring in these forbidden states are included;
(g) The range of sensitivity studies that need to be carried out (data and modelling assumptions);
(h) Whether an uncertainty analysis is required;
(i) Whether Level 1, 2 and 3 PSAs are required;
(j) The main results of the PSA that are to be presented.

It is accepted that, for example, sabotage, terrorist attack and war are excluded from the scope of a PSA. Although some attempts have been made to model such threats, there are no established methods of doing so.

Agreement on the scope of the PSA is important since different end uses place different emphases on the various parts of the analysis. For example, an analysis that is intended to consider hydrogen control or the ability of the containment to withstand the loadings that would arise during a severe accident might not need to include the transport of radioactive material within the containment.

The scope of a Level 2 PSA could range from a full scope analysis, which is part of a fully integrated Level 3 PSA, to a limited analysis. The latter could include an analysis of the performance of the containment in severe accident situations but one that does not go on to determine the frequency and magnitude of the source terms that would arise from containment failure.

The best option is where the Level 2 PSA is part of a fully integrated PSA since the requirements for the Level 2 PSA will be recognized in carrying out the Level 1 PSA so that all plant related features that are important for the severe accident modelling will be fed into the Level 1 analysis. If this is not the case, the reviewers will need to pay special attention to the grouping/regrouping of the core melt sequences into plant damage states to ensure that the containment systems have been addressed correctly.

In the agreement on the scope of the Level 2 PSA consideration also needs to be given to the following:

(1) The basic approach to the modelling of the progression of severe accidents (e.g. using small or large event trees),
(2) How accident management measures and recovery actions are to be taken into account in the PSA,
(3) The range of sensitivity studies that need to be carried out (data and modelling assumptions),
(4) How the uncertainties in the severe accident modelling will be addressed and whether a full uncertainty analysis is required,
(5) Whether the analysis is to be extended to a Level 3 PSA.

It is necessary for the reviewers to check that the PSA being produced meets the agreed scope so that the analysis being carried out will be adequate to meet the aims and objectives agreed for the PSA. At this stage, the review would consider the scope of the analysis. A detailed review of the technical issues is given in Section 3. If the scope of the PSA falls short of what has been agreed, this should be brought to the attention of the utility so that the scope of the analysis can be changed at an early stage.

2.3.4. Applications of PSAs

A PSA has many potential applications beyond satisfying the immediate objectives of identifying design weaknesses and considering risk targets/criteria, referred to in the preceding section. The regulatory body may propose the set of applications which the PSA is to be used for, and reach an agreement on this topic with the utility. Many of the potential applications can be achieved using a basic PSA, as covered in this book, but others, particularly operational uses such as maintenance planning, require the special characteristics of a living PSA [17], such as explicit modelling of

each train and separate initiating events for each loop. The range of PSA applications could include, for example:

- Optimizing the technical specifications,
- Identifying accident management measures,
- Determining the change to the risk from the effects of ageing,
- Controlling equipment outages for maintenance,
- Supporting plant modifications,
- Evaluating operational events from a risk based perspective,
- Introducing graded QA.

It is advisable that the regulatory body and the utility agree on the intended (and potential future) uses of the Level 2 PSA and confirm that the proposed scope of the analysis is consistent with these uses. Again, if the intended uses do not meet the expectations of the regulatory body, this needs to be brought to the attention of the utility at an early stage so that additional uses can be considered.

Some typical uses of Level 2 PSAs (taken from Ref. [9]) are as follows:

(a) To gain qualitative insights into the progression of severe accidents and containment performance;
(b) To identify plant specific vulnerabilities of the containment to severe accidents;
(c) To provide a basis for the resolution of specific regulatory concerns;
(d) To provide a basis for the demonstration of conformance with quantitative safety criteria;
(e) To identify major containment failure modes and to estimate the corresponding releases of radionuclides;
(f) To provide a basis for the evaluation of off-site emergency planning strategies;
(g) To evaluate the impacts of various uncertainties, including assumptions relating to phenomena, systems and modelling;
(h) To provide a basis for the development of plant specific accident management strategies;
(i) To provide a basis for plant specific backfit analysis and evaluation of risk reduction options;
(j) To provide a basis for the prioritization of research activities for minimization of risk significant uncertainties;
(k) To provide a basis for a Level 3 PSA consistent with the PSA objectives.

In addition, the regulatory body should consider what role the Level 2 PSA will play in the decision making process. If it is intended to use the insights gained from the Level 2 PSA as part of a risk informed approach, this needs to be taken into account in reaching the agreement about the uses of the PSA.

The applications intended for the PSA will often determine the scope of the PSA itself — whether a Level 1, 2 or 3 PSA is required, the range of initiating events and of modes of operation included, and the level of detail in the component modelling. The reviewers need to check that the scope is adequate for the intended applications. Approximations and simplifications which are acceptable for a basic PSA can lead to significant errors in some of the applications, particularly those which might cover a range of equipment configurations. It is necessary to check that this is not likely to cause problems.

2.3.5. Sensitivity studies and uncertainty analysis

The reviewers need to verify that studies have been carried out to determine the extent to which the results of the analysis are sensitive to:

- Assumptions made in various parts of the analysis;
- Analytical models selected (or the parameters that influence them) for severe accident phenomena;
- Data used in quantitative analysis.

In particular, the reviewers need to check to ensure that the scope and level of detail of such studies are consistent with the objectives of the PSA. For example, for a Level 2 PSA, a structured sensitivity study addressing major assumptions, modelling parameters and data may be sufficient if the major aim of the study is to gain qualitative insights on plant response to severe accident conditions. A rigorous propagation of uncertainties may be necessary for studies in which the quantitative results are important, for example, studies performed to demonstrate that quantitative safety objectives are met.

In all cases, the reviewers need to check that the sensitivity/uncertainty analyses address the topics in which there is significant uncertainty and those that are dominant contributors to severe accident progression.

2.4. REVIEW OF METHODS AND ASSUMPTIONS

2.4.1. State of the art

The reviewers usually determine the standard of the PSA that the regulatory body would expect the utility to carry out. This would be expected to be a state of the art analysis which conforms with the best modern practices in PSA using methods that have been proven to bring about reasonable improvements over previously existing methods.

It is recognized that PSA methods are evolving. However, it is important that both the regulatory body and the utility determine what the state of the art is in PSA and this needs to be agreed between both parties. A review of the state of the art was carried out by CSNI. This is presented in Ref. [18] for Level 1 PSA.

2.4.2. Level of detail

The reviewers need to determine whether the level of detail of the PSA is sufficient to include all significant interdependences. These can arise due to support systems such as electric power systems and cooling water systems, which all need to be modelled explicitly in the analysis.

The reviewers need to determine whether the level of detail of the PSA is sufficient for the intended applications. For example, if the PSA is to be used to control equipment outages during maintenance, the PSA is expected not to have any asymmetries (e.g. the model incorporates initiating events in each of the loops of the plant rather than lumping them together as a representative initiating event in one of the loops) and to model basic events which represent the individual components which might be removed from service during maintenance. If such applications are not definitely planned but are a possibility for the future, the PSA needs to be structured so that it can be readily adapted to their inclusion.

It is recognized that the level of detail of the systems analysis has a significant influence on the cost of the PSA as well as on the credibility of the results. Significant dependences may be missed if the level of detail is not enough to uncover them. It is good practice to reach a level that provides assurance that all significant dependences are included in the model.

For example, plant specific calculations of severe accident behaviour are essential to an analysis performed for the purposes of measuring reductions in risk associated with proposed accident management measures; extensive use of 'reference plant' results is inappropriate for such an application.

Interdependences can arise in a number of ways, including:

(a) *Support system*s such as electric power systems and cooling water systems. Although they will have been included in the Level 1 PSA/plant damage states, their status is important in determining how the accident sequences progress after core melt has occurred.
(b) *Phenomena which are addressed in different time frames* in the model of how the accident progresses. For example, the likelihood of a hydrogen burn occurring in one time frame will depend on the safety systems that have operated and whether a burn has occurred in an earlier time frame.
(c) *Human actions* which have been addressed in one time frame and may arise again in a later time frame.

The reviewers need to determine the level of detail that the regulatory body would expect to see in the PSA and confirm with the utility that this is what is intended before the PSA is started.

2.4.3. Methods of analysis

The reviewers need to determine whether the methods used for the analysis are adequate to meet the aims and objectives of the PSA. More detailed guidance is given in the later sections of this report on the various aspects of PSA.

The reviewers will ideally identify the state of the art methods and tools for each task, and then make a comparison with the ones used in the PSA. At this stage, the reviewers do not need to check that the methods and tools have been correctly applied. Whenever a method or tool different from the state of the art is identified, this matter is to be raised immediately with the utility as a significant area of concern.

Where screening methods have been used in the analysis or cut-offs applied to the event sequences/cut sets, the reviewers need to check that this does not lead to significant underestimation of the risk or to invalidation of the PSA for one of its uses.

For a Level 2 PSA, this would include:

- The codes used to model the progression of the severe accident,
- The framework (usually an event tree analysis) for the modelling of severe accident sequences,
- The probabilistic quantification of the event sequences.

The reviewers need to identify what methods and tools are used (or proposed for use) for each of the PSA tasks, ensure that the ones to be used are consistent with the state of the art and check that these methods and tools have been correctly applied.

2.4.4. Sources of data

Data are required in the PSA for initiating event frequencies, component failure probabilities, component unavailability during periods of test or maintenance, common cause failure probabilities and human error probabilities.

The reviewers need to confirm that all the sources of data have been identified and are relevant. The aim is to ensure that plant specific data are used whenever possible. Where this is not possible, use of data from the operation of the same type of reactor system or of generic data is acceptable. Where no relevant operating data are available and judgement has been used to assign the initiating fault frequency, the basis for this judgement is to be stated and shown to be valid, as far as possible.

It is necessary for the reviewers to determine whether the data used in the PSA are acceptable. The preference is for best estimate data which are appropriate for the

purposes of the PSA and cover all the causes of failure which could occur, with the uncertainties identified.

For Level 2 PSA, the accident progression analysis is usually carried out in an event tree framework referred to as CETs or APETs. These event trees delineate the various ways in which an accident sequence can proceed after the onset of core damage.

Quantification of the event trees is accomplished by assigning conditional probabilities to each of the branches that emerge from event nodes in the trees.

Although the conditional probabilities for some of these branches can be quantified through the use of statistical data, for example, those involving containment system operation or operator actions, many branches represent alternative outcomes of events that are governed by severe accident phenomena about which there is a significant degree of uncertainty. This uncertainty means that the physically correct outcome of an event is not known. Conditional probabilities are associated with such events to weight the outcomes according to the strength of the evidence suggesting one outcome versus another. These conditional probabilities are usually generated through a more or less formal expert judgement process.

The reviewers need to be satisfied that the framework for making these expert judgements is sound and is applied consistently throughout the analysis, and that the technical information used to make such judgements is stated and shown to be valid, as far as possible. They need to take account of plant specific accident progression analysis that has been carried out, adaptation of analysis for similar plants and applicable research data.

2.4.5. Use of best estimate methods, assumptions and data

The reviewers need to check that best estimate methods, assumptions and data have been used in the PSA wherever possible. This is a particular requirement for Level 2 PSA where conservative assumptions will lead to a model of the accident sequence progression which is not realistic, and hence may provide limited or misleading insights into where the weaknesses might be in the design and operation of the plant and which accident management measures would be useful in reducing the risk.

However, it is recognized that best estimates are generally more difficult and time consuming to derive and lead to a PSA of greater complexity than a conservative approach. Also, many analysts contributing to the PSA will tend to err on the conservative side as a matter of prudence, this being a principle of design basis analysis. Thus any PSA will be expected to contain many aspects which are conservative to a greater or lesser degree. If the only objective of the PSA is to show that the core damage frequency is less than a specified criterion, conservatism would be acceptable. For nearly all other objectives, however, substantial use of the conservative approach

will distort the estimates of the relative contributions to risk from, for example, components, systems and events, and thus frustrate the objective.

With the aim of best estimates throughout the PSA, it is important to check that the conservatism present is not so great that it leads to an unacceptable bias and distortion in the results of the PSA. This will largely be a matter of judgement on the part the reviewers. It is usually straightforward to obtain best estimates of all the numerical data used in the PSA.

Where an uncertainty analysis is not part of the PSA, i.e. where the PSA is based on point values alone, all the values and assumptions input need to represent best estimates of the mean values and not, for example, of the median values, which can be very non-conservative with respect to the mean. Where an uncertainty analysis is performed, the values characterizing the input distributions, for example median values and percentiles, should be best estimates of those values.

There are several areas of a PSA, for example, human reliability analysis, external events and common cause failures, where performing a detailed best estimate analysis of each case could be impossibly time consuming. The technique of screening is then used to select the dominant cases for detailed analysis, leaving the remainder with their conservative screening values in place. This deliberate introduction of conservatism into the PSA may be regarded as acceptable provided that the reviewers can be satisfied that the degree of conservatism is not so great as to throw serious doubt on the results. The importance factors calculated in the PSA can be helpful in reaching a view on this. In cases of doubt, the conservative screening values can be replaced in the PSA by best estimate values, even though these may have to be assigned by judgement rather than by further analysis.

The reviewers should note that the effect of including conservatism in the Level 2 PSA may be significantly different from that in the Level 1 PSA. In the Level 1 PSA, the use of conservative safety systems success criteria, initiating event frequencies or component failure data would lead to an overestimate of the core damage frequency. However, in the Level 2 PSA, a conservative assumption in the modelling of one of the phenomena, which would occur during the severe accident, may not be conservative with respect to other phenomena.

Hence, it is important that the reviewers should check that any conservatism included in the analysis would not lead to an unacceptable bias and distortion in the results of the PSA. This will be largely a matter of judgement on the part of the reviewers.

Where an uncertainty analysis is performed, the values characterizing the input distributions always need to be realistically estimated.

2.4.6. Validation and verification of computer codes

The computer codes used in the PSA need to be validated and verified. In this context, *validation* is defined as demonstrating theoretically that the calculational

methods used in the computer code are fit for their purpose and *verification* is defined as ensuring that the controlling physical and mathematical equations have been correctly translated into computer code.

The computer codes required for a Level 2 PSA include the codes which model the severe accident phenomenology, including the codes which model individual phenomena as well as the integrated codes and the probabilistic codes for quantifying the event trees used to model the development of a severe accident — see Section 4.

The reviewers need to check that the analysts have used the codes within their limits of applicability. In addition, they need to confirm that the predictions of the codes are consistent with the analyses carried out for similar plants and experimental information. Where integrated codes are used, their predictions should be compared with those obtained using separate effects codes.

It is necessary for the reviewers to determine whether the codes which have been selected by the PSA team are fit for their purpose and whether the users of the codes are experienced in their use and fully understand their limitations. It is advisable that the regulatory body and the utility reach an agreement on the set of codes to be used.

2.5. REVIEW/AUDIT OF THE UTILITY'S PSA PRODUCTION PROCESS

2.5.1. Scope of the review/audit

In addition to carrying out a review of the technical issues involved in carrying out a PSA, the regulatory body may also carry out a review/audit of the utility's PSA production process and the procedures being used to give confidence that those parts of the PSA which have not been reviewed in detail have been performed satisfactorily. If any discrepancies are found, this does not automatically mean that the PSA is flawed, but the reviewers need to ask for an explanation and justification for what was actually done and investigate the affected aspects of the PSA in more detail.

The review/audit may verify that the procedures that will be used for each of the main PSA tasks, i.e. each of the topics addressed in the following sections, are adequate. It is usually the case that the utility will develop its own detailed procedures for each of the PSA tasks, or adopt existing procedures, since this will help to ensure uniformity in approach across the PSA production process.

The reviewers need to check that the utility has procedures in place for the production of the PSA which set out the basic principles and methodologies to be followed and that they are adequate to produce a state of the art PSA.

The reviewers need to check that the procedures are detailed enough to avoid misinterpretations by different members of the PSA team so that they will be applied in a uniform and appropriate way throughout the PSA production process and will avoid the performance of tasks in a way that would not be acceptable.

In some countries, the PSA procedures need to be approved by the reviewers, and this will give the utility confidence that they are working within an approach generally acceptable to the regulatory body. Alternatively, the procedures followed for an already approved PSA can be used.

In particular, regarding the users of the codes, the audit should confirm that:

(1) The users are experienced in the use of the codes and understand the code limitations.
(2) Adequate guidance and training has been provided in the use of the codes.
(3) The codes have been used to evaluate standard problems to gain experience.

2.5.2. Quality assurance

One of the reviewers' tasks is to determine whether the utility has suitable QA arrangements in place for the production of the PSA. Some guidance on QA procedures for a PSA is given in Refs [8, 19].

The QA arrangements should include an internal process for checking the PSA methods and results. In addition, it is good practice to have arrangements in place for an independent peer review of the PSA. The existence of such an independent peer review may allow for a reduction in the extent of the review carried out by the regulatory body.

2.5.3. Organization of the PSA production team

Regarding the PSA production team, the reviewers should determine whether:

(a) The utility has assembled a team with sufficient depth and breadth of experience to enable the efficient production of the PSA.
(b) The composition of the utility PSA team is in line with the PSA procedures established by the utility.
(c) The PSA team is under the direction of utility personnel.
(d) The PSA team includes representatives from the plant operating staff.
(e) Where external consultants are used, they are fully integrated into the PSA team.
(f) The utility personnel are fully aware of the PSA methods and techniques being used and of their strengths and limitations.
(g) Training is provided for the less experienced members of the PSA team.
(h) All the members of the PSA team work within the procedures provided and the QA arrangements.
(i) Arrangements are in place to check the PSA as it is being prepared and to carry out an independent peer review of the PSA.

2.5.4. Future updating/development of the PSA

The reviewers need to check that the PSA is being prepared and documented in a way that makes it easy to update and to extend its use to other applications. The PSA report needs to be a living document which is modified to incorporate any changes which result from the regulatory review, changes to the design or operation of the plant and changes in modelling assumptions or data.

The reviewers may consider it necessary to check that the utility has taken steps to maintain control of all the documents and workbooks used in the performance of the PSA, according to applicable QA requirements, to allow for any later audit or review by the regulatory body.

It is considered good practice for the utility to maintain at least an adequate number of PSA specialists on its staff to ensure the maintenance of the basic PSA capabilities acquired in the process of preparing the PSA. This group is a key element for potential applications of the PSA.

3. REVIEW OF LEVEL 1 PSAs FOR FULL POWER OPERATION

This section gives guidance on the technical issues that need to be addressed in carrying out a review of a Level 1 PSA for initiating events occurring at full power. This covers:

- Identification and grouping of initiating events;
- Accident sequence analysis;
- Systems analysis;
- Analysis of dependent failures;
- Analysis of passive systems, components and structures;
- Human reliability assessment;
- Data required for the PSA;
- Analysis of computer based systems;
- Analysis of internal and external hazards;
- Quantification of accident sequences;
- Sensitivity analysis, uncertainty analysis and importance analysis;
- Interpretation of the results of the PSA;
- Audit of the PSA QA.

Accident sequence and systems analyses are almost invariably performed using a combination of event trees and fault trees for their evaluation. These two types of

tree are logically equivalent and, in principle, any combination is acceptable, provided that it is adequately documented. The division of the analysis between event trees and fault trees is largely a matter of preference, convenience, the availability of suitable computer codes and how well the representation of the analysis is communicated to the reader. The most common approach is that of the small event tree/large fault tree, where support systems are modelled in the fault trees. A variant of this is to model the accident sequence using a functional fault tree in place of the small event tree. Another approach, which has been used in many PSAs, is that of the large event tree/small fault tree, where support systems are modelled in the event trees. The event tree diagrams can then quickly become very large indeed, calling for great concentration from the reader in following the sequences. A discussion of these matters is to be found in Ref. [8].

3.1. IDENTIFICATION AND GROUPING OF INITIATING EVENTS

3.1.1. Identification of initiating events

The starting point of the PSA is the identification of the set of initiating events which have the potential to lead to core damage if additional failures of the safety systems occur.

The reviewers should check that a systematic procedure has been used to identify the set of initiating events used in the PSA. A number of approaches are possible:

(a) Analytical methods such as hazards and operability studies (HAZOPs) or failure modes and effects analysis (FMEA),
(b) Deductive analyses such as master logic diagrams,
(c) Comparison with the lists of initiating events developed for the PSAs for similar plants and with existing guidelines,
(d) Initiating events identified from the analysis of operating experience of the plant under investigation and of similar plants.

Subject to the agreement on the scope of the PSA, the set of initiating events identified will include internal initiating events (such as LOCAs and transients), internal hazards (such as fire, explosion and flooding of internal origin) and external hazards (such as earthquakes, aircraft crashes and flooding of external origin). Loss of grid power (off-site AC power) always has to be included, conventionally classed as an internal event, and specified in terms of the duration of the loss.

The reviewers need to check that the set of initiating events identified is as complete as possible, within the scope decided for the PSA. It is recognized that it is not possible to demonstrate completeness. However, by using a combination of the

methods identified above, it is possible to gain confidence that the contribution to the risk from initiating events which have not been identified would be small. The reviewers are expected to see, as a minimum, the last two items (lists from previous PSAs/existing guidance and the results of operational experience) in the PSA, together with some analytical approach. The reviewers should pay particular attention to any design features which are novel or peculiar to the plant in question as potential sources of new initiating events.

Where FMEA has been used, this needs to have been carried out for all the operating front line, support and standby systems to identify possible initiating events (or consequential failures which could constitute initiating events) that could arise through failure to operate, partial failure to operate or inadvertent operation.

The set of initiating events identified should include partial failures of equipment since it is possible that they could make a significant contribution to the risk.

The set of initiating events should include events of very low frequency. For any events that are not considered in the PSA (e.g. rupture of the reactor pressure vessel), the reviewers need to check the criteria that were used to screen out these events. Where only a Level 1 PSA is carried out, screening criteria based on frequency considerations are acceptable. If the PSA is to be extended to Level 2 or Level 3, attention also needs to be paid to the potential radiological consequences; low frequency events with potentially serious consequences must not be screened out.

For twin or multiple unit sites, some safety systems may be shared or cross-tied. In this case, the reviewers need to check that those initiating events that can affect both units (e.g. loss of grid power and most external events) have been identified and that the PSA takes account of the shared systems which are required by both/all of the units (instead of being fully available for one unit). Missiles from a turbine disintegration could strike a vulnerable part of another unit, an event that needs to be identified, even though it may be screened out later after analysis. It is possible that interconnections between units could lead to an accident in one unit giving rise to an initiating event in another. This is unlikely to be the case in a well engineered plant, but the reviewers may consider it necessary to check this point.

It is necessary that the set of initiating events considered in the PSA be compared with that for similar plants to ensure that any other relevant initiating events have been included. Where differences are identified, additional initiating events may be defined or justification provided of why this is not appropriate.

It is good practice to check that a review of the operating experience of the nuclear power plant (if it is already operating) and of similar nuclear power plants has been carried out to ensure that any initiating events that have actually occurred are included in the set of initiating events addressed in the PSA.

3.1.2. Grouping of initiating events

In order to limit the number of event trees to be constructed in the accident sequence analysis (Section 3.2), some initiating events can be grouped together for further analysis in the same event tree.

The reviewers need to check that only initiating events resulting in similar accident progressions and with similar success criteria for the mitigating systems have been grouped together. The success criteria used for that specific group have to be the most stringent criteria of all the individual events within the group.

Where initiating events with slightly different accident progressions and/or success criteria for the mitigating systems have been grouped together, the reviewers should check that the corresponding event tree has been developed to envelope all potential sequences and consequences of these initiating events. However, where such initiating events have been grouped, the reviewers need to be satisfied that this does not introduce undue conservatism into the analysis.

The initiating events which cause a containment bypass (e.g. steam generator tube rupture) must not be grouped with other LOCAs where the containment would be effective.

3.1.3. Further guidance on initiating events

The categories of initiating events for a nuclear power plant typically include the following:

(a) Increase in reactor heat removal (e.g., opening of secondary relief valves or steam line breaks);
(b) Decrease in reactor heat removal (e.g., loss of main feed or feed line breaks);
(c) Decrease in reactor coolant system flow rate (e.g., reactor coolant pump trip, pump seizure or shaft break);
(d) Reactivity and power distribution anomalies (e.g., uncontrolled control rod withdrawal, control rod ejection or boron dilution);
(e) Increase in reactor coolant inventory (e.g., inadvertent operation of the emergency coolant injection system);
(f) Decrease in reactor coolant inventory (e.g., LOCAs due to primary relief valves opening or primary pipework leakages and including interfacing systems LOCAs).

The reviewers need to be satisfied that the lesser events within each of the categories are identified as well as the extreme ones, since these are often much more frequent and can make a greater contribution to the risk. In categories (a) and (b) above, for example, a turbine control malfunction or trip would be more frequent than a major steam or feed line break.

3.1.3.1. LOCAs

The list of initiating events usually includes all the different sizes and locations of breaks which can lead to a loss of primary coolant, and is based on the actual design and layout of the plant and includes failures of valves and, in particular, of relief valves.

The LOCAs identified are usually categorized and grouped according to the success criteria of the safety systems that must be operated to prevent or limit core damage.

For LOCAs in the reactor coolant system piping, the reviewers need to pay particular attention to the locations of the break, since this can influence the success criteria for the required safety systems.

LOCAs are usually divided into large, medium and small LOCAs, on the basis of the safety systems required. Depending on the plant design, a different set of equipment may be required to provide protection from very small LOCAs such as those involving reactor coolant pump seal failure.

The success criteria for the LOCA groups should be supported by analysis and take account of equipment failures that could occur as a consequence of the break or the harsh environment generated by the LOCA.

Interfacing system LOCAs and steam generator tube ruptures are usually grouped separately since the primary coolant leakage from the break bypasses the containment and hence is not available for re-circulation from the containment sump.

3.1.3.2. Transients

In identifying initiating events that lead to transients, the reviewers need to pay specific attention to the plant specific features. Typical examples of initiating events for PWRs, which depend on specific plant features, are as follows:

(1) Steam generator tube ruptures;
(2) Loss of secondary cooling through loss of feedwater or loss of condenser vacuum;
(3) Spurious operation of systems which are not present in other plants of the same type;
(4) Loss of the main heat sink (e.g., the cooling water intake may be susceptible to slow blockage, giving warning time, as well as to rapid blockage).

Breaks of secondary circuit piping, especially relevant for PWRs, including steam line breaks and feed line breaks, should be considered as special types of transients. Plant specific operating experience requires consideration to identify any plant specific transients which need to be considered in the PSA.

Loss of a support or supply system has to be given special attention, especially where the system also has safety functions after a reactor trip. These events often affect many systems and sometimes support and supply systems have not been engineered with the same safety emphasis as front line systems. Procedures and instrumentation to enable diagnosis of problems might be less comprehensive and complete. Typical examples of such initiators are:

- Loss of an AC or DC bus,
- Loss of instrument air,
- Loss of component cooling and service water,
- Loss of room cooling.

In the identification of events related to loss of support systems consideration needs to be given to not only support functions to mechanical components but also those to instrumentation and control (I&C) systems (solid state components), including the reactor protection system.

3.1.3.3. Loss of grid power/station blackout

Loss of grid/external AC power is an important initiating event and it is necessary for the reviewers to pay particular attention to this event when it is followed by loss of all on-site AC power in the event sequence, since PSA studies have shown that this situation (known as station blackout) has made a significant contribution to risk for a number of plants. The combined event (loss of all external and on-site AC power) is sometimes treated in PSA as an initiating event in itself. This is acceptable provided that it is quite clear from the documentation that the logic is correct in that there is no double counting (e.g., for the frequency of loss of grid power, the frequency of blackout has to be excluded) and no omission.

The duration of power loss (and more particularly of station blackout) can be critical to the development of accident sequences, since some plants may have weak defences against a prolonged blackout. The frequency of loss of grid power therefore needs to be specified as a (usually stepwise) function of the duration of the loss. The reviewers need to check that the derivation of this frequency/duration function is clearly documented and based on records of grid loss in the area, and that account is taken of any site specific factors such as redundancy of grid lines or susceptibility to storm damage.

Different durations of loss of grid power may be treated in the PSA as different initiating events (analogous to different LOCA sizes) or, alternatively, the restoration of AC power at different times may be treated as headings in the event tree. Both approaches are acceptable, but both warrant careful review.

Where station blackout is treated as an initiating event, the frequency of loss of grid power needs to be multiplied by the probability of failure of the on-site AC power system. The duration of the blackout is determined by the restoration of power from the grid or, if the repair of failed systems is within the scope of the PSA, by restoration of the on-site power. The latter will, strictly, be accounted for in a best estimate analysis, but may be disregarded if it can be seen that there is only a small probability of restoring the on-site system before the grid is restored. Whatever approach is taken to the modelling of station blackout, there need to be clear interfaces between the structure of the event trees and that of the database analyses. There also should be clear connections in the event trees between the duration of blackouts and the resulting effects such as pump seal failures.

3.2. EVENT SEQUENCE ANALYSIS

The next step in the analysis is to determine the response of the plant to each of the groups of initiating events identified above. The event sequences are identified that could occur leading either to a safe state, where the reactor is shut down and the residual heat is being removed, or to core damage.

This requires that the safety functions that need to be performed for each of the groups of initiating events are identified along with the *success criteria* for the safety systems in performing these safety functions.

The analysis then models the accident sequences which could occur following success or failure of the safety systems. This is usually done by *event tree analysis* where the event trees are drawn in two steps — functional event trees are developed at a safety function level for each of the initiating event groups and these are then developed into the detailed event trees which model the behaviour of the safety systems in performing the safety functions.

The event sequences which lead to core damage are then grouped into *plant damage states* (PDSs) which form the starting point for the level 2 PSA.

3.2.1. Success criteria

The reviewers should check that criteria have been developed for what constitutes core damage. This is often done by adopting indirect criteria where core damage is assumed to occur following prolonged exposure of the top of the core or overpressurization, situations which need to be differentiated for comprehensive analysis. Core exposure is an acceptable surrogate for core damage only if limited possibilities exist to mitigate core damage after core exposure starts. This is often assumed for light water reactors but is not necessarily applicable for all reactor types. If a significantly long time interval is required to cause core damage after exposure, then this needs to be taken into account in framing a realistic definition of core damage.

The safety functions required to prevent core damage need to be identified for each of the initiating event groups. The safety functions required would typically include detection of the initiating event, reactor shutdown, residual heat removal and containment protection, depending on the reactor type and the nature of the initiating event.

The safety systems available to perform each of these safety functions need to be identified. The success criterion for each system can then be determined as the minimum level of performance required from the system and is expressed, typically, in terms of the number of trains of a redundant system which are required to operate, or the number of relief valves which are required to open and close. These relate to the requirements derived from the transient analysis which are expressed in terms of performance criteria (flow, pressure, response time, etc.). The success criteria also specify the requirements for the support systems based on the success criteria for front line systems.

It is important to check the success criteria of the safety systems to determine whether they depend on the prior success or failure of other safety systems and ensure that this is taken into account in the definition of the success criteria. An example of this arises for a large LOCA in a PWR where the requirement for the low pressure injection system (LPIS) may be different depending on the number of accumulators which have injected water into the primary circuit.

The success criteria need to identify the operator actions required to bring the plant to a safe, stable shutdown state. Identification usually follows from the emergency procedures, which must be available at least in outline, or by use of an analysis technique such as event sequence diagrams. It is good practice for this to be done as a co-operative effort between systems analysts and human reliability analysts.

It is important that the success criteria specify the mission times for the safety systems based on the transient analysis carried out.

The safety systems that would fail as a result of the initiating event need to be identified and taken into account in defining the success criteria. Examples of this are where the initiating event involves the failure of a support system, for example the electric power and cooling water systems, or causes a harsh environment in an area where safety system equipment is located. In either case this can lead to failure of the required safety systems. Another example arises for a large or intermediate LOCA in a PWR where, if the break occurs in a cold leg, the flow would be lost from the trains of the ECCS connected to that leg and this needs to be recognized in defining the success criteria.

Wherever possible, realistic success criteria based on best estimate transient analysis need to be defined and used in the PSA. This is preferable to using the conservative success criteria which are used in deterministic design basis analysis. However, if conservative success criteria have been used in the PSA for some of the

systems in any accident sequence, this needs to be clearly indicated and justified. In addition, the results need to be reviewed carefully to ensure that such conservatism does not dominate the risk and hence obscure insights from the PSA. If plant specific accident and transient analyses have been performed as part of the PSA in order to determine safety systems success criteria, the reviewers need to check the quality of these analyses.

Regarding the computer codes used to define the success criteria, the reviewers need to check that:

(a) The calculation methods used are well qualified to model the transients and accidents being analysed and to obtain a best estimate prediction of the results.
(b) Both the computer codes and the code users have been subject to QA procedures. The analyses have been performed only by qualified code users. A record documenting the qualifications is available.
(c) The origin and the version of the computer codes used is clearly documented and must be referenced. Computer codes are verified and validated for the relevant area of their application. Verification, validation and benchmarking (if done) are well documented.
(d) All sources of primary plant data are clearly referenced. Best estimate input data and assumptions are used whenever possible. Derivation of the input data for computer codes from primary information is documented in such a way that it allows adequate control, review, checking and verification.
(e) For each case analysed, a sufficient description of input data, basic assumptions, safety system set points and capabilities is provided.
(f) All calculations are well documented and the analysis results which are to be used further on in the PSA study are well identified.

3.2.2. Event sequence analysis

The reviewers should check that the event tree analysis for each of the initiating event groups covers all the safety functions that need to be performed and the operation of the safety systems required as identified by the success criteria. The status of the front line safety systems (success/failure) usually forms the headings on the event tree, to which are added any operator actions, particularly recovery actions, which directly affect the course of an accident. Any other events with a direct and significant effect on the sequence may also be included as headings.

The event trees are usually organized in a way which reflects the dependences of an event heading on previous headings. Given this, there is still some flexibility in the ordering of the headings. Nonetheless, the most natural way is to order them chronologically, following the time sequence of the demands made on the systems or

the operators. This order may be modified to some extent so as to maximize the number of non-branching points and thus simplify the tree, keeping to the rule that an event must appear after all other events on which it is dependent. Any operator actions in the event tree need to appear in chronological order, since the probability of error will be conditioned by the whole sequence of events up to that point. It may be that events will occur in a somewhat different time order on different branches of the same tree. This does not matter as long as the dependences are correctly observed. If this cannot be done, an event can appear under two headings, with branching at the appropriate one.

Event tree analyses usually identify and model all the dependences that can occur due to equipment failures and operator errors. Dependences due to equipment failures can occur where the failure of a support system would lead to failures in two or more of the front line systems that are identified in the success criteria for an initiating event group. Another example is where the failure of the ECCS system in the injection mode would mean that it would not be able to operate in the recirculation mode. Dependences due to operator errors can occur where an operator action is required before a safety system is able to operate. For example, for accident sequences for a PWR in particular, the operator needs to carry out an intentional depressurization of the primary circuit by opening the power operated relief valves (PORVs) before water can be injected by the low pressure ECCS into the primary circuit. In addition, dependences can arise due to the operator making mistakes in carrying out the accident management procedures.

Event tree analyses cover all possible combinations of success or failure of the safety systems in responding to an initiating event and identify all the sequences leading either to a successful outcome, where a sufficient number of the safety systems have operated correctly, or to core damage.

If one event tree is used to model several initiating event groups, the reviewers should check that this event tree does indeed envelope all sequences which can evolve from the different initiating event groups and that this grouping does not introduce undue conservatism.

The PSA documentation should contain a detailed description of the event trees, the assumptions made, the conditions created by the initiating event and the safety system requirements for the different event tree branches. The event tree diagram itself provides no reasoning, only the results of reasoning, and hence cannot be understood completely without reference to an accompanying text. The reviewers need to pay attention to each of the nodes on the tree where the sequence does not branch, to ensure that the reason for this is clear and valid. The documentation should explain and justify the selection of headings in the event tree, particularly for a complex event (such as a recovery procedure) or where more than one event is included under one heading. If simplifications or assumptions are made in the event trees, their effects have to be clearly identified and justified.

Where operator actions are modelled in the event tree analysis, the reviewers need to make certain that the procedures for the initiating event have been produced (or will be produced for a plant being designed) and cover the event sequence being addressed. In addition, the timing of the required operator actions has to be determined on the basis of plant specific best estimate thermohydraulic analyses and this needs to be reflected in the event trees.

If expert judgement is used to estimate available time frames, the basis for the judgement needs to be checked. Personnel from the operating organization of the plant should take part in the estimation process.

After reviewing the event tree preparation process and documentation, the reviewers need to select one (or more) event trees and work through its preparation process in detail to assess the adequacy of the modelling, assumptions and simplifications. The focus should be on the initiating event groups that have been found to make important contributions to the core damage frequency in past PSAs for similar plants.

An example of a situation where a detailed review would be worthwhile is a reactor coolant pump (RCP) seal LOCA for a PWR. This can occur due to loss of cooling and water injection systems and has been shown to be an important contributor to the risk for some PWR plants.

Another example is that of sequences in which relief or safety valves on the primary or secondary circuit are actuated to open. The reviewers must check that failure to close of these components leading to an induced LOCA or secondary depressurization has been considered in the event tree or that a justification is provided for not doing so.

The reviewers should check that the personnel who prepared the event trees have communicated with the personnel who participated in the systems analyses, human reliability analyses and sequence quantifications in the development of the event trees.

If the different system success requirements in the event trees are modelled by means of 'house events' in the system fault trees (Section 3.3.1), the house event descriptions need to be reviewed and the interfaces with the respective event trees checked.

If support system states are identified in the event trees, the documentation of the system states and the interfaces with the fault trees have to be checked.

3.2.3. Plant damage states

The next stage of the analysis is to group the event sequences identified as leading to core damage into PDSs, which form the interface between the Level 1 PSA and the Level 2 PSA. To make this grouping, the core damage accident sequences need to be characterized according to the general physical plant state to which each accident sequence leads and to the possible availability of the safety systems which could prevent or mitigate a release.

It is necessary to check that the event sequences which lead to core damage have been clearly identified from the event tree analysis. For each sequence identified, there needs to be a clear explanation of why it leads to core damage.

The reviewers need to check that the definitions of the PDSs are sound in that they take account of the characteristics of each core damage sequence which could influence the containment response or the release of radioactivity to the environment. These would typically include the following:

(a) The type of initiating event that has occurred (intact primary circuit or LOCA).
(b) The safety systems failures (in the reactor protection system, residual heat removal system and ECCS) which have occurred leading to core damage. For example from a Level 1 PSA perspective, it might make no difference whether a low pressure ECCS 'fails' due to a fault in the system itself or the system is rendered non-functional due to high primary circuit pressure; however, there is a big difference between these two cases from a Level 2 perspective.
(c) The state of the primary circuit pressure (high or low) at the time of core damage.
(d) The time at which core damage occurs (early or late relative to the time of reactor scram).
(e) The integrity of the containment (intact, failed, isolation failure, bypassed due to a steam generator tube rupture (SGTR) or an interfacing systems LOCA).
(f) LOCA with or without pressure suppression (BWRs).
(g) The pool is subcooled or saturated when core damage occurs (BWRs).
(h) The availability of the containment protection systems (containment sprays, heat removal systems and hydrogen mixing/recombiners).
(i) The availability of AC/DC power and recovery times.
(j) The operator actions which have been attempted and failed.

This grouping of event sequences into PDSs is usually a co-operative effort between Level 1 and Level 2 PSA analysts. The systems availability aspect of the PDS definitions can be addressed in several ways. One is to include the availability of the containment systems as headings on the Level 1 event trees, so that their system fault trees can be linked in and dependences accounted for in the evaluation. Another way is to model the systems on the containment event trees, although care is then needed to ensure that correlations with the Level 1 sequences, such as dependence on common support systems, is maintained. Yet another way is to use a separate computer program which takes the sequence information from the Level 1 event trees, links in the fault trees for the containment systems and acts essentially as an extension to the Level 1 trees. Such a program can also be written to group the sequences according to all of the characteristics in the definitions of the PDSs, with input of the appropriate information on, for example, timing and pressure, giving the

frequency of each PDS as the output, ready for the Level 2 analysis. Where this approach is taken, the reviewers should check that the assumptions, simplifications and dependences have been clearly described.

The PSA analyst may select one particular event sequence to represent all the sequences leading to a PDS. This representative sequence needs to be chosen to present the most severe challenge to the containment, but the variation in severity within the PDS does not need to be so great that it introduces undue conservatism.

The reviewers should check that the way the PDSs have been defined is consistent with what has been done in previous PSAs for similar plants. Further guidance on PDSs is given in Ref. [9].

3.3. SYSTEMS ANALYSIS

The next step in the analysis is to model the systems failures which are identified in the event tree analysis. This is usually done by fault tree analysis where the top event of the fault tree is the system failure state(s) identified in the event tree analysis. The fault trees extend the analysis down to the level of individual basic events which typically include component failures, unavailability of components during periods of maintenance or test, common cause failures of redundant components and operator errors.

3.3.1. Fault tree analysis

The reviewers should check that fault trees have been developed for each of the safety system failure states identified in the event tree analysis. The failure criteria defining the top event of the fault tree for each system function are the inverse of the accident sequence success criteria. In some cases, more than one model may be needed for the same system to address the success criteria defined for different initiating event groups or in different branches of the event tree, depending upon the sequence of events prior to the demand for the system. Alternatively, one fault tree may be used incorporating house events to switch in the appropriate success criteria. Fault trees that have house events warrant careful examination. It is useful to include the list of all house events, adding the description of how they are to be used. The PSA documentation needs to describe the dependence of system success criteria on the initiating event group and the prior failures in the event tree sequence. It is desirable that the PSA includes a table summarizing the success criteria of the system for the important accident sequence conditions.

The reviewers need to check that the fault trees model all the individual basic events which could lead either directly or in combination with other basic events to the top event. The set of basic events to be modelled on the fault trees needs to be

identified by a systematic analysis, for example, an FMEA which may have been carried out as part of the design assessment to identify the important component failure modes and a review of operator actions supported by task analysis to identify potential errors.

The fault tree model should include all the safety system components that are required to be operational and all the support systems including, for example, electric systems, cooling systems and I&C systems. It also needs to include passive components whose failure could lead to failure of the system (e.g. undetected filter blockage and pipe leaks), where these have not been screened out on the basis of very low probability.

The hardware dependences, including the functional dependences which could arise within systems, need to be identified and modelled explicitly in the fault tree analysis. It is good practice for the analysts to tabulate all these dependences in a dependence matrix, which can be used as a basis for constructing the fault trees and is helpful to the reviewers in checking them. Such dependences must not be included as part of the component failure dependences included in the common cause failure probabilities of the system. These are reserved for the more uncertain dependences which have not been explicitly identified and which are quantified by means of beta factors and similar approaches.

The intersystem dependences which could arise due to shared components need to be identified and modelled explicitly in the fault tree analysis. These could arise in separate safety systems which perform the same safety function or in the associated support systems. These need to be included in the fault trees for different systems (or different system failure modes) containing the same component.

The basic events modelled in the fault trees need to be consistent with the available component reliability data. The component boundaries and component failure modes need to be consistent with those defined in the component failure database. This is equally valid for both active and passive components.

The degree of resolution of the components in the fault tree should be sufficient to ensure that all the hardware dependences can be modelled. For example, pump cooling water systems are expected to be explicitly modelled in the fault trees to ensure that the dependences which can arise due to multiple pumps having the same cooling water system or water sources are taken into account correctly, as opposed to including the loss of cooling failure mode in the overall pump failure rate. The essential requirement is that a failure probability can be assigned to each basic event and that this is independent of all other basic events. There is no need, for example, to break a diesel generator down into its component parts when adequate reliability data are available on the whole system and can be reasonably regarded as independent of other equipment at the plant.

Where components are grouped together into supercomponents, the failure modes of each of the elements must have the same effect on the system. In addition,

all the supercomponents must be functionally independent in that no component appears in more than one supercomponent, or elsewhere as a basic event.

The support systems for components and subcomponents need to be identified and modelled in the fault trees to ensure that all hardware dependences have been explicitly taken into account. The support systems required typically include cooling systems for pumps and rooms, lubricating oil systems, power supplies to control circuits or to instrumentation circuitry, air systems and support systems for components in the support systems.

The operator errors which can contribute to safety system failure should be identified and are usually modelled explicitly in the fault trees. A review of HRA is presented in Section 3.6.

The common cause failures which can affect groups of redundant components need to be identified and modelled in the fault trees. The analysis should identify all the relevant component groups and the important failure modes. The basic events representing common cause failure need to be modelled in the fault trees (Section 3.4).

The temporary unavailability of individual components or trains of equipment which are taken out of service during the lifetime of the plant for testing, maintenance or repair need to be identified and modelled explicitly in the fault tree analysis. This may be done by either including basic events in the fault trees to represent component outages or by carrying out multiple runs of the fault tree analysis with different house events being introduced to represent the items of equipment which are removed from service during the allowed outage states, and then averaging the results.

The modelling of unavailability as a result of maintenance must be consistent with the way the system is actually taken out of service for maintenance and with the maintenance unavailability data that are available to quantify these fault events. Maintenance unavailability modelling is most typically high level modelling, at the system, train or major component group level. Where operation of the plant outside its technical specifications has been excluded from the scope of the PSA, maintenance configurations that are prohibited by the technical specifications or operating procedures are not to be modelled in the fault trees. Alternatively, maintenance restrictions on multiple components can be reflected by deleting mutually exclusive events from the initial cut sets.

The reviewers need to select some of the fault trees for a detailed review. It is important to focus on the systems that are important contributors to the core damage frequency in the PSA or have been found to be important in previous PSAs for similar types of nuclear power plants.

The reviewers need to be satisfied that there is a proper system of uniquely coding/labelling each of the basic events in the fault trees, and that this is used consistently throughout all the fault trees in the PSA.

3.3.2. Systems information required

To ensure that there is a valid and auditable basis for the fault trees, functional descriptions are required for each system for which a fault tree has been drawn, which identify:

(a) The function of the system,
(b) The mode of operation being modelled (for systems with more than one mode),
(c) The components that must operate/change state and their normal configuration,
(d) Whether the component operations are manual or automatic,
(e) The conditions that must exist for automatic signals to be received by the components.

In addition, it is helpful if a simplified schematic system diagram is provided for each system which shows the system as modelled in the fault tree, including:

- All the system components modelled in the fault tree,
- The normal configurations of the components,
- The pipe segments or wiring segments connecting the components,
- The support system interfaces (power, electric, cooling, etc.).

The functional descriptions and schematics provided for the safety system need to be sufficiently clear to allow the fault trees to be understood and reviewed in detail. It may be useful, however, to supplement this system information by a commentary in the PSA documentation explaining how this information was developed into the fault tree, so that the reviewers can clearly understand each node on the tree.

Simplified schematics also need to be provided for the control wiring of remotely operated components. Instrumentation is generally not included in such schematics. However, it is useful to have tables of the instrumentation in each system that identify the power supplies and other significant support systems.

3.4. ANALYSIS OF DEPENDENT FAILURES

In past PSAs, dependent failures have often been found to be one of the dominant contributors to the core damage frequency and to the other PSA results. Hence, the reviewers need to pay special attention to the treatment of dependences.

3.4.1. Types of dependences that can occur

The different types of dependences that can occur include the following:

(a) Functional dependences,
(b) Physical dependences,
(c) Human interaction dependences,
(d) Component failure dependences.

Functional dependences between safety systems or components can arise when the functioning of one system or group of components depends on the functioning of another system or component. These dependences can arise for a number of reasons including the following:

- Shared components;
- Common actuation systems;
- Common isolation requirements;
- Common support systems — power, cooling, instrumentation and control, ventilation.

Functional dependences include physical interaction between systems or components which can occur when the loss of function of a system or component causes a physical change in the environment of another system or component, for example, where loss of heating on a section of pipe allows it to freeze in cold weather.

Physical dependences can arise in two ways. Firstly, an initiating event can cause the failure of a safety system or component which leads to the failure of some of the safety systems or components required to provide protection. One example of this is where loss of all or part of the electrical distribution system, instrument ventilation system or service water system can lead to a transient and also degrade, or cause the failure of, one or more of the required safety systems. Another is for an interfacing system LOCA, where high pressure primary coolant flows back through low pressure piping following a valve failure. Because of the location of the LOCAs, the discharge of the primary circuit fluid can lead to the failure of components in the ECCS due to harsh environmental conditions or flooding.

Secondly, an internal hazard (such as a fire or a flood) or an external hazard (such as extreme environmental conditions, a seismic event or an aircraft crash) can cause an initiating event (a transient or a LOCA) and failure of some of the safety systems or components required to provide protection. For internal hazards, the safety system failures can arise as, for example, a consequence of pipe whip, missile impact, jet impingement and environmental effects.

Human interaction dependences arise when the operators make errors during repair, maintenance, testing or calibration tasks which lead to the unavailability or failure of safety systems or components such that they will not operate when required following an initiating event.

Human interaction dependences include:

(1) Test or maintenance activities that require multiple components to be reconfigured;
(2) Multiple calibrations performed by the same personnel;
(3) Post-accident manual initiation (or backup initiation) of components that requires the operator to interact with multiple components.

Component failure dependences cover those failures of usually identical components which are otherwise not analysed. Such failures may be caused by errors in design, manufacture, installation and calibration or by operational deficiencies and are treated quantitatively by common cause failure methods or other dependence quantification approaches. Common cause failure probabilities are usually quantified by using the alpha factor approach, the beta factor approach, the multiple Greek letter (MGL) approach or the binomial failure rate model to assess the probabilities of common cause failures on similar (redundant) components. Additional guidance in this area is given in Ref. [13].

3.4.2. Inclusion of dependences in the PSA

The reviewers need to check that a systematic analysis has been carried out to identify all the potential dependences which could reduce the reliability of safety systems and components in providing protection against initiating events. This will ensure that the selection of common component groups and the screening for inclusion in the PSA has been carried out correctly to ensure that important common cause failure groups have not been omitted. In addition, some of those dependences which are important in the PSA may be selected for a detailed review.

Whenever possible, functional dependences, physical dependences and human interaction dependences should be modelled explicitly in the event tree/fault tree analysis. In addition, an allowance is made in the analysis for the component failure dependences which are not modelled explicitly in the PSA. The reviewers should check that these dependences have been modelled correctly in the fault tree/event tree analysis.

Adequate justification needs to be provided for the common cause failure probabilities used in the PSA. Where possible, they need to be based on plant specific data. Where this is not possible, use of data from the operation of similar plants or generic data is acceptable.

3.5. ANALYSIS OF PASSIVE SYSTEMS, COMPONENTS AND STRUCTURES

In modern reactor designs there is a tendency to incorporate passive safety systems to carry out safety functions such as decay heat removal and emergency

core cooling. The PSA needs to take account of the reliability of these systems just as it does for the active systems. A separate issue is that of the treatment in the PSA of failures of passive structures and components, particularly of high energy pipework and vessels.

3.5.1. Passive safety systems

These have been introduced into modern designs (e.g. advanced pressurized water reactors (APWRs) and advanced boiling water reactors (ABWRs)) to provide higher reliability than can be obtained from active systems since they do not depend on support systems such as electric power, and often not on active initiation by the protection system. They are thus particularly valuable during station blackouts. Although the novelty of these passive systems has sometimes been viewed as presenting difficulties in PSA, their treatment is in principle the same as that of the passive systems, such as accumulators, and of inherent passive safety features, such as natural circulation of reactor coolant when the pumps are not available, which have always been incorporated into PSA.

There are, however, some aspects of novel designs of passive safety systems which warrant the attention of the reviewers. They must, as with active systems, have been shown to be effective by thermohydraulic analysis and by extensive tests. This deterministic demonstration of effectiveness needs to cover the full range of accident conditions for which they are claimed. Passive systems tend to work at much lower pressures than do active systems so that thermohydraulic performance predictions may be more difficult.

The successful performance of passive systems will have been demonstrated within a set of boundary conditions (e.g. for coolant temperature, pressure and inventory) which can only be ensured by the correct system set-up, including the correct configuration of the relevant valves (not necessarily within the passive system itself). Given the correct boundary conditions, and a satisfactory demonstration of effectiveness, it may be assumed that the system will work. The failure probability of the passive system is then the probability that the boundary conditions are not realized, i.e. that the system set-up is incorrect. This can be found by standard fault tree analysis, but the reviewers need to check that full account is taken of the potential for human error in leaving the system in the proper condition, as well as of all necessary valves (e.g. check valves) which are required to act and any active initiation signals.

3.5.2. Passive structures and components

These items may include structures, such as walls, floors and supports, and high energy pipework and vessels.

Structures. Failure of structures as a consequence of certain high energy events, for example seismic events and the impact from missiles generated by failures of pressurized or rotating components, is taken into account in the analysis of internal and external hazards (Section 3.9), and the detailed review of conditional failure probabilities (fragilities) requires assessment by specialists in these areas. Otherwise, the failure of a properly engineered structure is generally taken to have such a low probability that it need not be considered in the PSA. The reviewers may accept this approach, provided that the regulatory body has accepted the deterministic safety case for the structures, and that there is nothing in the operating history of the plant which casts doubt on particular items.

Pipework and vessels. The significance of these in PSA is twofold. First, a spontaneous failure will constitute an initiating event, and an estimate of its frequency will be required. Secondly, the pipework associated with a standby safety system may fail when it is brought into action, contributing to the system failure probability.

As regards initiating events, the main interest is in breaches of the primary circuit (LOCAs) and of the secondary circuit (steamline breaks and feedline breaks). For some plants, the utility may claim that certain components in the primary and secondary circuits (e.g. the reactor pressure vessel, the steam generator shells and critical lengths of pipework) have been engineered and inspected to such a high standard that the possibility of their failure may be ignored, i.e. that it is outside the design basis of the plant, and no specific protection needs to be provided. If the regulatory body accepts this claim in its deterministic engineering assessment, then the PSA reviewers may accept that these failures need not be included in the PSA model, or may be included with a correspondingly low estimated failure rate. For the other plants, it has to be recognized that the estimation of failure rates is subject to large uncertainties, due to the scarcity of relevant data and to the number of design, manufacturing and operating parameters which can influence the failure rates.

In many PSAs to date it has been common practice to base the initiating event frequencies on rather crude global estimates derived from limited data on failures observed in, largely, non-nuclear applications, with little account taken of plant specific factors. When the reviewers find that this approach has been taken, they will need to check the overall sensitivity of the PSA results to the frequencies adopted. If the sensitivity is low, and the values used are reasonably consistent with those found in other, peer reviewed, PSAs, this approach may be regarded as acceptable.

In recent years, however, improved methods for estimating failure rates in pipework have been developed [20, 21]. The mainstay of these methods, which have achieved a reasonable level of credibility, has been the compilation of comprehensive databases on pipework failures including events categorized as incipient failures, leaks and ruptures and with more detailed information on the design, inspection, service conditions and failure mechanisms. Such a database can then be used more or less directly, by selecting the data relevant to the plant in question, and by making use of

correlations between, for example, small leaks (which have a larger population) and ruptures, to provide plant specific failure rates.

Alternatively, the database can be used in conjunction with a probabilistic fracture mechanics code where it serves, firstly, to inform the expert judgements which need to be made on the uncertain values which are input to the code and, secondly, to validate the failure rates which are produced as the output of the code. This provides a more flexible tool, which can also be used to address the changes in risk due to different inspection strategies.

Where a probabilistic fracture mechanics code has been used in the PSA, the reviewers need to check that it is a state of the art code which has had adequate peer review QA, and that the code users are sufficiently qualified and experienced to be aware of its capabilities and limitations. If use has been made of a code or method which is not well established, it will need to be reviewed by specialists in this field, with the emphasis on validation against data from operational experience and/or experiments. A theoretical analysis without validation has little credibility for producing the absolute values needed in PSA, even though it may have some value in giving relative changes.

In standby safety systems, it is generally assumed that failure of the pipework contributes relatively little to unreliability of the system, and so this is often ignored in the PSA. Experience appears to bear this out and so the reviewers may accept this approach, provided (as with structures) that there is nothing in the history of the plant which casts doubt on the assumption.

3.6. HUMAN RELIABILITY ASSESSMENT

A significant issue in PSA is HRA and in particular the organization of the HRA activity, which includes the identification of the human actions to be considered, incorporation of these actions in the plant logic model (event and fault trees) and quantification of the related events. Given the high degree of safety system redundancy, diversity and reliability, fault sequences involving human errors leading to initiating events or failure to mitigate them often contribute significantly to the frequency of core damage.

The present description relates to the classical static representation of human behaviour in a PSA which is the most common approach used. More recently, the cognitive aspect of human behaviour in the dynamic interaction with the working environment has been taken into consideration using more advanced methodologies [22].

3.6.1. Framework for HRA

The reviewers should check that the HRA has been performed in a structured and logical manner and that all the steps of the analysis are documented in a

traceable way. This is particularly important since there is a wide variation in available methods for performing HRA and the state of the art in this area is still evolving. Consistent and correct application of the methods selected is a critical factor in a successful HRA.

The framework used for guiding the HRA needs to address all the key elements of the process. Guidance on the organizational aspects of the performance of HRA is contained, for example, in the systematic human actions reliability procedure (SHARP) framework [23].

The HRA procedure used usually includes the following important steps:

(a) Identification of human interactions,
(b) Establishment of the importance of human interactions (qualitative and quantitative screening),
(c) Incorporation of human actions into the appropriate parts of the logic model,
(d) Selection of suitable HRA methods,
(e) Quantification of human interaction events,
(f) Documentation of the analysis performed.

It is suggested that the reviewers compare the HRA process used in the PSA to SHARP to check that all the necessary steps have been carried out.

It is important to realize that a framework for guiding the overall HRA does not prescribe specific methods for performing the actual quantification of human error probabilities (HEPs). HEPs may be derived by using the techniques for the human error rate prediction (THERP) method [24], the human cognitive reliability (HCR) method [25] or the success likelihood index method (SLIM) [26], which are some of the commonly used methods. Other methods are also available and can be used where appropriate.

The reviewers should check that qualitative descriptions have been drawn up for each of the key human interactions which identify all the significant aspects associated with the action of the plant personnel. These would include:

- The timing of the action,
- The information available,
- The influence of prior actions.

The reviewers need to look for information in the PSA documentation and the event sequence boundary conditions to ensure that the situational and contextual influences on the plant personnel during the accident scenario are understood.

It is important to check that the screening of the human interactions identified has been carried out correctly so that human errors which could be significant to the core damage frequency have not been screened out from detailed consideration.

Screening is carried out to minimize the necessity for detailed modelling and quantification of all human actions in the logic model. This is done by first assuming conservative screening values for the human error probabilities. Detailed modelling and quantification is then done only for the human interactions which make a significant contribution to the core damage frequency.

3.6.2. Categorization of human interactions

Human interactions are usually classified as one of the following three types:

(a) *Type A*: human interactions occurring before the initiating event affecting the system or component availability,
(b) *Type B*: human interactions that cause an initiating event,
(c) *Type C*: human interactions which are performed in response to an initiating event.

Type A human interactions take place during normal plant operation before a plant trip occurs. They have a potential to cause the unavailability or failure of a component or system when it is required. Errors may occur during repair, maintenance, testing or calibration tasks. For many PSA studies, the Type A actions have been analysed using the THERP method [24]. However, this is not the only method and other methods may have been used.

The reviewers need to check that important Type A interactions have been identified and included in the assessment in a thorough and consistent manner. This usually involves a review of the plant maintenance, testing and calibration procedures to identify these actions for the systems modelled in the PSA.

The reviewers should check that the maintenance and test department practices to minimize human induced dependences, such as the use of different crews for redundant trains, are reflected in the HRA.

The reviewers also need to verify that the quantification process has been done correctly. It is also helpful to review the history of the plant for Type A human errors. The reviewers should pay particular attention to plant configurations in which valves are isolated (actuated and closed/opened) for test and maintenance purposes or calibration processes which can disable key instrumentation for either operator information or automatic functioning of safety systems.

Type B human interactions are those actions that cause an initiating event. HRA analysis of these actions is rarely done within the scope of the PSA analysis.

The reviewers ought to check that the human errors causing initiating events are accounted for in the occurrence frequencies of the initiating events analysed.

Type C human interactions take place following plant trip when the operator is following the procedures and training to bring the plant to a safe state. These actions are usually the most important human interactions to be considered in the PSA.

There are a number of available methods with which to analyse these actions, such as the HCR, THERP methods and SLIM methods. However, the state of the art in this area is still evolving.

Regardless of the method chosen for analysing Type C human actions, the same review process as for Type A actions needs to be performed. The aim is to check that:

(1) The process for identifying the Type C actions to be analysed is thorough and comprehensive.
(2) The quantification process has been performed accurately and consistently.
(3) Input and review from the plant operators has been included in the evaluation.

In some cases, the results of simulator observations may have been incorporated into the process.

3.6.3. Assessment

The reviewers need to check that the specific methods and/or techniques used for the HRA are suitable and that they have been correctly applied.

The plant specific and event sequence boundary conditions warrant careful consideration, for example, the adequate integration and/or feasibility of the human actions from a systems point of view within every single event sequence has to be examined and traceably documented. This refers to issues such as:

(a) Description of human actions;
(b) Precise indication of relevant part/subpart/paragraph of operational documentation, if they exist;
(c) Modelling in system functions and event sequences (together with a description of previous failures);
(d) Necessity/feasibility/entry and/or transfer criteria of considered human actions referring to the modelled position in the PSA (boundary conditions, assumptions and prerequisites).

With reference to the specific HRA method and/or technique selected, all the information and data needed for the assessment of the event sequences which depend on human performance have to be considered. Finally, it is necessary to pay attention to a coherent HRA and PSA modelling in the framework of a static assessment. This means, for example, that the interconnections between human actions have to be examined along an event path (sequence).

Thus a detailed HRA should be performed for all the human actions that appear in important cut sets using the initial screening values. It is also important to ensure that combinations of human actions are not truncated out of the screening quantification

because human action dependences have usually not been considered at this point. Often in screening, the dependence between human interactions is set to 1.0 to ensure that the related human action dependence is not eliminated in the process.

The reviewers need to check that the screening values used initially to help focus the analysis effort represent an upper bound for the human error probability.

To assess pre-accident (Type A) human actions, the following should be clearly identified and documented in the PSA:

(1) The components with which the operator or other personnel interact,
(2) The tasks and restoration actions that are specifically involved in each interaction,
(3) The relative locations of the different components when the operator interacts with multiple components,
(4) The components that have to be restored and for which alarms are activated in the control room if not restored,
(5) The type of post-test or post-maintenance validation process that is performed after a test or maintenance (such as operational test or plant staff observation).

It is important to check that all this information is given in the PSA. Evaluations of the probabilities of human error need to be reviewed to assess the data and quantification techniques used.

In order to assess post-accident (Type C) operator actions, it is important that the PSA clearly identify and document two sets of actions:

(i) Post-accident operator actions required for systems to operate successfully,
(ii) Post-accident operator recovery actions associated with specific accident minimal cut sets.

The first set of operator actions, those required for systems to operate successfully, includes manual operations of systems and components and manual initiations of systems and components as a backup to automatic initiations. All these operator actions should be identified clearly and documented in the PSA, including whether or not the actions can be taken from the control room, the procedures used, the control room indications used, the alarm and feedback indicators, the times required for the actions and the stress levels of the actions.

It is important to ascertain that all this information is available in the PSA and has been properly documented.

The reviewers need to check whether the methods and techniques selected are applicable and adequate for the assessment of human interactions modelled and considered in the PSA. This has to be assessed in particular for operator actions for which no (or no written) procedures are available.

The specific operator performance modelling should to be checked using appropriate techniques, for example, walk-through or talk-through procedures.

The reviewers then need to review the specific evaluations of human error probabilities to determine their consistency with the approach used.

Checks may be needed to determine whether the estimated probabilities are sensible with regard to the influences present and the assumptions made. The involvement of plant personnel needs to be sought in the assessment and modelling process.

It is important to identify any cases where several operator actions are combined together in the same sequence and to ensure that any dependences between the actions have been accounted for.

If expert judgement methods, such as the direct estimation approach, are used, the reviewers should examine the process carefully to find out how it was carried out. The review should cover the detailed description of human interactions, the situational influences with regard to the event sequences or scenario, the selection and number of experts, and the elicitation process itself.

The second set of operator actions, those required to recover specific minimal cut sets of accident sequences, includes those recovery actions that are linked to combinations of events (the minimal cut set events).

The reviewers need to check that the specific rules used for excluding and including recovery actions are identified and justified. The rules should cover the feasibility of the recovery actions. The modelling of human interactions has to be thoroughly documented. The PSA needs to identify clearly and document all the minimal cut sets that have recovery actions and the recovery action included. If more than one recovery action is applied to the same cut set, then verification is required that if the probabilities of these actions are independent there are no dependences between them, or if they are dependent then that the dependence is accounted for.

For the recovery actions that have been included, the reviewers need to check that the time to diagnose and correct the failures (this may mean that co-ordination is required between the main control room (MCR) staff and auxiliary operators), the location at which the recovery can be performed (the MCR or locally), the environment at the location, the access to the location and the stress level are all identified, justified and documented.

For the incorporation of the human interaction events into the systemic analyses, Type A actions are usually located in the fault trees and these need to be inspected for double counting or omission of common cause influences. Type C actions are usually located in the event trees or at a top level in the fault trees.

The reviewers should check the coherence of the modelling of the HRA and the systemic analyses in the overall PSA model, i.e. the incorporation of the results of HRA into the PSA has to be assessed.

3.7. DATA REQUIRED FOR PSAs

This section addresses the data required for the following items:

— initiating event frequencies
— component failure probabilities
— component outage frequencies and durations.

The data required for common cause failure probabilities and human error probabilities are discussed in Sections 3.4 and 3.6, respectively.

One of the main issues with data is their applicability to the plant in question, its particular components and operating regime. It is not often that there is much data available which are entirely applicable, and the reviewers need to recognize that the analysts will have had to use their judgement in selecting the best sources for each case. Clearly, plant specific data are always to be preferred to generic data but, even for a plant which has been operating for a number of years, the plant specific data are often rather sparse and have to be combined in some way with generic data. A balance has to be struck between the use of a small amount of more applicable (plant specific) data and the larger amount of less applicable data.

The reviewers need to ensure that the maximum use has been made of plant specific data, to compare them with the generic data and to satisfy themselves that there are reasonable explanations for any notable differences. This is important even when the two sources are combined, for example, using a Bayesian approach. Differences might arise for plants where the maintenance practices are more or less stringent. If there is no immediate explanation for any difference and the item is of importance in the overall PSA results, the reviewers need to carry out further investigation into the matter.

Data from the operation of similar plants are to be preferred to more generic data, such as those from other PWRs or BWRs, but may not have been readily available to the PSA analysts. For a new plant, the designers may have supplied them with data for a similar plant which they have designed and which has been in operation for a number of years, but the analysts may still have had to rely largely on generic data. In any case, the reviewers need to check that the data have been sufficiently well justified in the PSA documentation and shown to be relevant, item by item.

For initiating events with a low frequency or for equipment with a low failure probability, the data will be sparse or non-existent, even on a generic basis, and the values to be used in the PSA will then have to be assigned by informed judgement. The reviewers need to be satisfied that the bases for the judgements on these numerical estimates have been given and are acceptable.

3.7.1. Initiating event frequencies

The reviewers need to check that each of the initiating events, identified by the systematic analysis described in Section 3.1.1, has a frequency assigned to it. Many of these events can have a number of different and independent root causes (which need to have been identified in that analysis) and the reviewers should check that the frequency assigned to the initiating event covers all of these causes. The reviewers also need to check that there has been no double counting. For example, if a control fault were to cause the opening of a relief valve and is listed separately as an initiating event, then its frequency has not been included in the frequency of spurious opening of the valve. Similarly, where the scope of the PSA includes internal and external hazards (Section 3.9), and where a hazard which is explicitly evaluated can be the cause of, say, a transient, then its frequency has not been included in the frequency of the transient. It is also important to check that the frequency assigned to each initiating event group (Section 3.1.2) is the sum of the frequencies of the events in that group.

For an operating plant, the reviewers need to check that an analysis has been performed of all the initiating events which have occurred. If it has been in operation for more than a few years, it may be possible to base the frequencies of the more frequent events on these plant specific data, supplemented where necessary by more generic data. If the plant has been in operation for many years, there may be justification for excluding the first few years of data, because during this initial period the frequency of transients is usually elevated, but decreasing.

In some cases, such as initiators caused by loss of plant support systems, fault trees may be used to estimate the event frequency — see Section 5.2.2 of Ref. [8] and Section 6.6 of Ref. [3].

3.7.2. Component failure probabilities

The selection of generic data for each type of component and the applicability to the plant under consideration need to be justified in the PSA documentation. Plant specific data are preferable, if available.

If a combination of generic data from different sources is used, the methods used for selection of the specific data or for integration of the data from more than one source need to be given.

The component failure probabilities as input to a PSA are for failure on demand where the demand comes from the initiating event. For most components, however, the usual, and acceptable, assumption is that the failure has occurred during the standby period between the last test and the demand, or during the mission time for running components, and that the occurrence of the failure is random in time. If the failures of some components are treated as being caused by the demands, the reviewers

will need to see a justification of this. Thus standby component failure rates are generally quoted in rates per hour. These are then multiplied by half the appropriate surveillance test interval to give the value of failure per demand to be input to the PSA evaluation. If the failure rates are quoted as per demand in generic data sources, they must first be translated to rates per hour by dividing them by half the test interval appropriate to the source of the data, and then back to failures per demand by multiplying by half the test interval for the plant in question.

As noted above, the best approach may be to combine plant specific with generic data in obtaining the final estimates for the PSA quantification. This combination may be made by inspection and judgement or by using a Bayesian approach. The latter has the advantages of being more consistent and repeatable, and also of combining the uncertainty distributions in the same process, but the use of judgement, where an acceptable basis is stated, may give values which are just as valid. In either case, care needs to be taken that the generic data/Bayesian priors are not inconsistent with the plant specific data, in terms of both component definitions and numerical values, or that any discrepancies have been adequately explained and accounted for in the combination process.

The reviewers may audit how the analyst used plant records to make plant specific estimates of the number of events or failures. The reviewers also need to check the consistency between the definitions of failure modes and component boundaries used in the PSA and the definitions used in the data records.

The estimation of the number of demands, operating hours or standby hours is important in the analysis of specific plant records. The reviewers need to check this estimation for selected components.

The results of the data analysis are usually shown in a table that gives, for each component that appears as a basic event in the fault trees (or occasionally in the event trees), the component definition, the failure mode, the estimated mean failure rate and some measure of the associated uncertainty. Where the scope of the PSA includes an uncertainty analysis, the distribution of each failure rate is required and this is usually characterized by the median and the 95 and 5% probability limits or a range factor. The mean must always be given, since this is the measure generally used in any point calculations and in comparisons with other PSAs.

Where components such as pumps are required to run for some time post-trip, the mission times that are used with their operating failure rates need to be justified, taking account of the definitions of the long term safe states used in the event tree analysis. For some accident sequences, following a large LOCA for example, the time required for recovery of the plant to a safe state may be a matter of weeks or months. In such cases, the reliability model has to allow for replacement/repair of components which have failed during the mission time, if this is within the scope of the PSA, and this will then require estimates of the times required for access and replacement/repair of the components. Times for access should include considerations of the

radioactive environment of the component during the particular accident sequence. For many accident sequences, however, the mission time will only be a matter of a few hours and replacement/repair may not be practicable. In these cases, while it is still preferable to determine the appropriate mission time for each component in each sequence, it is often the practice for a blanket mission time, such as 24 hours, to be adopted as a conservative approximation. This may be acceptable provided that it has been justified and does not introduce an undue degree of conservatism.

Further guidance on data may be found in Ref. [27] and in Section 5.3 of Ref. [8]. Appendix I of Ref. [3] contains representative ranges of component failure rate and unavailability data that have been used in past PSAs to assist in determining the validity of the data used. These ranges are derived from Ref. [28].

3.7.3. Component outage frequencies and durations

This section addresses the data for the frequencies and durations for component outages for test, maintenance or repair. The reviewers need to be satisfied that these data be a realistic reflection of the practices in use at, or planned for, the specific plant, although a small degree of conservative bias may be acceptable.

For the calculations of system and component unavailabilities due to maintenance, testing or calibration, the use of plant specific data, where possible, is preferable to the use of generic data. The analysis should include an evaluation of the impact of unscheduled maintenance on system and component unavailability. This represents a time consuming task because the plant maintenance and component unavailability records need to be reviewed and analysed. This task may be less onerous for stations that keep a computerized log of such records.

If a plant specific analysis has been performed, the reviewers need to check that the calculations have been performed correctly. If generic data have been used, the reviewers need to verify that the source is recent and is recognized as acceptable.

Further guidance can be found in Section 5.3 of Ref. [8].

3.8. ANALYSIS OF COMPUTER BASED SYSTEMS

3.8.1. Introduction to computer based systems

Programmable computers are increasingly being used in the protection and control systems of nuclear power plants. It is expected that all future designs will be computer based, whether they are for new plant or for major upgrades of existing plants. However, they present problems for reviewers which are distinctly different from those of traditional hard wired systems, particularly as regards the estimation of their reliability.

The reliability analysis of a hard wired system is generally based on the assumption that deterministic analysis and testing will have ensured that there are no significant errors in the design, so that its failure rate will be dominated by the random and common cause failures in the hardware. For a computer based system, on the other hand, assuming that it has adequate redundancy, the failure rate will generally be dominated by errors in the software, with the contribution from hardware faults being relatively small.

One of the main problems posed by the use of discrete logic in computers (as opposed to the continuous response from a hard wired system) is the vast number of possible combinations of digitized inputs from the sensors on the plant (the *input space*), combined with an inability to interpolate with any confidence between successful tests. Thus testing cannot be relied on to give a reliability figure for the system, particularly since the number of tests, although it may run to tens of thousands, can in practice be only a small subset of the input space.

Another feature of a software based system is that advantage is usually taken of the ease with which the functionality of the system can be extended, i.e. it performs more functions, both safety and non-safety, than a hard wired system would have done. These include some of the calculations, for example to give the sub-cooling margin, which the operator would have previously done by hand, but may also involve the derivation of more sophisticated quantities which enable the operator to maintain a higher power level without loss of safety margin. Overall there is a clear tendency towards a system of considerable complexity, to the extent that there may be no one person who has a good understanding of the whole system and its relation to the safety case of the plant.

The reviewers need to recognize that, at the present state of the art, it is not possible to derive a failure rate for a software based system on an objective and fully defensible basis. The reliability assigned to the system is ultimately a matter of judgement on the part of the utility. This judgement will rest mainly on the extent to which the deterministic safety case for the system has been satisfied, and for this the PSA reviewers would normally rely on the views of the specialists who carry out the regulatory review of that deterministic case. The requirements of such a case have been evolving in recent years and the main features are now reasonably well established [29–34].

Since it cannot be proved that the software is free from errors, the emphasis is on the quality of the production process, to show that the procedures adopted will have minimized the likelihood of errors being made in producing the software and maximized the likelihood of finding any errors by checking the code (static analysis) and by testing the completed system (dynamic testing).

Errors are almost certain to have been made, and there can be no assurance that they have all been found, but it is important to distinguish between unsafe errors, which could prevent the system performing its safety functions, and those which

either have no effect on the plant or are in the safe direction. It is quite possible that the software will actually be free from errors with a safety impact, although this can never be demonstrated conclusively. It is good practice for the designers to separate out the parts of the software which perform the more critical safety functions (sometimes referred to as the *safety kernel*), and which therefore have the potential to contain unsafe errors, so that checking and testing can be concentrated in those areas.

3.8.2. Reliability analysis of computer based systems

In the reliability analysis, computer based systems are usually first decomposed into parts which can be treated separately and where the dependences between the parts can be identified clearly, as for the analysis of a conventional system. If the system is integrated, the dependences may well be too great or too uncertain to be modelled with any confidence and the system would then have to be treated as a whole. If, however, the system is effectively a set of subsystems each of which performs a fairly simple safety function, as may occur when it replaces an earlier hard wired system, without extending the functionality, then decomposition is advantageous, since estimates and judgements can be made on each part separately.

The reviewers need to be satisfied that the failure probability of the computer system hardware has been calculated in an acceptable way. A standard approach, as described in Section 3.3, should have been followed, taking account of both random and common cause hardware failures. Account also needs to have been taken of the self-checking facilities which are usually built into such computer systems, since these are there to reveal any hardware failures. If the system has adequate redundancy of trains (e.g. threefold or fourfold) and is otherwise well designed, the failure probability calculated for the hardware is usually relatively low, for example 10^{-5} failures per demand or less. Values greater than this may indicate a weakness in the design or a problem with the analysis, and may prompt the reviewers to investigate the matter in more detail, perhaps in conjunction with the regulator's computer specialists.

A judgement on the software contribution to the total system failure probability needs to take account of all relevant factors, which include:

(a) The size and complexity of the system (the number of lines of code is an indication);
(b) The novelty of any of its features;
(c) Whether it identifies a safety kernel;
(d) The degree of conformity with procedures and standards in the production, checking and testing processes;
(e) The independence of the teams performing the static analysis and the dynamic testing;
(f) The number of errors found in these two processes;

(g) The extent of the use of formal analysis tools in the static analysis;
(h) The number of dynamic tests carried out;
(i) The experience of the designers of the system;
(j) Experience with similar systems in service.

As regards the last item, it can be very helpful to compare the system with a similar system (perhaps non-nuclear) for which there is some operating experience, making allowance for the similarities and the differences. In practice, however, this approach is unlikely to be useful except for the smaller and simpler systems.

The software failure probability of a large integrated protection system might be judged, taking account of the above factors, to be of the order of 10^{-4} failures per demand. If the probability is claimed to be much lower than this, the reviewers need to investigate in greater depth, preferably in conjunction with their computer specialist colleagues, to see if there is an acceptable argument for assigning a low failure rate to the system in question.

3.8.3. Software dependences

Since the reliability that can be claimed for a computer based protection system may be rather limited, relative to the requirements of the safety case for the plant, it would usually be backed up by a diverse system. If the diverse system is hard wired, then complete independence may be assumed. If, however, the diverse system is another computer based system, then the degree of dependence must be estimated. The designers may have gone to considerable lengths to achieve diversity in both the hardware and software, using, for example, different teams, programming languages and manufacturers, and may then claim complete independence. Such a claim should not be accepted since some dependence between the two sets of software must be regarded as inevitable, although the degree will be a matter of judgement.

Where a control system and a protection system are both computer based, consideration needs to be given to software dependences between them. There may be the potential for a software error to give rise to a control fault (initiating event) and also disable the protection system against that fault. Where the control and protection systems both appear on an event tree, some dependence needs to be assumed.

3.8.4. Sensitivity studies

As will be clear from the comments above, there are substantial uncertainties in the failure probability assigned to computer based systems and to the dependence between different systems in the same plant and this needs to be addressed by sensitivity studies.

The reviewers need to be satisfied that a suitable range of studies has been carried out to determine the sensitivity of the results of the PSA to the failure probabilities used for the computer based systems, including any dependences between these systems.

3.8.5. Further considerations

Computer components are liable to be more vulnerable to some environmental conditions such as temperature than those of hard wired systems. If this has not been ruled out in the deterministic case, for example, by qualification of the equipment, then the reviewers must be satisfied that it has been modelled in the PSA.

Computer components are also liable to be vulnerable to electromagnetic interference, for example, from mobile phones. The reviewers need to check whether administrative measures have been put in place to prevent this from being a problem and whether it is necessary to make some allowance in the PSA, perhaps by increasing the initiating event frequency for spurious control actions.

It is very likely that changes will be made to the software, to remove errors and to improve its functionality, both before its installation and throughout its operational life. Because it is difficult to predict all the implications of such changes, it is of great importance that they are subject to very careful checking and testing, following an established checking procedure. This may not have any direct effect on the PSA but the reviewers need to be aware of the status of the changes and be clear as to which have been allowed for in the specification of the plant under review.

The PSA reviewers will need to work in consultation with computer specialists, and should be aware that they are liable to use a slightly different set of concepts and terminology to those common in PSA. Some effort may be needed to ensure good communications.

3.9. ANALYSIS OF INTERNAL AND EXTERNAL HAZARDS

This section provides guidance on the review of the PSA for internal and external hazards, sometimes referred to as external events, even when internal hazards are included. These hazards are initiating events and need to be regarded as being of the same importance as initiating events caused by internal plant faults (transients and LOCAs). This section addresses the identification of internal and external hazards and the screening carried out to eliminate those which are unimportant contributors to the core damage frequency. It then gives guidance on three specific hazards — earthquakes, internal fires and internal floods — which have typically been among those found to give significant contributions to risk. This guidance illustrates the general approach, which can be adapted to the review of the analysis of other hazards. Further guidance can be found in Refs [11, 12, 35].

For some hazards, their definition as initiating events and the calculation of their effects on the plant, in terms of conditional probabilities of failure for its structures, systems and components, are specialized areas of PSA. The incorporation of the plant failures due to hazards into the PSA is, however, the same in principle as that for transients and LOCAs, and very often the same event trees and fault trees can be used, perhaps with some adaptation, although in some cases new trees are needed to represent the accident sequences.

A key feature of most hazards is that they can cause a disturbance to the operation of the plant and can also disable or degrade the safety systems required to give protection against the disturbance. They can also be the cause of several plant faults at the same time, requiring more safety systems to operate.

Since dependences are usually important in hazard analysis, the reviewers need to pay particular attention to the way these are modelled. One approach is to model each dependence explicitly within the structure of the event and fault trees, as is normally done for plant based initiating events. This approach allows the evaluation of the hazard related dependences to be integrated with that of, for example, the random and common cause failures and human errors, and so it may be preferred. Another approach is to evaluate the fault and event trees without the hazard related dependences, and then to account for these by manipulating the appropriate accident sequence minimal cut sets where dependent failures in the same minimal cut set have been identified.

3.9.1. Identification of internal and external hazards

The selection of hazards for incorporation into the PSA usually starts with a list of hazards which is as complete as possible, regardless, in the first instance, of their potential for causing damage or of defences built into the plant. In the compilation, or checking, of such a list, it is useful to refer to the lists in USNRC NUREG/CR-2300 PSA procedures Guide [36] or in other PSAs. The hazards are normally categorized by a scheme such as:

- *Internal hazards:*
  - — fires
  - — flooding
  - — missiles
  - — dropped loads.
- *Natural external hazards:*
  - — earthquakes
  - — high winds
  - — extreme temperatures (air and sea water)
  - — floods

— lightning
— meteorites.

- *Human made external hazards:*
  — aircraft crashes
  — explosions
  — toxic gases.

The list of candidate hazards is then reduced by screening out those which:

(a) Are inapplicable to the site/plant (e.g. volcanoes for most sites);
(b) Are of negligible frequency (e.g. relative to the core damage frequency (CDF) from internal plant faults);
(c) Can have no significant impact on the plant.

The screening is normally done in several stages, first by inspection and judgement, then by rough estimates of frequency/impact and finally by more detailed estimates, for example, as described in Ref. [11]. It is good practice to inspect the screening process reported in the PSA documentation to ensure that there is a justification for the exclusion of each hazard screened out, rather than a bald statement of what has been included. The remaining hazards need to be accounted for in the PSA. Some will need detailed analysis with specialist input, for example, earthquakes, internal fires and aircraft crashes. Other hazards, which are clearly only going to make a minor contribution to risk, may be given an approximate treatment — hand calculations may suffice. In the latter case, it is desirable for the results of the hand calculations to be incorporated in the computerized evaluation of the PSA, so that importance factors can be calculated and sensitivity studies performed without recourse to supplementary manual manipulations.

Each hazard has to be defined in terms of its specific source or of a parameter giving its impact potential (e.g. wind speed). It is also generally subdivided into bands or ranges as follows:

(1) Seismic event — bands/ranges of earthquake severity/peak ground acceleration (pga);
(2) Winds — bands/ranges of wind speeds;
(3) Internal fires — each room with combustible material;
(4) Aircraft crashes — type of aircraft (military, light aircraft, airliner or helicopter);
(5) Internal floods — specific sources (pipe breaks or tank overflow).

Each of these subdivisions is usually treated as a separate initiating event in the PSA, with its own event frequency. For continuous parameters, the frequency of the

band is, of course, the difference between the exceedance frequencies at either end of the band. The reviewers need to check that the subdivision is not so coarse that it conceals the dominant contributions to risk. For example, if a seismic event was divided into many bands of pga values, those of relatively high frequency, with pga just above the design basis level, may cause relatively little damage while those in the highest pga band may be very likely to lead to core damage but be of very low frequency, leaving a maximum contribution to risk from an intermediate band. A division into only two pga bands would obscure this insight and may well give the wrong total risk for the hazard. On the other hand, a fine subdivision is not usually warranted, in view of the large uncertainties in all hazard analyses. For minor hazards, a single specified event is often acceptable.

For most hazards, the plant will have been designed to withstand specified levels/types, and a deterministic case will have been made that hazards within the design basis will not lead to core damage (although the plant may have to be shut down for inspections and repair of damage to items of plant which are not important to safety). The probability that a hazard within the design basis will cause damage to safety related plant is not then zero, and it may be included in a refined analysis, but it is common practice, and acceptable, to assume that it is negligible, i.e. that all the risk comes from hazards which are beyond the design basis. The reviewers need to be aware that an assumption that a hazard outside the design basis necessarily leads to core damage may be excessively conservative.

3.9.2. Seismic analysis

Guidance on the review of seismic analysis can be found in Refs [11, 12]. The analysis, in general, includes the following steps:

(a) Estimation of the frequency of seismic events as a function of their severity at the plant, which is often characterized by the pga — often referred to as the seismic hazard curve.
(b) Estimation of component and structural failure probabilities (fragilities) as a function of seismic severity.
(c) Evaluation of physical and systematic dependences between components due to the seismic event.
(d) Estimation of the effects of the seismic event on the possibilities for and probabilities of human error. This needs to cover psychological factors, such as increased stress as well as confusion arising from loss of equipment and spurious indications.
(e) Calculation of the core damage frequency due to the seismic event by combining the frequency of a seismic event of a given severity with the probability that

the accident sequences occur, and then summing over the range of seismic events possible at the site.

(f) Sensitivity studies and uncertainty analysis.

The reviewers need to check that each of these steps is clearly identified in the PSA and that the bases are given for the data and models used in each step. The data and models used warrant careful review to determine that they are consistent with accepted data and models used in these areas.

The relationship between the frequencies of seismic events and their severity (seismic hazard curve) at the site is usually based on relevant historical experience for the regions around the plant or for regions of similar seismicity. The estimation of the curve needs to consist of a parametric fit to data, with associated uncertainty distribution. The maximum severity cut-off for the curve needs to be identified and justified.

Soil failures as a direct result of an earthquake, for example, liquefaction and slope instability, should be considered.

The data for component and structural fragilities are often sparse and have to be extrapolated to cover the range of accelerations. This is usually done by assuming a log–normal distribution and fitting this to the available data points, or to parameters (e.g. the median and 5th/95th percentiles) given by expert judgement, in the absence of relevant data. Other assumptions may also be acceptable, if a reasonable justification has been given, as is a stepwise approximation, in view of the high degree of uncertainty in this area. An indication of the extent of the uncertainties in the fragility curves needs to be given, in so far as these can be known, and where the scope of the PSA includes an uncertainty analysis these uncertainties will have to be quantified. Sources for the fragility curves and their uncertainties need to be documented.

Evaluation of physical dependences between components usually cover cases in which tanks, walls and ceilings can collapse and fall on critical components and cause their failures. These are often the dominant contributors to failure in seismic events. It is important that the evaluations also cover support structures, tables, cabinets and instrument racks that can fail or fall over as a result of a seismic event and cause the failure of critical components.

It is necessary to carry out a detailed and specific HRA for seismic events. By this means the effects of seismic events on the probability of human error are estimated and human error probabilities that are increased by the seismic event and those that are not are identified, with a rationale for these assessments. Human error dependences in the PSA should also be assessed for possible increases in their probabilities due to seismic events. The recovery actions need to be reviewed to identify changes in any conditions due to seismic events that result in higher non-recovery probabilities (such as room access concerns or hazardous room environments).

The calculation of the core damage frequency needs to combine the initiating seismic frequencies and minimal cut set probabilities with sufficient resolution of seismic load parameters to provide for an accurate numerical integration. The sum of the component fragility and its unavailability due to internal plant causes must be used as the component unavailability in these calculations. Alternatively, they can be modelled as separate basic events in the fault tree, giving a more adaptable model, for example, for sensitivity studies.

The reviewers should select specific accident sequences in order to review in greater depth the steps used to obtain the contribution to the accident sequence frequency from seismic events. Accident sequences due to loss of off-site power are generally dominant contributors to the core damage frequency from seismic events and need to be included in the sequences examined.

3.9.3. Fire analysis

Guidance on the review of fire analysis can be found in Ref. [3]. The analysis in general includes the following steps:

(a) Initial screening to eliminate fire scenarios in rooms that are small contributors to plant risk;
(b) Estimation of the frequency of fires of different sizes starting in different rooms of the plant;
(c) Assessment of the type of plant disturbance potentially caused by a fire;
(d) Calculation of the propagation of the initiated fire and propagation of fire effects to affected components and operators;
(e) Estimation of non-detection and non-suppression probabilities for the initiated, propagating fire;
(f) Evaluation of component dependences and component failure probabilities due to the effects of fires;
(g) Estimation of the effects of fires on human actions and possibilities for increasing the probabilities of human errors being identified;
(h) Calculation of the core damage frequency due to fires by combining the fire initiation frequency with the component failure probabilities and failure of operator recovery actions.

The reviewers need to assess whether each of these steps has been clearly documented and whether the basis and assumptions for the data and models have been given. Specific points to address in the review include the following:

(1) The documentation needs to state clearly what specific event is considered for the initiation of a fire in each area in which fire is considered. When more than

one initiating fire can occur, the PSA needs to describe the basis for the differentiation.

(2) If a screening process is carried out, for example to identify the critical locations or compartments, the screening technique, including the basis for any screening of fire initiation frequencies used, needs to be assessed for its validity.

(3) Evaluation of the potential impact of fires on plant operation should include component or system actuation due to fire effects which, for example, could initiate LOCA type sequences.

(4) The databases used for the fire initiation frequencies need to be referenced so that the reviewers can check for consistency between the databases and the data for the plant analysed.

(5) If generic databases are used to derive the frequencies of fires that are not detected and become established, then differences in fire detection efficiencies need to be considered in applying the generic data to the specific plant.

(6) Plant specific data or data from plants similar to the one in question need to be reviewed in the PSA to determine whether plant specific fire initiating frequencies can be estimated. If plant specific data exist, plant specific initiating frequencies are expected to be estimated by means of accepted Poisson approaches describing the likelihood and Bayesian approaches describing the uncertainties in the parameters.

(7) The propagation of the effects of a fire needs to be calculated by means of one of the accepted fire propagation approaches. Input parameters to the calculations warrant careful review to determine whether they represent the actual plant. The parameters to be reviewed need to include the amount of permanent or transient combustible material available in each zone. The transmission of smoke through ventilation ducts and the heating of instrument and component compartments is usually included in the propagation analyses.

(8) The probabilities of non-detection and non-suppression are incorporated into the fire propagation analysis to determine the probability that the fire propagates to critical equipment without detection or suppression. Account should be taken of the physical layout and of manual as well as automatic actions in determining non-detection and non-suppression probabilities.

(9) The evaluation of multiple components that can simultaneously fail owing to a fire needs to include consideration of the effects of heat, smoke and water due to the operation of fire suppression systems.

(10) The evaluation of operator actions related to the fire should take account of the effects of smoke (through ventilation ducts) and hazardous effects due to materials in fire suppression systems. Effects on the operator also need to include the effects of fire on the availability of instrumentation and related equipment.

(11) The quantification of fire barrier efficiency should be documented in the PSA. The reviewers need to check whether penetrations in the barriers, such as doors that may have been left open, have been taken into account in probability assignments.
(12) Fires in MCR control panels can lead to MCR evacuation and transfer of control to a shutdown panel location. Procedures for operator actions may suffer from diagnostic difficulties and the panel may have limited instrumentation, which would affect the HRA. This needs to be taken into account in the PSA.
(13) If fault trees are developed for fire suppression systems, the treatment of dependences caused by fires should be reviewed.
(14) The results of the fire analysis need to be as clearly presented and structured as the rest of the PSA analysis. It is good practice to perform sensitivity analyses on those areas of the analysis where especially questionable assumptions have been made.

Further guidance on internal fires PSA can be found in Ref. [35].

3.9.4. Internal flood analysis

Guidance on the review of internal flood analysis can be found in Ref. [3]. The analysis in general includes the following steps:

(a) Initial screening to eliminate flooding scenarios in rooms that are small contributors to plant risk,
(b) Identification of the possible water and steam sources,
(c) Assessment of the type of plant disturbance potentially caused by the flooding,
(d) Evaluation of the frequency of occurrence of an initiating event caused by these sources,
(e) Estimation of the likelihood that the operator does not detect and control the flooding,
(f) Identification of the components that are affected by the flooding,
(g) Calculation of the frequency of core damage due to internal flooding by combining the initiating event frequencies with the probability of occurrence of the accident sequence.

The reviewers should check that all these steps are clearly identified, the data used are documented and the calculations performed are clearly presented.

The initiating event evaluations should include operator or maintenance personnel errors of inadvertently opening valves as well as tank and valve ruptures.

Evaluation of the potential impact of flooding on plant operation usually includes component or system actuation due to flooding effects, which could initiate special sequences.

The frequencies of initiating events are first screened for their potential contribution to the core damage frequency. Initiating event frequencies that are significantly lower than the internal event core damage sequence frequencies can be screened out.

Consideration of components affected by flooding should take into account elevations, barriers, doors and drains. Drain blockage needs to be considered. A conservative approach is to assume that all components fail in the compartment that is affected. If this assumption does not cause a significant contribution to the core damage frequency, the initiating event can be screened out. It is necessary to assess the possibility of flooding from one room to another through equipment drains.

All potentially contributing initiating events need to be evaluated in terms of the means of detecting and controlling the event. The means then needs to be considered in estimating the non-detection probability.

Additional human actions that may be needed to mitigate the flooding sequence should be identified and assessed for their probability of success/failure. These include, for example, isolation and subsequent restoration of the electric power supplies. It is important that the HRA takes into account the loss of I&C equipment and spurious indications that may be generated due to the flood.

3.10. QUANTIFICATION OF THE ANALYSIS

The next stage is to quantify the analysis to determine the core damage frequency and to identify the sequences which contribute to core damage. This requires that a Boolean reduction be carried out for the logical models developed using event trees and fault trees for each of the initiating event groups. The accident sequence frequencies are then calculated using the data, for example, for initiating event frequencies, component failure probabilities, component outage frequencies and durations, common cause failure probabilities and human error probabilities. A number of computer codes are available that can be used to carry out this analysis.

The reviewers need to verify that the PSA quantification process is technically correct and thorough, and that key dependences are correctly accounted for in the quantification process. The quantification process needs to have been carried out using a suitable computer code which has been fully validated and verified. In addition, the users of the codes need to be adequately experienced, and understand the uses and limitations of the code.

It is necessary for the reviewers to check that the accident sequences/cut sets identified do actually lead to core damage. This is advisable for a sample of the sequences, focusing on those which make a significant contribution to the risk.

Where cut-offs are used in the quantification process (either on cut set order or frequency), the reviewers should check that they have been set at a sufficiently low level that they would not lead to a significant underestimate of the frequency of core damage.

3.11. SENSITIVITY ANALYSIS, UNCERTAINTY ANALYSIS AND IMPORTANCE ANALYSIS

While the more important products of a Level 1 PSA may be qualitative, such as the identification of weaknesses in the design, interest is always focused on the calculated value of the core damage frequency, since this is the quantity which, within the limitations of the art, encapsulates all the judgements which have been made by the analysts on the safety of the plant, and is the principal quantity which is used in comparisons with the results of other PSAs and with probabilistic criteria. As noted before, the aim is for the PSA to be based on a reasonably realistic representation of the plant and its operations, and to give a best estimate of the core damage frequency, i.e. one without deliberate or known bias. The calculation may be based on point values, yielding a single point value for the frequency, or it may incorporate the propagation of uncertainties throughout the analysis, yielding a probability distribution for the frequency. In the latter case, the core damage frequency quoted, for comparison purposes, should be the mean of the distribution, and not the median, or other measure, which can be very different from the mean for a skewed distribution. In a point value calculation, the reviewers need to ensure that the input data are best estimates of the means.

There is a divergence of views among PSA practitioners as to which of these approaches is correct and the reviewers should follow the policy of their regulatory body, or national practice, as to whether a point value calculation is acceptable or whether a formal uncertainty analysis is required. If a probabilistic criterion has to be met at, say, a 95% confidence level, then an uncertainty analysis is needed to demonstrate this. Where a point estimate is regarded as acceptable, but is considered to be the mean of an implicit probability distribution, the reviewers need to be aware that the use of mean values for the input data to the PSA will not in general yield the mean for the output, the core damage frequency. This is due to the non-linear nature of the analysis, largely arising from the use of redundancy in safety systems. In such a case, the reviewers should look for a justification, in the PSA documentation, that the error thereby introduced is small. An argument that this is so may be based on the dominance of common cause failures, which are additive rather than multiplicative, over random failures, as is normally the case for modern plant designs.

Whichever approach is taken, the calculation of the core damage frequency should be complemented by sensitivity studies to explore the major uncertainties

separately. In addition, importance analyses are required to be performed to identify the significant initiating event groups, the system and the basic events that contribute to the risk.

These three areas are discussed below.

3.11.1. Sensitivity analysis

The aim of carrying out a sensitivity analysis is to address those issues such as the modelling assumptions and data which are suspected of having a potentially significant impact on the results. These assumptions or data are generally in the areas where information is lacking and heavy reliance must be placed on the analyst's judgement. Sensitivity analysis can be performed by substituting alternative assumptions or data and evaluating their individual impacts on the results. In the case of data, a judgement has also to be made on the worst plausible value to be used in the sensitivity study, and this is usually based on the measures of uncertainty quoted with the mean values in the data listing.

Throughout their review, the reviewers need to have identified and noted items of data or assumptions which are candidates for sensitivity studies, owing to their uncertainty or their reliance on judgement. Some of these may later be filtered out on the basis of their importance factors, and others added which have a significant impact on the PSA results. The reviewers should be wary, however, of discarding a candidate for sensitivity studies just because it has a low calculated importance factor, since this can simply reflect the assumptions made. Modelling assumptions need to be addressed case by case, since they do not appear as such in the PSA results, but it may be possible to use simple bounding calculations rather than rerunning the PSA evaluation. The reviewers should check that sensitivity studies have been performed on all the appropriate assumptions and data.

Section 6.5.2 of Ref. [8] provides additional guidance in the area of sensitivity analysis for component failure dependence and human error dependence.

3.11.2. Uncertainty analysis

The aim of carrying out an uncertainty analysis is to provide quantitative measures and qualitative discussions about the uncertainties in the results of the PSA — namely, the frequency of core damage, the frequency of the dominant accident sequences and accident sequence categories. Additionally, important figures show the order of the contribution of specific uncertainties.

Uncertainties can be classified into three general categories:

— incompleteness
— model uncertainty
— parameter uncertainty.

Incompleteness. The aim of the PSA model is to identify all the possible scenarios that can lead to undesirable consequences — core damage for a Level 1 PSA. However, there is no guarantee that this process can ever be complete and that all possible scenarios have been identified and properly assessed. This lack of completeness introduces an uncertainty in the results. This type of uncertainty is difficult to assess or quantify.

A careful review of the identification of initiating events and the plant response modelling needs to be performed in order to gain confidence that the uncertainty introduced by incompleteness is reasonably small.

Model uncertainty. Even for those scenarios that have been identified, there are uncertainties introduced by the relative inadequacy of the conceptual models, the mathematical models, the numerical approximations, the coding errors and the computational limits. For the time being, quantification of model uncertainties is still a very difficult task, and there is no generally accepted method available yet.

The reviewers need to assess the relative importance of model uncertainties by reviewing the results of the sensitivity analysis discussed above.

Parameter uncertainty. The parameters of the various models used in the PSA are not known because of scarcity or lack of data, variability within the populations of plants and/or components, and assumptions made by experts. Parameter uncertainty is, at present, the most readily quantifiable among the three types of uncertainties.

The reviewers may consider it useful to focus on the method(s) used for uncertainty analysis, the basis of selected distributions and input values for different parameters (including error factors or standard deviations), and on whether dependences have been properly treated in the uncertainty quantification (e.g., in the correlation of variables) to ensure that the uncertainty analysis process is technically accurate and that the uncertainties have been propagated through the models correctly.

More details about parameter uncertainty analysis can be found in Section 6.4.1 of Ref. [8].

3.11.3. Importance analysis

Importance analysis determines the importance of contributions to core damage frequency, accident sequence frequencies and system unavailability. Importance analysis is particularly important for PSA applications such as design modifications or identification of weaknesses. Importance analysis and sensitivity analysis are related.

Various types of importance factor are normally calculated automatically for each basic event by the computer code used for the evaluation of the PSA. These typically include the Fussell–Vesely and Birnbaum importance factors and the risk reduction and risk achievement worths. The reviewers need to check which types of importance measure have been produced, and will expect to see at least the Fussell–Vesely factors. The

reviewers should check that the importance analysis results are in general agreement with the sensitivity analysis qualitatively, and that they make logical sense.

More details about importance analysis can be found in Section 6.5.1 of Ref. [8].

3.12. RESULTS OF PSAs

The value of a PSA lies largely in the successful communication of its results to the users, who probably include non-specialist senior managers as well as PSA specialists, in both the regulatory body and the utility. The reviewers therefore need to ensure that the principal results are presented clearly and succinctly, in non-specialist language, so that they can be understood accurately and readily by all the expected readers. The reviewers also need to be aware that different groups of PSA analysts, users and reviewers may use somewhat different terminology and concepts and have their own views as to what needs to be included in a PSA, and this must be taken into account when judging the clarity of the presentation of the results.

Since the results of the PSA are heavily dependent on its scope, the principal numerical results are usually accompanied by a statement of the scope, preferably by listing all the possible contributors to risk that have not been included. The reviewers are advised not to accept a plain presentation of, say, the core damage frequency which leaves the reader to find all the qualifications elsewhere in the text of the PSA report.

Operator recovery actions, or accident management measures, generally refer to steps taken when the accident situation has gone beyond the design basis of the plant, sometimes using unqualified equipment. As such they are often regarded, particularly by regulatory bodies, as inspiring a much lower level of confidence than that from the operation of the qualified safety systems. It is then good practice to present the results of the PSA both with and without these recovery actions/accident management measures, although only the results including them need to be put forward as best estimates. Some regulatory bodies insist on the presentation of results without any credit being taken for such actions/measures, while taking a keen interest in the benefit which can be attributed to them in terms of risk reduction.

3.12.1. Review of PSA results

The results of a Level 1 PSA should give a numerical estimate of the CDF and include sufficient information to give insights into identifying the main contributions. These would typically include:

(a) Core damage frequency;
(b) Contribution to the CDF from each of the initiating event groups;

(c) Dominant accident sequences which contribute to the CDF;
(d) Results of sensitivity studies (Section 3.11.1);
(e) Results of uncertainty analyses (Section 3.11.2) giving confidence limits (typically the 5 and 95% bounds) for each of the main results of the PSA;
(f) Importance measures for basic events, safety systems, etc. (Section 3.11.3).

The reviewers should check that the results are presented of sensitivity studies for all contributions of high importance and that all important assumptions, models or data values are stated.

The reviewers need to be satisfied that the global results of the PSA are plausible, the interpretation and conclusions drawn from the results are logical and correct, and the overall objectives of the PSA and the PSA requirements and guidelines are met.

The results of the PSA may be compared with those for similar plants and any differences identified and investigated since this may provide additional help to the reviewers in the identification of potential weaknesses of the PSA.

Where operating experience is available for the actual plant or for similar plants, it is good practice for the reviewers to compare the results of the PSA with what actually happened to ensure that all the event sequences which have actually occurred are modelled in the PSA. In addition, the conclusions of the PSA should be compared with the operating experience of the plant to check consistency. In both cases, these are likely to be redundant checks since past experience is expected to have been incorporated in the PSA.

The reviewers need to check the assumptions made in the PSA carefully. In particular, where relevant experiments have been carried out, the reviewers should compare the experimental results with the assumptions made in the PSA. In addition, where major expert opinions have been formed in previous PSAs, any deviations should be identified and explained.

The reviewers need to check whether the contributions to the risk from issues such as operator error and common cause failures and the benefits from carrying out accident management measures are reasonable in relation to the results from other PSAs.

3.12.2. Use of PSA results

The core damage frequency should be compared with the probabilistic safety goals for the plant (if such goals have been defined).

The results of the PSA are usually used to determine whether there are any weaknesses in the design and operation of the plant. Where such weaknesses are identified, consideration needs to be given to identifying improvements which could be made to reduce the core damage frequency.

The reviewers need to check whether the overall design and operation of the plant is well balanced. Confirmation is required that none of the initiating event groups or accident sequences makes an unduly large contribution to the core damage frequency and that the relative importance of any component or safety system is not unduly large.

Where conclusions have been drawn on the level of safety of the plant, the basis of each conclusion warrants careful review to determine whether it has been derived in a logical way.

It is good practice for the reviewers to seek advice from those experts who are familiar with the plant design and operation about whether the interpretation and conclusions drawn from the PSA results are generally in agreement with their understanding of the plant.

3.13. AUDIT OF PSA QAs

As discussed in Sections 2.2–2.4, it is good practice for the QA procedures used in performing the PSA (including technical procedures) to be reviewed and approved by the regulatory body at an early stage of the PSA (ideally, before actual analysis starts). Whether or not this is done, the regulatory body may conduct audits during the process of PSA development to ensure that the QA procedures are indeed being followed, and that the process for performing the PSA is being properly managed. The frequency of an audit can be determined to meet specific needs. To receive the maximum benefit from the audits, it is important that the first one be carried out at an early stage in the PSA development, so that any deficiencies identified in that audit can be corrected then.

4. REVIEW OF LEVEL 1 PSAs FOR LOW POWER AND SHUTDOWN

This section gives guidance on the technical issues that need to be addressed in carrying out the review of a Level 1 PSA for initiating events occurring during the low power and shutdown modes of operation. This is referred to here as a shutdown PSA (SPSA).

These modes of operation are important since PSAs carried out in recent years have shown that they usually make a significant contribution to the core damage frequency. This arises from the wide range of activities taking place during low power and shutdown conditions, the simultaneous unavailability of safety system equipment, the blocking of automatic actuation of safety systems and the high reliance on

operator actions to restore safety functions. Traditionally, less attention has been given to the design and operation of nuclear power plants for these operational states.

The format of this section follows that of Section 3 for PSAs for full power operation. One additional topic has been added — the identification of the POSs which arise during low power and shutdown conditions.

Much of the guidance given in Section 3 for full power PSAs is also relevant to SPSAs and is not repeated here. This section gives specific additional guidance which is applicable to SPSAs. No additional guidance has been identified for three topics, namely the analysis of passive structures, systems and components, the analysis of computer based systems and the audit of PSA QAs, topics which are not discussed in this section. Hence, this section covers:

- Plant operating states (POSs);
- Identification and grouping of initiating events;
- Accident sequence analysis;
- Systems analysis;
- Analysis of dependent failures;
- Human reliability assessment;
- Data required for the SPSA;
- Analysis of internal and external hazards;
- Quantification of accident sequences;
- Sensitivity analysis, uncertainty analysis and importance analysis;
- Interpretation of the results of the SPSA.

The potential for releases from all the sources of radioactivity in the plant needs to be addressed in the SPSA. These include:

- The reactor core;
- Spent fuel in storage;
- Spent fuel in transit from the reactor core to the storage facilities;
- Radioactive waste in, for example, storage tanks and waste processing facilities.

The accident sequence and systems analyses are usually carried out using a combination of event trees and fault trees. However, the approach is not as well developed for some of the accident sequences addressed in the SPSA as it is for full power operation. Hence, the reviewers need to be aware of developments in modelling techniques.

The SPSA can provide useful insights into:

- Outage planning,
- Plant operations and procedures during outages,

- Technical specifications for low power and shutdown conditions,
- Outage management practices,
- Personnel training,
- Emergency planning and EOPs
- Hardware modifications.

4.1. PLANT OPERATING STATES WHICH ARISE DURING LOW POWER AND SHUTDOWN CONDITIONS

4.1.1. Plant familiarization

The first stage of the review process is information gathering and plant familiarization. As for the full power PSA, the review team needs to interact with the PSA production team and the plant operating and maintenance personnel to become familiar with the plant design, operational features and practices during low power and shutdown conditions and hence ensure that these are modelled accurately in the PSA.

The information gained during the review of the full power PSA should be used in the review of the SPSA. Ideally some or all of the members of the same review team ought to participate in order to take advantage of this experience.

The review team need to become familiar with the design, operation and maintenance of the plant during outages. This information includes the technical specifications applicable to shutdown conditions, maintenance schedules, operating procedures for startup and shutdown, and relevant emergency procedures. In addition, it is important that the reviewers study the available SPSAs that have been performed for plants with similar designs.

4.1.2. Identification of the POSs

During low power and shutdown operation, the plant operational configuration and conditions change significantly. Generally (for plants where refuelling is carried out off-line), there are three different types of outages as follows:

— Regular refuelling outages. During this period, major maintenance activities are also carried out.
— Planned outages where specific maintenance activities are carried out.
— Unplanned but foreseeable outages which follow a disturbance during full power operation.

This is reflected in the plant technical specifications, which are usually divided into several operational modes, each having its own operational requirements.

During these outages, the activities that are being carried out change as do the conditions of the reactor, along with the status of the safety systems and the containment. The aim of the SPSA is to determine how the risk changes with time as these activities take place. In the SPSA, the changes in the way that the plant is being operated are modelled by defining POSs which are stages during the outage during which the activities being carried out, the conditions in the reactor and the status of the safety systems are relatively stable.

The reviewers need to be satisfied that the PSA analysts have carried out a systematic review to identify all the different POSs that could occur during low power and shutdown conditions. These should be consistent with the way that the plant is being operated during low power and shutdown as specified in, for example, the plant technical specifications, operating procedures and maintenance procedures.

Each of the POSs identified needs to be defined fully in terms of:

(a) The *activities being carried out,* which include, for example, refuelling, maintenance and recovery from a reactor trip.
(b) The *conditions in the reactor* such as the reactor power level (for low power)/decay heat level (for shutdown), the reactivity coefficient and the location of the fuel during refuelling.
(c) The *conditions in the primary circuit*, which include the reactor coolant system pressure, temperature and water level, whether the reactor cooling system is intact or has been opened for inspection or refuelling activities to take place and whether loop isolation valves are open or closed.
(d) The *means of decay heat removal*, which include use of the steam generators, the residual heat removal (RHR) system and the fuel pond cooling system.
(e) The *status of the safety systems and the support systems*: for example, which safety systems/number of trains are available to provide protection against initiating events; whether the safety systems will be automatically initiated or manual initiation is required; which support systems/number of trains are available.
(f) The *status of the containment and the containment systems*: for example, whether the containment is open or closed, since this will change during major maintenance and refuelling outages; which of the containment protection systems/number of trains are available.
(g) The *condition of barriers*, since some of the barriers which were claimed for the full power PSA fire and flood analysis may fail or not be present during shutdown; for example, fire doors may be open so that the potential for a fire to spread between areas of the plant during shutdown is different from that during full power operation.
(h) The *duration of the POS*, which is required to understand how the core damage frequency will change with time and to calculate the average risk.

If unplanned but foreseen outages are included within the scope of the SPSA, the definition of the POSs would need to take account of the cause of the outage. For example, if the cause of an outage is due to a system failure, the definition of the corresponding POS should take this into account.

In addition, the set of POSs should include plant shutdown before an anticipated or imminent external hazard such as high winds or flooding from an external source. All such dependences need to identified and included in the definition of the POS.

4.1.3. Grouping of the POSs

In general, a systematic review of the activities carried out during low power and shutdown conditions will identify a large number of POSs and it would not be possible to analyse all of them explicitly in the SPSA. Where POSs have similar characteristics with respect to the plant conditions, the initiating events that could occur and the availability of safety system equipment, it is usual to group them to reduce the amount of analysis required. In addition, SPSAs sometimes do not address all the POSs which have a very short duration — for example, the relatively short duration transient states which occur between two longer duration POSs.

Where the set of POSs has been condensed, the reviewers need to be satisfied that the POSs included in the same group have similar characteristics. Where conservative assumptions are made in the grouping process, this should be done in such a way that it does not bias the results of the PSA.

Where POSs have not been addressed explicitly, the reason for not including them needs to be fully documented and any judgements made fully justified. This should provide assurance that the applications for which the SPSA will be used do not require the POSs which have been screened out.

The reviewers need to be satisfied that the set of POSs identified for analysis include all the different modes of operation of the plant which are not covered in the PSA for full power operation.

The reviewers should also be satisfied that POSs have been defined which address spent fuel transfer and storage, and the activities involving radioactive waste.

4.2. INITIATING EVENTS

4.2.1. Identification of initiating events

A wide variety of accident sequences and consequences are considered in SPSAs, including:

- Loss of decay heat removal from the reactor core,
- Loss of decay heat removal from one or more fuel elements during fuel handling and storage,
- Loss of containment for parts of the plant containing radioactive material,
- Mechanical damage to fuel during fuel handling or from a dropped load,
- Inadvertent criticality events during fuel handling/storage or in the radioactive waste handling systems,
- An increase in radiation levels due to incidents during refuelling.

The reviewers need to be satisfied that the set of initiating events identified covers all the consequences included within the scope of the SPSA that could arise during low power and shutdown conditions.

The types of initiating events that can occur during low power and shutdown conditions include the following:

(a) *Events threatening normal heat removal* including intrinsic failures in the operating decay heat removal system or in the support systems;
(b) *Events causing a loss of primary circuit inventory* due to pipe breaks in the reactor coolant system, draindown events caused by maintenance errors and other failures affecting the primary circuit boundary;
(c) *Events threatening primary circuit integrity* including inadvertent actuation of high pressure safety injection during cold states;
(d) *Events affecting reactivity control* including a decrease in the primary circuit boron concentration, an ingress of clean condensate into the reactor coolant system and control rod ejection or withdrawal.

The reviewers need to be satisfied that all the initiating events which could occur during each of the POSs have been identified. This should be done using a systematic procedure such as that described in Section 3.1.1 for Level 1 PSAs. The set of initiating events identified for the SPSA should be as complete as possible (within the agreed scope and applications of the PSA (Section 2.3.3)) and consistent with those included in the PSA for power operation. This would include internal initiating events, and internal and external hazards as appropriate.

It is advisable that a comparison be made with the SPSAs for similar plants and a survey of operating experience be carried out to ensure that any relevant initiating events have not been missed.

The set of initiating events identified needs to include operator initiated events, since previous PSAs have found them to be particularly important during low power and shutdown conditions. Examples of these are:

(1) When the reactor coolant system is being drained to midloop level to allow steam generator tube inspection, an operator error could lead to overdrainage,

cavitation affecting the pumps in the RHR system and a consequent loss of decay heat removal from the core (in PWRs).

(2) Valves may be incorrectly positioned during maintenance so that a drain path is established from any fluid system.

(3) Operator errors could occur during filling of the reactor vessel and during the maintenance of main circulation pumps or control rod drives located underneath the reactor vessel (in BWRs).

4.2.2. Grouping and screening of initiating events

In general for an SPSA, a large number of POS/initiating event combinations are identified so that a grouping and screening process is required to reduce the analysis to a manageable size. This is done in much the same way as for full power Level 1 PSAs (Section 3.1.2). Each initiating event group is then analysed using a single event tree/fault tree model.

Within a POS, the grouping criteria used need to ensure that the initiating events included in the group are similar with respect to:

(a) The effect of the initiating event on the availability and operation of safety systems and support systems,

(b) The demands made on the safety systems and support systems (success criteria),

(c) The expected response from the operators,

(d) The consequences that could arise from the initiating event.

Some examples of initiating event groups which have been defined in previous SPSAs are as follows:

(1) Loss of residual heat removal;

(2) Loss of support systems;

(3) Pipe break LOCAs;

(4) Maintenance induced LOCAs (either into the containment or into the interfacing systems);

(5) Loss of on- and off-site electrical systems;

(6) Challenges to primary circuit integrity, for example, cold overpressurization and secondary side events leading to thermal transients;

(7) Reactivity events, for example, boron dilution and return-to-criticality events;

(8) Local criticality events, for example, refuelling errors or errors in fuel handling;

(9) Area events, for example, internal fires and flooding;

(10) External hazards, for example, high winds, earthquakes, aircraft crashes;

(11) Drop loads, for the additional loads which are lifted during shutdown conditions.

The reviewers should be satisfied that the initiating events which are grouped together all lead to the same accident progression, and make the same demands on the safety systems and the operators.

As for the full power PSA, the characteristics of the initiating event group need to be defined on the basis of the most restrictive initiating event(s) within the group. However, care needs to be taken in the grouping process such that it does not unduly bias the results of the SPSA.

4.3. ACCIDENT SEQUENCE MODELLING

As for the full power PSA, the next step in the analysis is to model the response of the plant during each of the POS/initiating event groups identified. This is done by identifying the safety functions that need to be carried out, defining the success criteria for the systems that perform these safety functions, carrying out an event tree analysis to identify the accident sequences that could occur following success or failure of the safety systems and grouping the end point of the event trees into plant damage states.

4.3.1. Success criteria

The reviewers need to check that the PSA analysts have defined the consequences that are addressed in the event sequence analysis. For initiating event groups which lead to a loss of decay heat removal from the reactor core, the criterion used for core damage needs to be consistent with that used for the full power PSA. However, additional criteria will have to be defined for, for example, initiating events which lead to a loss of decay heat removal from spent fuel in transit or storage, an inadvertent criticality and a release from systems which handle or store radioactive waste.

As for the full power PSA, the safety functions that have to be performed to prevent these adverse consequences occurring after an initiating event should be identified, the safety systems which are available to perform these safety functions should be identified and the minimum level of performance required from the safety systems (success criteria) should be defined. The safety functions required for an intact core are the same as those identified for the full power PSA, although the success criteria might be different depending on the decay heat level.

This is a more difficult task for the SPSA than for the full power PSA due to the different types of event sequences and consequences that could occur. The reviewers need to be satisfied that a systematic approach has been followed which gives confidence that all the required safety functions have been identified and the associated safety system success criteria defined.

The reviewers should be satisfied that sufficient analysis has been carried out to provide justification for all the success criteria used in the SPSA. Thermohydraulic criticality or other types of analysis will be required. In practice, this will range from detailed analysis with integrated thermohydraulic models for success criteria relating to decay heat removal at low power to relatively simple calculations to determine boil-off rates from the spent fuel storage pool. Best estimate models, assumptions and data need to be used whenever possible.

For any of the POSs which have a long duration, the decay heat level may change and this in turn might change the safety system success criteria and provide a longer timescale for operator actions to be carried out. If a POS has been subdivided to take account of the reducing decay heat level, additional event sequence analysis needs to be carried out and the appropriate transient analysis made to provide a justification for the different success criteria used.

4.3.2. Event sequence analysis

The reviewers need to be satisfied that the methods used for the event sequence analysis are acceptable. The basic approach used in the SPSAs carried out to date for initiating events affecting an intact reactor core is usually very similar to that used for the full power PSA, i.e. a logical model is constructed using event trees and/or fault trees.

These are usually based on the full power PSA models with appropriate revisions to reflect the different plant availabilities and success criteria; for example, the headings relating to reactor trip can be removed if the reactor is already shut down and those relating to the operation of particular safety systems can be removed if they are not available during the POS. Event tree headings can also be added where additional operator actions are required — for example, where automatic initiation has been disabled and manual initiation is required. However, although the logical model is very similar, the conditional probabilities at the branch points may be very different.

For the POSs in the middle of the outage, the behaviour of the reactor may be completely different, for example, when the reactor coolant system is at midloop level or is open. In this case, completely new event trees need to be drawn. The reviewers have to pay careful attention to these POSs and check that the thermohydraulic behaviour has been properly understood.

Additional models will need to be developed for the sequences which address the other consequences included in the SPSA, for example, the parts of the analysis that relate to releases for sources of radioactivity other than from fuel in the reactor core. It needs to be recognized that the methods for carrying out this part of the SPSA are less well developed than for those leading to core damage and the reviewers need to ensure that any developments in the methods used are acceptable.

In each case, the event sequence analysis needs to address all the safety systems and operator actions that are required for each of the POSs/initiating event groups/consequences identified.

4.3.3. Plant damage states

The event sequences identified in an SPSA need to be grouped into PDSs. For accident sequences which lead to core damage, the set of PDSs identified for the full power PSA (Section 3.2.3) will need to be supplemented by additional ones which represent the conditions which are unique to shutdown and refuelling. This includes states where the reactor vessel head has been removed or the RCS is open for inspection.

In addition, PDSs will need to be defined for the other types of event sequences identified in the analysis, i.e., those which lead to releases of radioactivity from spent fuel in transit or storage and from radioactive waste systems.

The reviewers need to check that an adequate set of additional PDSs have been defined and that they are consistent with those already identified.

4.4. SYSTEMS ANALYSIS

As in a full power PSA, a systems analysis is usually carried out using fault trees so that the guidance given in Section 3.3 is applicable. The starting point for the development of the fault trees included in SPSAs will be those developed in full power PSAs. However, there are a number of differences as follows:

(a) The safety system success criteria may be different.
(b) The safety systems may be in operation rather than on standby, for example, the RHR system (for PWRs).
(c) The safety systems may need to be initiated manually rather than automatically — this is the case for the high head safety injection (HHSI) system, where the automatic start is disabled during shutdown to prevent cold overpressurization of the reactor coolant system (for PWRs).
(d) The level of redundancy may be lower since some of the trains of the safety systems may have been removed from service.
(e) The possible modes of operation of the safety systems may be different, for example, some of the modes of the system involving cross-connections may not be available during maintenance activities.
(f) The required mission times may be significantly different.

Also, additional fault trees will need to be developed since some safety systems are not modelled in the full power PSA, for example, the cooling systems provided

for spent fuel in transit or storage. For that case the fault trees used in SPSA have been developed from those used in full power PSA, and the reviewers have to be satisfied that a systematic approach has been used to identify all the features of the POS that would affect the reliability of the safety system and that the necessary changes have been made to the fault trees.

4.5. ANALYSIS OF DEPENDENT FAILURES

The guidance given in Section 3.4 on the types of dependent failures that can occur and how they need to be addressed in a PSA is also relevant here. However, it needs to be recognized that the dependences that are identified in an SPSA are likely to be different from those identified in a full power PSA.

The reviewers should be satisfied that a systematic analysis has been carried out to identify all the dependences that could influence the way that event sequences develop and affect the reliability of safety systems. This is particularly important for an SPSA since the maintenance, testing and other activities being carried out and the relatively high reliance on operator actions have the potential to introduce more dependences than would be identified in a full power PSA.

A justification needs to be provided that all the dependences have been identified. This information is usually presented in the form of a dependence matrix, which is useful for grouping POSs and initiating events, checking system availabilities and supporting the event and fault tree models.

The common cause failure probabilities used in the SPSA will need to be reviewed carefully. The numerical values are likely to be different from those used in the full power PSA since maintenance, testing and other activities could introduce additional mechanisms which would affect the potential for a common cause failure to occur.

4.6. HUMAN RELIABILITY ASSESSMENT

The guidance given in Section 3.6 for reviewing the HRA and the associated HEPs included in the full power PSA is also applicable to SPSAs.

Before starting the review, the reviewers should liaise with plant operating and maintenance personnel to become familiar with the way that outage and maintenance activities are carried out during low power and shutdown conditions. This will allow the reviewers to form a view on whether the HRA models adequately reflect the conditions in the plant.

The reviewers have to be satisfied that the HRA has been carried out in a structured and logical manner. This is particularly important since the level of activity at the plant is very much higher during shutdown conditions than during full power operation. The HRA needs to be well documented so that the process used for modelling human errors in the event/fault trees can be well traced.

Regarding the three types of human interactions identified in Section 3.6.2, the grouping for the SPSAs is as follows:

Type A (occurring before the initiating event): although the basic approach to modelling human errors is the same as for the full power PSAs, the numerical values of some of the HEPs may be different.

Type B (causing an initiating event): these human errors are again assumed to be included in the initiating event frequencies which are derived from operating experience and hence are not usually addressed explicitly.

Type C (following an initiating event): these human errors are particularly important during shutdown due to the factors identified below. They have tended to be dominant contributors to core damage frequency in most SPSA studies performed to date, so that a realistic assessment of these HEPs will be required.

In estimating the HEPs to be included in the SPSA, the following negative factors need to be considered:

(1) The higher levels of activity in the plant;
(2) The increased difficulty in diagnosing initiating events that have occurred and carrying out the appropriate recovery actions;
(3) The change from automatic to manual actuation for some of the safety systems;
(4) The use of external contractors to carry out much of the maintenance work;
(5) The higher workload and longer working hours during this period;
(6) The procedures often being less detailed than those for full power operation since there are a large number of POSs that could occur during shutdown;
(7) The operators often being less well trained to deal with accidents occurring during shutdown than those during full power operation;

along with the following positive factor:

(8) The timescale available for operator actions to be carried out being longer than that for the equivalent accident sequence occurring during full power operation due to the lower decay heat level.

The HRA needs to take account of these factors in a systematic manner in deriving the HEPs used in the SPSA. This is usually done using the same methods as those for full power PSAs (Section 3.6.3). However, where there are long timescales available for operator actions to be carried out, caution needs to be exercised in applying the time–reliability correlations used in a full power PSA since the timescales available during shutdown conditions are often well outside the range in which these correlations are applicable.

Owing to the complexity of the HRA model included in the SPSA, it is necessary that the initial quantification of the SPSA use conservative screening values for the HEPs and this analysis be reported. This allows the more important operator errors to be identified so that the review can focus on them.

The HRA model needs to take account of the dependences which occur between operator actions. It is common practice to assume that there is a high degree of dependence between successive operator actions unless they are carried out by different individuals or are well separated in time and location.

4.7. DATA REQUIRED FOR THE SHUTDOWN PSA

This section gives guidance on reviews of the data required for SPSAs which is additional to that given in Section 3.3.

4.7.1. Initiating event frequencies

The initiating event frequencies used in SPSAs are either derived from operating experience from similar plants that is in turn derived from the initiating event frequencies used in full power PSAs, with factors applied to take account of the different conditions during shutdown, or calculated using a mathematical model which includes all the ways that the initiating event can occur. In each case, a justification needs to be provided that the initiating frequency is applicable.

The initiating event frequencies can be specified in two ways depending on the aim of the SPSA:

(a) If the aim is simply to estimate the contribution to the average core damage frequency which would arise during each of the POSs, the initiating event frequency used would be the annual average frequency multiplied by the fraction of time that the POS exists.
(b) If the aim is to estimate the point-in-time core damage frequency during the POS, the annual frequency is used.

In each case, the frequency is specified on a per year basis. In the first case the contributions to the CDF from each of the POSs can be added together to obtain the total contribution to the CDF from low power and shutdown POSs. In the second case, the results of the SPSA can be used to plot how the core damage frequency changes with time as the plant proceeds through the various POSs (which is equivalent to what would be plotted on a risk monitor). The latter approach is preferred since it allows the reviewers to determine whether there are very high peaks in the risk. The occurrence of such peaks in the risk even for very short periods of time may be undesirable even if the average risk is acceptable.

The initiating event frequencies need to be consistent with those used in the full power PSA and with operating experience data. However, this needs to take into account differences in the design and operation of the set of plants from which the data were obtained and reflect the different plant alignments which occur during shutdown conditions.

Where the initiating event frequencies from the full power PSA are modified for use in the SPSA, the reviewers should be satisfied that this takes account of:

(1) Differences in physical conditions, for example, the lower pressures and temperatures in the reactor coolant system during shutdown, which may affect the frequency of pipe break LOCAs;
(2) Operator errors during maintenance which may affect the frequency rate of fluid systems being inadvertently drained due to incorrect valve alignments;
(3) Overdrainage of the reactor coolant system — this can occur due to human errors during periods when the RCS is at midloop level.

Where modelling techniques are used to derive initiating event frequencies, the reviewers need to be satisfied that all possible causes of the initiating event have been included in the analysis.

4.7.2. Component failure rates

The component failure rate data used in SPSAs should be applicable to shutdown conditions. However, since such data are generally not available, the component failure rates used are the same as those in the full power PSA and reasons need to be given for their applicability.

The reviewers should be satisfied that the component failure rates used in the SPSA and in particular the POSs reflect low power and shutdown conditions and the maintenance activities that are being carried out.

4.8. ANALYSIS OF INTERNAL AND EXTERNAL HAZARDS

The guidance given in Section 3.9 is applicable to the review of the analysis of internal and external hazards included in SPSAs. Some additional guidance is given below for internal fires, internal flooding and dropped loads.

The analysis needs to focus on all the structures, systems and components which are in a different condition than during full power.

4.8.1. Internal fires

SPSAs for internal fires need to take account of the fact that the initiating event frequencies may be increased (e.g. owing to welding operations being carried out),

additional inventories of combustible materials may be introduced into some areas of the plant, automatic fire suppression systems may not be available and some of the fire barriers may not be fully effective (e.g. fire barriers may have been removed, fire doors left open or penetration seals removed).

Where possible, it is necessary that the reviewers carry out a plant walk-through to determine the status of the fire protection systems during a representative subset of the POSs to ensure that this is accurately reflected in the SPSA.

4.8.2. Internal flooding

The SPSA should take account of the following:

(a) Sources of internal flooding may be different from those during full power operation, for example, water systems which are pressurized during power operation may be depressurized during shutdown; temporary water systems and hose connections may be in use.
(b) Initiating event frequencies may be increased, for example, owing to incorrect valve alignments leading to flooding.
(c) Flood protection features may be defeated, for example, there is an increased potential for drainage systems to become blocked due to debris which has accumulated during maintenance activities, doors in segregation barriers may be left open and penetration seals may be removed.

As for internal fire, the reviewers need to carry out a plant walk-through to identify the potential for internal flooding to occur and determine the status of the flood protection systems during a representative subset of the POSs to ensure that these are accurately reflected in the SPSA.

4.8.3. Dropped loads

There are a relatively large number of heavy loads lifted during maintenance outages and hence there is an increased potential for dropped loads to occur. In addition, there is the potential for dropped loads to directly affect spent fuel when the core is open during refuelling or in the fuel storage pond.

The reviewers should be satisfied that all the loads that are lifted during the various POSs have been identified and that a schedule of loads has been drawn up. This would typically include the reactor pressure vessel head internals, spent fuel flasks and large components such as pumps and shielding blocks.

The reviewers need to be satisfied that an analysis has been carried out to determine the potential for dropped loads to occur which could lead to initiating events, failure of safety systems, damage to spent fuel elements during refuelling and fuel storage, or release of radioactive waste. The analysis should provide a good

justification for the frequency with which loads would be dropped onto critical areas of the plant.

4.9. QUANTIFICATION OF ANALYSES

Accident sequence quantification, sensitivity studies, uncertainty analyses and importance analyses are usually carried out using the same techniques as those for full power PSAs (Sections 3.10 and 3.11) and the reviewers need to be satisfied that they are carried out in an acceptable way.

The main difference for SPSAs compared with full power PSAs is the more significant role that sensitivity studies play for them. The set of sensitivity studies carried out needs to address:

(a) The choice of the bounding conditions used to characterize the POSs,
(b) The assumptions made regarding the availability of safety system equipment,
(c) The effects of or changes in the way that maintenance activities are scheduled,
(d) The duration of the POSs,
(e) The way that the success criteria vary with the decay heat level.

The reviewers should be satisfied that an adequate range of sensitivity studies have been carried out for addressing all the above issues.

4.10. INTERPRETATION OF THE RESULTS OF SHUTDOWN PSAs

The requirements for the presentation of the results of SPSAs are the same as those given in Section 3.12. The results should be presented for each of the POSs addressed in the analysis. It is advisable that the results present a risk profile for a typical outage schedule.

The reviewers need to consider the results of the PSA to determine whether there is a need for any safety improvements to be made. Possible areas of improvement which have been identified in previous SPSAs include:

(a) Improvements in outage planning and maintenance scheduling to reduce the level of unavailability of safety systems during particular POSs;
(b) Development of more detailed operating, maintenance and accident procedures;
(c) Modifications to the plant technical specifications;
(d) Hardware modifications;
(e) Improvements in the training of personnel;
(f) Improvements in management practices.

The reviewers are advised to encourage use of the SPSA during the preparation of an outage plan and during the actual outage to help to optimize it. In particular, this optimization should determine whether it is better to carry out some maintenance or test activities under power or during shutdown and whether certain tests should be performed simultaneously or sequentially.

The reviewers need to use the results of the SPSA to identify the critical operator actions and determine what can be done to reduce the likelihood of errors occurring. One of the areas where this has happened is drainage of reactor coolant systems to midloop level for steam generator tube inspection in a PWR. The likelihood of an error occurring which would lead to overdrainage of the primary circuit has been reduced by a variety of methods including:

(1) Provision of a better method of indicating the water level in the primary circuit to the operators;
(2) Provision of additional sources of makeup water (which, for some plants, is initiated automatically at low reactor coolant system levels);
(3) Limitations on carrying out activities that could affect primary circuit integrity during midloop conditions;
(4) Inclusion of procedural steps to prevent fast or slow boron dilution accidents during shutdown conditions.

5. REVIEW OF LEVEL 2 PSAs

This section provides guidance on the technical issues that need to be addressed in carrying out the review of a Level 2 PSA. These include:

- Familiarization with plant data and systems,
- Level 1–Level 2 PSA interface,
- Accident progression modelling,
- Containment performance analysis,
- Probabilistic modelling framework,
- Quantification of containment event trees,
- Characterization of the radiological source terms,
- Results of Level 2 PSAs,
- Audit of Level 2 PSA QAs.

Many of the examples used in this section are based on the experience gained from reviewing Level 2 PSAs for nuclear power plants with PWRs.

5.1. FAMILIARIZATION WITH PLANT DATA AND SYSTEMS

The first task is for the reviewers to become familiar with the design and operation of the plant and with the way that it would respond to the phenomena that could occur during a severe accident.

The reviewers need to become familiar with:

(a) The design and operation of the systems which may be initiated during a severe accident to mitigate its consequences;
(b) The important plant and containment characteristics which may provide insights on accident progression and potential vulnerabilities.

5.1.1. Familiarization with the systems which may be operated during a severe accident

The reviewers need to understand the function and operation/actuation of plant systems. The information required to do this includes:

(a) Design documentation for the safety systems and the containment systems;
(b) System capacity, operating limits and actuation criteria;
(c) The support systems required for operation.

Some of this information may already be available in the Level 1 PSA documents.

The systems which are relevant to the severe accident consequences are:

Reactivity control systems

— boration systems;
— moderator systems (for Canadian deuterium–uranium (CANDU) reactors).

Core cooling systems

— all high and low pressure ECCSs;
— accumulators (for PWRs);
— long term reactor heat removal systems;
— alternative reactor pressure vessel (RPV) injection systems.

Containment systems

— containment isolation systems;
— systems whose failure could lead to containment bypass (interfaces between high and low pressure systems, letdown lines) (for PWRs);
— containment sprays;

— containment fan coolers;
— hydrogen control systems;
— long term containment heat removal systems;
— filtered containment venting systems;
— alternative containment injection systems;
— reactor building ventilation systems (for BWRs).

Other systems

— reactor coolant system (RCS) depressurization systems.

A thorough review of the containment isolation system, and of other systems with a potential for containment bypass, is needed.

If containment systems analysis is part of the Level 2 PSA, the procedures for the review are the same as those described in Ref. [9]. Systems dependences are of paramount importance. For instance, analysis of the containment isolation system is normally not part of a Level 1 study. This system is dependent on the availability of power sources (AC and/or DC), thus these dependences must be clearly identified in the review. The same is true of the active hydrogen control systems, of the venting system and of the containment cooling systems.

Level 2 PSAs may model post-core damage operator interventions to mitigate the consequences of a severe accident, see Ref. [1]. In addition, systems may be automatically initiated if physical conditions change during the progression of an accident after core damage. For example, the ECCS may be actuated when available, if during a high pressure transient some mechanism causes depressurization of the primary system. Therefore, the EOPs must also be checked to understand the operator response in the course of a severe accident, before and after core damage, and the potential for interventions using available systems after core damage. The degree to which these procedures are supported by training and exercises is important in assessing the probability that they may be carried out successfully.

5.1.2. Plant and containment data

A useful way for a review team to develop a general understanding of the plant characteristics is for them to compare key design and operating parameters for the plant being analysed with those of plants of similar design and configuration. This information can also suggest ‘typical’ severe accident vulnerabilities that need to be addressed in the Level 2 PSA [1, 9]. Collecting and evaluating the data for key plant and containment design features is, therefore, a critical part of the review process.

The plant and containment features which could influence the progression of a severe accident include:

Reactor

- Reactor type;
- Power level;
- Reactor power/RCS volume ratio (related to accident progression times and recovery opportunities);
- Fuel type (metal, oxide or mixed oxide fuel);
- Cladding type and mix (zirconium or stainless steel cladding, related to peak core temperatures, melting characteristics, hydrogen generation rates and concrete interaction behaviour);
- Mass of fuel (total energy content of core);
- Mass of cladding material (indicator of maximum hydrogen production);
- Control rod materials and mass (low temperature melting material).

Reactor coolant system

- RCS coolant/moderator volume;
- Number and coolant volume of accumulators;
- Mass of coolant available and maximum pressure for ECCS.

Containment

- Containment free volume (potential for non-condensable gas buildup and hydrogen concentration);
- Containment pressure/temperature design values (capacity to withstand quasi-static loads);
- Containment structure (steel shell, concrete, e.g., suggest appropriate failure modes);
- Suppression pool volume (for BWRs);
- Suppression tower (for WWERs);
- Concrete composition (non-condensable gas generation after vessel failure);
- Cavity/pedestal design (suggests potential for debris dispersal during high pressure sequences and ex-vessel debris–structure interactions during low pressure sequences);
- Sump volume and location (for PWRs) (possibility of degraded recirculation cooling due to clogging with debris);
- Containment geometry (the extent of compartmentalization suggests the potential for local combustible gas accumulation).

No amount of data or drawings can substitute for the reviewers actually seeing the systems being analysed. Hence it is important for the reviewers to carry out a plant walk-through of the containment and key plant systems.

5.2. INTERFACE BETWEEN LEVEL 1 AND LEVEL 2 PSAs

5.2.1. Plant damage states

The interface between a Level 1 PSA and a Level 2 PSA is usually accomplished by defining PDSs which give the initial conditions and the boundary conditions for severe accident analysis.

This may be done as part of the Level 1 PSA or as the initial step of the Level 2 PSA. The discussion given in Section 3 is extended to include the containment systems which are usually beyond the scope of the Level 1 PSA so that the status of these systems may not be identifiable from the Level 1 PSA models. In this case, the availability of containment systems during various core damage sequences must be addressed by means of an extension to the Level 1 PSA system models. In some Level 2 PSAs, post-core-damage operator interventions are also identified in the definition of the PDSs, as explained below.

5.2.2. PDS grouping

The objective of PDS analysis is to combine event sequences from the Level 1 PSA that result in similar severe accident progression, present similar challenges to the containment and have the same potential for fission product release to the environment. By doing so, the number of unique accident conditions that need to be considered in the Level 2 PSA is greatly reduced. For example, a Level 1 PSA would typically use different event trees to model core damage following a spurious reactor trip versus the loss of feedwater. However, from the point of view of containment response, grouping of sequences from these two event trees may be similar and might be combined for Level 2 PSAs. It is worth noting that, in some cases, Level 1 PSA sequences may be split between different PDSs (rather than combined), since information such as that related to containment system operation may not have been important from a Level 1 PSA point of view and thus was not included in the Level 1 event trees.

To accomplish the PDS grouping, the Level 1 results are sorted according to the physical states of the plant systems that were required prior to the onset of core damage and the availability of systems that could be actuated subsequent to core damage, thereby terminating the accident or mitigating its consequences. The reviewers should be satisfied that the criteria used to combine similar core damage sequences ensure that the plant characteristics governing severe accident progression, containment response and fission product release to the environment are properly accounted for.

Typical grouping criteria, used, for example, for light water reactors, include:

- The type of initiating event that has occurred (intact primary circuit or LOCA);

- The status of the safety systems, such as those of the reactor protection system, the residual heat removal system and the emergency core cooling system (injection and/or recirculation);
- The availability of AC and DC power;
- The primary circuit pressure (high or low) at the time of core damage;
- The status of the RCS pressure reduction systems (the automatic depressurization system for BWRs and the PORV for PWRs);
- The time at which core damage occurs (early or late relative to the time of reactor scram);
- The integrity of the containment (intact, failed, isolation failure or bypassed due to steam generator tube rupture (SGTR) or an interfacing systems LOCA);
- Suppression systems status when core damage occurs;
- The availability of the containment protection systems (containment sprays, heat removal systems and hydrogen mixing/recombiners/ignitors).

For many accident sequences, the status of particular systems may not be known directly from Level 1 PSA system models. For example, the large break LOCA success criteria may require at least one of the (PWR) accumulators to function to prevent core damage. For event sequences involving failure of all the accumulators, the Level 1 PSA accident sequence event trees would not need to include the operation of other ECCS systems, and the next step in the sequence would be core damage. However, in the Level 2 analysis it would need to be known whether high and/or low pressure coolant injection systems were available during the sequence. Determining the status of such systems and other systems not covered in the normal Level 1 PSA requires an extension of the Level 1 PSA models. The reviewers should be satisfied that the Level 1 PSA models have been extended to include the status of systems not fully modelled in the Level 1 PSA which are important in the Level 2 PSA and thus included in the PDS definitions.

The EOPs for many plants include operator actions to be carried out when it is expected that the accident conditions are irreversible and that core damage will very likely occur within a short period of time. These include actions such as RCS depressurization and hydrogen control which are not normally modelled in Level 1 PSAs.

The reviewers need to determine the extent to which the actions given in the EOPs which equate to accident management have been included in the Level 1 PSA and ensure that this is carried forward to the Level 2 PSA.

The accident management measures which may be defined after core damage could include:

— primary system depressurization,
— initiation of alternate core injection systems,
— flooding the containment,

— flooding the reactor cavity/pedestal,
— venting the containment,
— venting the reactor pressure vessel (for BWRs),
— refilling the steam generators (for PWRs),
— actuation of the hydrogen control systems,
— actuation of containment sprays from alternate injection systems.

Therefore, the interface between Level 1 and Level 2 may include more information than is shown in the list of grouping criteria. For instance, including the primary system pressure before vessel breach rather than at the onset of core damage might be more appropriate when post-core-damage operator actions have been incorporated in the analysis.

5.2.3. PDS analysis and quantification

The systems availability aspect of the PDS definitions can be addressed in a number of ways:

(a) By extending the Level 1 event trees to include top events which address the availability of the containment systems, so that their system fault trees can be linked and dependences accounted for in the evaluation,
(b) By modelling all the systems not already modelled in the CETs, although care is then needed to ensure that the correlations with the Level 1 sequences, such as dependences on common support systems, are maintained;
(c) By using a separate computer program which takes the cut set equation information from the Level 1 event trees, links in the fault trees for the containment systems and, if appropriate, for the accident management systems, and acts essentially as an extension to the Level 1 PSA — known as bridge trees.

Such a program can also be written to group the sequences according to all of the characteristics in the definitions of the PDSs, with, for example, input of the appropriate information on timing and pressure, giving the frequency of each PDS as output, ready for the Level 2 analysis.

The reviewers need to be satisfied that the assumptions, simplifications and dependences have been clearly identified and justified.

For bridge trees that include fault trees of systems not included in the Level 1 PSA, the system reliability models need to be reviewed as described in Section 3.

5.2.4. Human reliability assessment related to PDSs

Where the PDS frequencies include operator actions after the onset of core damage, the reviewers need to be satisfied that the way that these HEPs have been

addressed is acceptable. In particular, the evaluation of the post-core-damage HEPs has taken account of prior human performance and dependences, the levels of stress for personnel and the uncertainties in the availability of reliable indications and signals in a severe accident environment.

The review of Level 2 HRAs should be carried out according to the guidelines presented in Ref. [15] and special attention should be paid to the following:

Staffing: A crisis team, separate from the control room staff, is usually set up which is responsible for decision making, and this needs to be taken into account in the HRA. The reviewers should be satisfied that the roles and responsibilities of the crisis team have been adequately defined and their interaction with off-site support services such as the fire brigade has been established.

Decision making: Uncertainties increase when shifting from Level 1 PSA to Level 2 PSA scenarios. This is a particular concern for the decision making process where less explicit decision rules, such as if <pattern of indications> then <action required>, are available — see Ref. [7]. However, the HRA needs to refer to procedural rules or to trained rules that support the decisions regarding accident management. The quantification of decision making in Level 2 PSA scenarios is difficult since there are limitations in the current HEP assessment techniques. It is expected therefore that the HRA carries out the quantification with a reasonable amount of conservatism.

Severe plant conditions: Level 2 HEPs need to account for severe plant conditions. The reviewers need to be satisfied that the following have been taken into account:

- Dependences from preceding (Level 1 PSA) human errors,
- Existing equipment failures that may disable a Level 2 PSA action,
- Difficulties in accessing the locations where accident management actions are to be carried out,
- A higher level of stress and workload.

5.2.5. PDS analysis results

The reviewers have to be satisfied that all the core damage sequences have been assigned to a PDS and that the sum of the PDS frequencies is approximately equal to the total core damage frequency.

In some PSAs, core damage sequences (or minimal cut sets) with very low frequencies are ignored in the PDS grouping process. If a cut-off frequency is applied, the reviewers need to check that:

(a) The total frequency of event sequences below the cut-off value is a small fraction of the total core damage frequency (less than, say, 1%);
(b) Those accident sequences that could potentially have major consequences have not been systematically screened out, for example, those where the containment has failed or is bypassed.

5.3. ACCIDENT PROGRESSION MODELLING

5.3.1. Accident progression models

Deterministic analysis of reactor and containment behaviour during postulated accident sequences represents the principal basis for phenomenological event quantification in a Level 2 PSA. Such analyses provide a plant specific technical basis for distinguishing the phenomenological event branch probabilities. The probabilistic framework of a Level 2 PSA (discussed in Section 5.5) is the mechanism for delineating and quantifying uncertainties in deterministic severe accident analyses. This section outlines various features of deterministic accident progression models that need to be examined in the course of a Level 2 PSA review.

5.3.2. Computer codes used to perform accident progression analysis

The accident progression analysis needs to cover all aspects of the process, including:

(a) Reactor coolant system thermohydraulic response (prior to the onset of core damage);
(b) Core heat-up, fuel degradation and material relocation within the reactor vessel;
(c) Failure of the reactor vessel pressure boundary, and the subsequent release of molten fuel and core debris to the containment;
(d) Thermal and chemical interactions between core debris and containment structures, such as concrete (or steel) floors and walls, pools of water and the containment atmosphere;
(e) Containment behaviour (including its pressure/temperature history, hydrogen mixing and combustion, and the effect of the operation of containment safeguard systems).

This can be done by a single integrated severe accident analysis computer code such as MAAP [37], MELCOR [38], ESCADRE [39] or THALES-2 [40]. These codes provide an integrated framework for evaluating the timing of key accident

events, thermodynamic histories of the reactor coolant system, core and containment, and corresponding estimates of fission product release and transport. However, the broad scope of these codes (and the requirement that calculations made with them be completed in a reasonably short time) requires simplifications in many aspects of the accident progression models used. Examples of these simplifications include lumped parameter approximations to material transport and thermodynamic conservation equations and the use of empirical correlations for complex physical processes. The reviewers should be aware of the areas in which these simplifications are made, and determine whether their effects are taken into account in the Level 2 PSA. The manner in which these effects (and other modelling uncertainties) are considered is addressed in more detail in Section 5.6.

Calculations with these integrated computer codes are often replaced by, or supplemented with, calculations performed with other computer codes that address specific aspects of severe accident progression. Examples of such computer codes and the phenomena that they model are listed in Ref. [5]. In general, the narrower scope of these codes allows important accident phenomena to be modelled in a greater level of detail than is afforded by integrated computer codes. The reviewers need to take note of the specific areas in which these codes are used and determine whether results obtained with them are used in conjunction with, or in place of, those obtained from integrated code calculations.

5.3.3. Treatment of important accident phenomena

The reviewers should be satisfied that important accident phenomena have been addressed by plant specific analysis (included, e.g., as an element of computer code calculations) or by applying information from other credible and relevant sources such as experimental data or published 'reference' plant analysis. The accident phenomena are given in the Appendix.

The reviewers should be satisfied that all the relevant accident phenomena have been addressed in the analysis. For each of the phenomena, the reviewers need to be able to identify the model, computer code or data source used to address it.

If published data from experiments or reference plant analysis are used to evaluate certain phenomena, the reviewers should be satisfied that the information is relevant to the plant being studied. If plant specific analysis is performed using one of the severe accident computer codes referred to above, the reviewers should be satisfied that the data used to perform the calculations have been checked as described in the next section.

5.3.4. Model input data

A large number of input data from different sources are required for a severe accident analysis, details of which are given below.

5.3.4.1. Plant specific data used to represent a plant

This type of information includes:

- The total volume of water in the RCS and the secondary side of the steam generators,
- The volumes of various compartments in containment and the means by which they are connected to each other,
- The type of concrete used to construct the containment.

The reviewers need to be satisfied that the basic data used to define the configuration, geometry and material composition of the plant have been defined and used appropriately in the models representing the plant. This information should be verified by comparison with plant design documents.

The reviewers need to check that thorough documentation and independent verification of this type of information is provided in the quality assurance documents associated with the Level 2 PSA. If such documentation is not available, the reviewers should carry out a spot check of the values of key parameters covering various portions of the plant model and compare them with those in plant design documents.

5.3.4.2. Plant modelling structure (spatial nodalization schemes)

The level of detail used to develop a nodal thermodynamic model (i.e. lumped parameter control volumes) should be examined. This review needs to include RCS and containment nodalization schemes as well as the core nodalization structure. Ideally, model optimization studies would have been performed to indicate the sensitivity (if any) to alternative schemes of such models.

For example, sensitivity studies might have been performed in which the core thermal response to a typical accident sequence was calculated using alternative axial and radial nodalization schemes. Similarly, the effects of thermohydraulic modelling simplifications (such as the number of interconnected control volumes used to represent multiple small compartments in the containment) may have been examined in sensitivity studies.

In the absence of such information, the reviewers should confirm that the spatial nodalization schemes used by the analysts are consistent with contemporary approaches used for similar plants.

Areas in which the plant model is asserted to be ‘conservative’ with respect to some process need to be given particular attention. For example, a model that neglects the heat capacity associated with boundary structures might be claimed to be conservative with respect to the calculation of peak internal atmosphere temperatures.

However, such simplifications might be non-conservative for other coupled phenomena, such as condensation of steam on walls, and lead to hydrogen stratification.

5.3.4.3. Accident scenario input

The reviewers should verify that the input data used to define the characteristics of a specific accident sequence are correct. The specific relationship between a computer code calculation and the accident sequences (or plant damage states) needs to be checked against the sources of data used for eventual quantification of events in the CET (Section 5.6). Such parameters include:

- Leak areas and their location;
- Performance specifications for operating equipment and systems, for example actuation/termination criteria, number of operating trains and flow or energy exchange rates;
- The timing of operator actions.

5.3.4.4. Input for models of accident phenomena

Unless otherwise required for reasons delineated in the accident analysis documentation, the model inputs that control how severe accident phenomena are treated need to be consistent from one calculation to another. Exceptions are sensitivity calculations performed with the explicit purpose of characterizing the effect of alternative credible models for uncertain phenomena. The reviewers should verify that a self-consistent set of phenomenological modelling assumptions is used in the code to generate the entire set of calculations used to represent baseline accident behaviour. Where calculations are performed with modelling assumptions that differ from the baseline values, the way they are used in Level 2 PSA needs to be checked as described in Section 5.6.

Again the reviewers need to pay particular attention to the areas in which selected modelling options are asserted to be ‘conservative’. For example, modelling choices that inhibit debris fragmentation and cooling in-vessel (which might be viewed as conservative from the point of view of thermal challenges to reactor vessel lower head integrity) also reduce steam production rates, thereby decreasing in-vessel hydrogen generation.

5.3.5. Results of Level 2 PSAs

It is usually impractical to examine the details of each and every calculation performed in support of a Level 2 PSA. However, the reviewers need to be satisfied

that the results are (in general terms) consistent with contemporary analyses for other similar plants.

The open literature contains numerous reports of detailed severe accident calculation, performed with various computer codes, for the accident sequences commonly found in Level 2 PSAs. Comparisons of calculated results with such reference analyses provide a useful basis for gauging the extent to which unique plant design or operating characteristics influence severe accident progression. In the absence of such information, the reviewers need to check global results by means of simple hand calculations, for example, mass/energy balances to estimate the timing of key events.

5.3.6. Treatment of major uncertainties

All engineering calculations are subject to some form of uncertainty. Although most Level 2 PSAs do not treat uncertainties in a rigorous manner, they need nevertheless to be accounted for via structured sensitivity studies or some other means. A well structured sensitivity analysis can identify which events and phenomena have the greatest impact on the calculated probability of containment failure or the magnitude of fission product source terms, without estimating their uncertainties quantitatively, i.e. the development of uncertainty distributions for all important output parameters. The reviewers need to be satisfied that a sufficient range of sensitivity studies has been carried out.

Typical issues that are examined as part of a structured sensitivity analysis are as follows:

In-vessel accident phenomena:

- Core debris relocation, fragmentation and coolability;
- Steam availability and associated hydrogen generation;
- Natural circulation (above the core) and induced RCS pressure boundary failures;
- Debris coolability and configuration in the lower head of the reactor vessel;
- Mode of reactor vessel failure;
- Hydrogen generation.

Ex-vessel core/debris phenomena:

- Debris fragmentation and dispersal following vessel breach at high pressure (direct containment heating issues);
- Fuel–coolant interactions on the containment floor;
- Debris coolability during corium–concrete interactions;
- Non-condensable gas generation.

Containment performance:

- Containment failure pressure, particularly for concrete structures;
- Thermal degradation of containment penetration seals;
- Leakage area associated with containment failure.

Containment phenomena:

- Heat loss to the environment for a steel shell containment;
- Natural circulation (buoyancy driven) flows;
- Hydrogen distribution (mixing/stratification);
- Hydrogen combustion (initiation/concentration threshold, burn completeness, flame propagation, speed);
- Effectiveness of engineered safeguard systems.

Other:

- Effect of operator actions.

The reviewers should be satisfied that sensitivity studies have been carried out for all phenomena significant for the plant being analysed. The specific parameters that can be varied to study the sensitivity of plant response depend strongly on the computer code used for the analysis. However, most codes provide some flexibility to the analyst for performing meaningful sensitivity calculations.

5.4. CONTAINMENT PERFORMANCE ANALYSIS

The severe accident phenomena identified above generate high pressures and temperatures within the containment. The aim of containment performance analysis is to determine whether the containment pressure boundary will be able to withstand these (and other) loads, which include:

- Internal slow quasi-static loads and rapid pressurization transients greater than those found under nominal design conditions;
- High temperatures;
- Thermo-mechanical erosion of concrete and steel structures (if contact with ejected core debris is possible);
- Impact from internally generated missiles;
- Localized dynamic loads, such as shock waves.

In some instances, these challenges may exist simultaneously. For example, high temperatures often accompany high pressures.

Engineering calculations of structural response to these types of challenge need to be performed as part of a complete Level 2 PSA. Quantitative failure criteria should be developed as the primary reference for estimating the likelihood of containment failure for a wide spectrum of accident sequences. These criteria need to be based on plant specific design and construction data, and represent realistic material response properties.

The reviewers need to check that the following features of the containment pressure boundary are included in the analysis:

(a) Containment configuration, construction materials and reinforcement. The containment designs include free standing steel shells, concrete backed steel shells, and pre-stressed, post-tensioned or reinforced concrete.
(b) Design of the containment liner with regard to containment penetrations.
(c) Penetrations of all sizes, their location in the containment structure and local reinforcement (including equipment and personnel hatches, piping penetrations, electrical assembly penetrations and ventilation system penetrations).
(d) Penetration seal configuration and materials.
(e) Local discontinuities in the containment structure (including shape transitions, wall anchorage to floors and changes in the steel shell or concrete reinforcement).

5.4.1. Structural response analysis

An analysis of the containment structural response to imposed loads should include interactions between the containment structure and neighbouring structures, both internal and external, includes the reactor vessel and pedestal, auxiliary buildings, and piping that penetrates the containment boundary.

The reviewers need to be satisfied that the analytical tools used to develop the containment failure criteria are accepted industry standards (e.g. rigorous finite element computer codes) or a method supported by experimental validation. Alternatively, experimental results can be used directly. For example, direct experimental data are available in the open literature regarding criteria for reactor containment penetration seal performance under conditions of high temperatures and pressures [41].

The reviewers must be satisfied that the way that the containment failure criteria are stated is acceptable. A complete structural performance assessment should distinguish conditions that would result in catastrophic failure of the pressure boundary from those that result in more limited leakage and identify the anticipated location of failure. For example, finite element analysis may suggest that increases in quasi-static pressure at relatively low temperatures may lead to tearing of a cylindrical (for

PWRs) containment wall where it joins the flat basemat floor. Under these conditions, and at this location, the anticipated size of the resulting opening in the containment wall is expected to be large. At the same pressure, but significantly higher temperatures, finite element analysis may suggest a different failure mechanism or location, and as a result a different size.

If external events are considered in the PSA, the structural response of the containment to postulated seismic events needs to be reviewed. As with other mechanisms for containment failure, the relationship between seismic intensity (ground acceleration) and the location and size of containment failure needs to be identified in the study. Analysis of structural response to dynamic loads (impulsive loads) is considerably more difficult than traditional static structural response analysis. It may not be practical to develop quantitative plant specific failure criteria. Rather, information presented in the open literature is commonly used to treat the possibility of containment failure due to in-vessel steam explosions [42], and catastrophic structural failure is often assumed to be a consequence of hydrogen detonations.

5.4.2. Containment bypass

In addition to structural failure of the containment pressure boundary, a thorough characterization of containment performance needs to include examination of the mechanisms and pathways by which fission products released from the RCS may bypass the containment and be released directly to the environment. The reviewers should examine the analyses performed to identify the locations, pathways and associated sizes of bypass mechanisms. Typical bypass mechanisms include interfacing system LOCA and SGTR.

With regard to SGTR, the reviewers also need to check that such events are not only treated as initiating events (carried forward from the Level 1 analysis) but are also considered as an event that may occur during in-vessel core degradation.

5.4.3. Failure of containment isolation

Two types of containment isolation failures are normally analysed and included in Level 2 PSAs. These are pre-existing leaks, i.e. undetected penetration seal failures or isolation valves which have failed in the open position and consequential isolation failure paths occurring after the initiating event.

Only leak paths that lead to leakage rates substantially higher than the design basis rate need to be considered.

5.5. PROBABILISTIC MODELLING FRAMEWORK

This part of Level 2 PSAs relates to providing a structured framework for organizing and displaying the alternative accident progressions that may evolve from a given PDS. This framework generally takes the form of CETs or APETs — the term CET is used here. These logic structures are the backbone of the Level 2 PSA model and need to be reviewed thoroughly.

5.5.1. Content and format of Level 2 PSA models

In reviewing the Level 2 probabilistic model, the reviewers should be satisfied that the following features are included in the assessment of the containment performance:

5.5.1.1. Explicit recognition of the important time phases of severe accident progression

Different phenomena may control the nature and intensity of challenges to containment integrity and the release and transport of radionuclides as an accident develops. The following time frames are usually identified in a Level 2 analysis:

(a) *After the initiating event but before the onset of core damage*: This time period establishes important initial conditions for containment response after core damage begins.
(b) *After core damage begins, but prior to failure of the reactor vessel lower head*: This period is characterized by core damage and radionuclide release from fuel while core material is confined within the reactor vessel.
(c) *Immediately following reactor vessel failure*: Prior analysis of containment performance suggests that many of the important challenges to containment integrity occur just prior to or following reactor vessel failure. These challenges may be short lived but often occur only as a direct consequence of the release of molten core materials from the reactor vessel immediately following lower head failure.
(d) *Long term accident behaviour*: Some accident sequences evolve rather slowly and generate relatively benign loads on containment structures early in the accident progression. However, in the absence of a mechanism by which energy generated within the containment can be safely rejected to the environment, these loads may increase steadily to the point of failure in the long term.

When linked end to end, these time frames provide a clear and chronological description of the alternative accident progressions represented in the PSA. The

reviewers need to be able to 'trace' individual accident sequences from the Level 1 PSA usually via a PDS through the alternative progressions of post-core damage accident behaviour.

5.5.1.2. Distinction of discrete system events from phenomena

Probabilities associated with 'events' in a CET are of at least two different types. One represents the conditional probability that an engineered system will operate, or fail to operate, upon demand or that a human will perform, or fail to perform, a specific activity. The probabilities of such events directly parallel those represented in Level 1 PSA accident sequence event trees and are developed in a similar manner.

The other type of probability represents uncertainties in the occurrence or effects of severe accident phenomena. For example, an 'event' may be included in a CET that depicts the divergence in plant behaviour that occurs or does not occur at some point in time when a hydrogen burn occurs. In this case, the split fraction associated with this event is not based on reliability data. Rather, it is a reflection of the uncertainties in the engineering analyses required to characterize hydrogen generation, release, distribution and combustion. The reviewers need to check that these distinct types of events are identified and treated appropriately in the logic.

5.5.1.3. Consistency in the treatment of severe accident events from one time frame to another

Many events or phenomena may occur over several time frames of a severe accident. However, certain limitations apply to the composite (integral) contribution of some phenomena over the entire accident sequence, and these are represented in the formulation of a probabilistic model.

A good example is hydrogen combustion in a PWR containment. Hydrogen generated during core degradation can be released to the containment over several time periods. However, an important contribution to the uncertainty in containment loads generated by a combustion event is the total mass of hydrogen involved in a combustion event. One possibility is that hydrogen released to the containment over the entire in-vessel core damage period accumulates without being burned, perhaps as a result of the absence of a sufficiently strong ignition source. Molten core debris released to the reactor cavity at vessel breach could represent a strong ignition source, which would initiate a large burn (assuming the cavity atmosphere is not inerted with steam). Because of the mass of hydrogen involved, this combustion event might endanger containment integrity.

Another possibility is that while the same total amount of hydrogen is being released to the containment during in-vessel core degradation, a sufficiently strong ignition source exists to cause several small burns to occur prior to vessel breach. In

this case, the mass of hydrogen remaining in the containment atmosphere at vessel breach would be very small in comparison with the first case, and the likelihood of a significant challenge to containment integrity at that time would be correspondingly lower.

The reviewers need to be satisfied that the logic for evaluating the probability of containment failure associated with a large combustion event occurring at the time of vessel breach can distinguish these two cases and preclude the possibility of a large combustion event if hydrogen was consumed during an earlier time frame.

5.5.1.4. Recognition of the interdependences of phenomena

Most severe accident phenomena and associated events require certain initial or boundary conditions to be relevant. For example, a steam explosion can only occur if molten core debris comes into contact with a pool of water. Therefore, it may not be meaningful to consider ex-vessel steam explosions during accident scenarios in which the drywell floor (for BWRs) or reactor cavity (for PWRs) is dry at the time of vessel breach. Logic models for evaluating containment performance have to capture these and many other such interdependences among severe accident events and phenomena. Explicit representation of these interdependences provides the mechanism for allowing complete traceability between a particular accident sequence (or PDS) and a specific containment failure mode.

5.5.2. Presentation of results

The total number of individual severe accident progressions represented by a Level 2 PSA model can be quite large. Consequently, grouping logic is often applied to determine the aggregate frequency of accident progressions that have common features. These features might include time and/or mode of containment failure, manual actions to terminate core damage, or engineered safeguards system operation. If these features are selected appropriately, accident progressions can be grouped in a manner that allows a common fission product source term to be assigned to them.

The reviewers should be satisfied that the final results are consistent with accident progression calculations performed for key accident sequences. Major contributors to various modes of containment failure need to be identified and described. Results need to be presented both in terms of total frequency of various levels of containment performance and in terms of conditional probability, given core damage. Unusually high, or low, probabilities of containment survival as well as important containment failure modes need to be traceable to deterministic analysis of key accident progressions.

5.6. QUANTIFICATION OF THE CONTAINMENT EVENT TREES

The reviewers should be satisfied that the methods and technical bases used to define the individual event probabilities used in the quantification of the CET are acceptable. The methods used need to be examined to ensure that the calculated results from the PSA can be used to achieve the stated objectives of the study. The technical bases used to quantify events need to be carefully examined to ensure they are traceable and that the probabilities generated from them represent an unbiased characterization of accident behaviour. That is, to ensure that appropriate consideration has been given to the uncertainties that accompany deterministic calculations of severe accident phenomena.

5.6.1. Assignment of event probabilities

There are many approaches to transforming the technical evidence concerning containment loads and performance limits to an estimate of failure probability, but the following approaches appear most often in contemporary studies:

Expert judgement: The least rigorous approach is to apply expert judgement in translating the qualitative terms expressing various degrees of uncertainty into quantitative (point estimate) probabilities. For example, terms such as 'likely' or 'unlikely' are assigned numerical values (such as 0.9 and 0.1). The subjectivity associated with this method is controlled to some extent by developing rigorous attributes for the amount and quality of information necessary to justify progressively higher confidence levels, i.e. probabilities approaching 1.0 or 0.0. The main concern about this method is that the estimates made may not be reproducible and may not provide a clear basis for understanding and resolving disagreements between the reviewers and the PSA team.

Convolution of two probability density functions: In this technique, probability density functions are developed to represent the distribution of credible values for a parameter of interest (e.g. the containment pressure load) and for its corresponding failure criterion (the ultimate pressure capacity). The basis for developing these distributions is the collective set of information generated from plant specific integral code calculations, corresponding sensitivity calculations, other relevant mechanistic calculations, experimental observations and expert judgement. The conditional probability of containment failure (for a given accident sequence) is then calculated as the convolution of the two density functions. It is important for the reviewers to realize that although an approach of this type may lead to a more traceable relationship between the estimated probability and the amount and quality of supporting data

(such as code calculations and verification, experimental data), it is quite possible for an analyst to use unsupported judgements in developing the input probability. Clearly, the reviewers need to check this point.

Decomposition methods: This is a more general form of the load resistance comparison method described above. The basic idea is to break down a question such as "Does the containment fail due to hydrogen combustion?" into a set of questions that can be more easily analysed. For example, the question posed in the previous sentence might be broken down into:

(a) How much hydrogen is generated?
(b) What is the hydrogen burn pressure, given *x/y/z%* hydrogen in the atmosphere?
(c) What is the probability that the containment fails given a pressure rise of *a/b*?

Such decompositions are often developed in the form of event trees. The problems the reviewers may encounter are similar to those where probability density functions are used. While the questions addressed in the decomposition are chosen because they can be more easily related to information from experiments or code calculations, the reviewers may still encounter probabilities which have been assigned without adequate support. The physical reasonableness of the decomposition itself also needs to be reviewed.

Most contemporary Level 2 PSAs use a mixture of approaches. The reviewers should be satisfied that the method used to quantify events that are found to be important contributors to risk measures such as the frequency of early containment failure, or the frequency of large fission product releases, are acceptable. A meaningful interpretation of the results must take into account situations where results may be heavily influenced by subjective values for the probability of 'unlikely' events.

5.6.2. Technical basis for event quantification

The input to the probabilistic models usually stems from several sources. For example, useful information will be available from:

- Computer code calculations of severe accident behaviour,
- Interpolation of results from code calculations,
- Applications of relevant experiments,
- Engineering calculations,
- Expert judgement (possibly using all of the above sources),
- Engineered systems analysis,
- Human reliability analysis.

The specific information used to support the assignment of event tree branch probabilities needs to be reviewed and compared with the following general guidelines. A quality Level 2 PSA will make maximum use of plant specific deterministic calculations. Use of generic information (e.g. from a reference plant analysis) needs to be justified, and is probably most appropriate for complex issues that are not treated by general purpose accident analysis codes (e.g. re-criticality following re-flooding of a damaged reactor core, and steam explosions). Interpolation or extrapolation of results from code calculations needs to be carefully examined to ensure that the results are applied in a manner that is consistent with the framework of the original calculations. Use of 'reference plant' analysis is only acceptable when accompanied by analysis or arguments that support its applicability to the plant under consideration. The reviewers should check any non-standard codes or hand calculations that were used, with particular emphasis on the assumptions.

Information derived from the containment system analysis (system unavailabilities, non-recovery probabilities and human error probabilities) needs to be reviewed with special attention paid to modelling consistency with relevant Level 1 PSA models.

5.6.3. Uncertainties in event quantification

The basic probability density functions representing uncertainty in each parameter involved in the CET may be propagated throughout the entire model to allow for calculation of statistical attributes such as importance measures, and to allow for the generation of uncertainty distributions on results such as the frequency of source term groups.

One means of performing this propagation of uncertainties is the application of Monte Carlo sampling techniques (such as Latin hypercube sampling). The application of this technique to Level 2 PSA logic models, pioneered in Ref. [43], accommodates a large number of uncertain variables. Other techniques have been developed for specialized applications, such as the direct propagation of uncertainty technique developed to assess the probability of containment failure as a result of direct containment heating in a large dry PWR [44]. However, these other techniques are constrained to a small number of variables and are not currently practicable for applications involving the potentially large number of uncertain variables addressed in a good quality Level 2 PSA.

If an uncertainty analysis of the type described above has been performed, the reviewers need to confirm that the probability distributions developed for key events reflect the full range of information on the subject.

However, in many Level 2 PSAs, comprehensive uncertainty analyses are not performed. In such cases, the reviewers should confirm that, as a minimum, sensitivity

studies were performed to determine the extent to which Level 2 PSAs are influenced by the specific value of probabilities assigned to events in the CET model.

The reviewers also need to determine whether event quantification is influenced by a bias in the information used to evaluate severe accident phenomena. For example, the exclusive use of calculations performed with a single computer code can lead an analyst to high levels of confidence that a particular event is 'certain', or conversely 'impossible'. However, these conclusions may conflict with results developed in other studies, using a different computer code, for very similar circumstances. Hence, the review team needs to include experts in severe accident phenomena to ascertain whether such biases exist in the CET structure or in event quantification. In addition, PSA codes may have limitations which influence the propagation of uncertainties and the robustness of uncertainty analysis, such as a limited capacity for event tree analysis, which forces the use of decomposition event trees. In these cases, the reviewers also need to evaluate carefully any uncertainty analysis performed for the PSA.

5.7. CHARACTERIZATION OF THE RADIOLOGICAL SOURCE TERMS

The next step in a Level 2 PSA is to estimate fission product release to the environment — referred to here as the radiological source terms. This is required if it is intended to carry out a Level 3 PSA to determine the public health and economic risks but is not required if all that is intended for the Level 2 PSA is an evaluation of the containment performance.

5.7.1. Grouping of radiological source terms

The accident sequences defined by a CET are usually grouped according to the major characteristics which influence severe accident progression. If a unique source term is assigned to each end state of the probabilistic logic model, these grouping characteristics need to include parameters that influence fission product evolution, and retention and transport through each of the major barriers to the environment. End states grouped in such a manner are referred to as release categories or source term groups.

The reviewers should be satisfied that the attributes used to define source term groups have similar radiological release characteristics and potential off-site consequences. These attributes are often plant and containment specific, with typical characteristics (for PWRs) being as follows:

Time of release

- Very early (containment failure or bypass prior to core damage or during core melt),

- Early (around the time of vessel breach),
- Intermediate (up to several hours after vessel breach),
- Late (to the end of Level 2 mission time).

Containment status at the end of Level 2 mission time

- Containment bypassed by interfacing systems LOCA,
- Containment bypassed by unisolated SGTRs (for PWRs),
- Containment not isolated,
- Containment penetration failure (enhanced leakage),
- Containment structural failure (large leak area),
- Containment vented (filtered/unfiltered),
- Basemat penetration,
- Design basis leakage.

Mode of ex-vessel releases

- Dry core–concrete interaction,
- Core–concrete interaction submerged,
- No core–concrete interactions.

Fission product removal mechanisms

- None,
- Containment sprays and/or fan coolers operating (time of operation may be specified also),
- Secondary containment or reactor building.

Pressure suppression pool (BWRs)

- Subcooled,
- Saturated,
- Bypassed (and time of bypass).

Time of core damage relative to accident initiation

- Within a few hours,
- After several hours (typically more than 10).

If a Level 3 PSA is to be performed using the Level 2 PSA source term groups, additional attributes may be defined, such as:

— location of the release
— energy of the release
— start time of the release (after the occurrence of the initiating event)
— release duration.

Verifying the similarity of source terms for accident sequences within a release category can be difficult without deterministic calculations of fission product release and transport. It is common practice to perform a source term calculation only for a single 'representative' accident progression within each release category. The reviewers need to be satisfied that the accident progressions are selected for representative source term calculations, and agree with the rationale used by the PSA analysts that other accident progressions within the same release category would result in a similar source term. The availability of calculations for alternative representative sequences in the most important source term categories would increase the reviewers' confidence in the results obtained.

5.7.2. Grouping of fission products

Fission products with similar chemical and physical properties are usually treated collectively in severe accident source term analysis [9, 10]. Distinctions among individual isotopes of major radionuclide species are not made in the calculation of fission product release to the environment. The grouping scheme is typically defined in the computer code used to generate source term estimates; a typical radionuclide grouping scheme is shown in Table I.

Depending on the objectives and scope of the Level 2 PSA, a detailed accounting of all the species of fission products may not be necessary. Occasionally, source term estimates are limited to the noble gases, halogen and alkali metal groups. This practice is generally acceptable because iodine and caesium release estimates tend to dominate the short term and long term human health consequences, respectively. The reviewers need to examine the method used to calculate radionuclide release to the

TABLE I. RADIONUCLIDE CLASSES (MELCOR GROUPING)

Radionuclide class name	Representative species	Member elements
Noble gases	Xe	He, Ne, Ar, Kr, Xe, Rn, H, N
Alkali metals	Cs	Li, Na, K, Rb, Cs, Fr, Cu
Alkaline earths	Ba	Be, Mg, Ca, Sr, Ba, Ra, Es, Fm
Halogens	I	F, Cl, Br, I, At
Chalcogens	Te	O, S, Se, Te, Po
Platinoids	Ru	Ru, Rh, Pd, Re, Os, Ir, Pt, Au, Ni
Early transition elements	Mo	V, Cr, Fe, Co, Mn, Nb, Mo, Tc, Ta, W
Tetravalents	Ce	Ti, Zr, Hf, Ce, Th, Pa, Np, Pu, C
Trivalents	La	Al, Sc, T, La, Ac, Pr, Nd, Pm, Sm, Eu, Gd, Tb, Dy, Ho, Er, Tm, Yb, Lu, Am, Cm, Bk, Cf

environment and be confident that the radionuclide grouping scheme is consistent with current, state of the art, practices.

5.7.3. Fission product release and transport

The analytical models (computer codes) used to calculate fission product release and transport should be verified as being appropriate for the task. Common computer codes used for this purpose are listed in Ref. [5].

If the objective of Level 2 PSA is to provide a technical basis for installing (or not installing) severe accident mitigation devices, such as a filtered containment venting system, independent source term calculations using a different computer code are advisable. Adaptation of source terms from reference plants will not be accepted. Independent calculations of source terms for selected sequences may be warranted if the frequency of large radionuclide release is unusually high, or if the PSA is to be extended to Level 3 analysis.

In many cases, however, source term results are used simply as a quantitative measure for ranking the relative importance of various accident sequences. Under such circumstances, a detailed review of calculated results may not be warranted. However, spot checks of results need to be made by comparison with those documented in other similar studies [43, 45].

If the frequency of occurrence of the following accident conditions is significant, the corresponding source terms need to be reviewed with particular care:

(a) *Steam generator tube ruptures*. Releases from unisolated SGTRs can span a very broad range. Very large releases can occur for accident sequences in which the steam generator secondary inventory is depleted; conversely, moderate releases may result if the ruptured tube(s) is submerged in water.
(b) *Releases from accidents with unisolated containment*. Depending on the size of the failed isolation(s), and on the path of release, estimates may vary from small to very large.
(c) *Releases from accidents with late containment failure*. Depending on the containment capacity, late failure may occur anywhere between 10 and 48 hours after core damage. Over these long time periods, revaporization of volatile species (halogen, alkali metals and chalcogens) from dry overheated surfaces can dominate the source term.
(d) *Releases from accidents with scrubbing provided by containment sprays*. The effectiveness of the containment spray in reducing airborne radionuclide concentrations can span several orders of magnitude, depending on the spray water temperature, droplet size and spray distribution within the containment atmosphere.

5.7.4. Treatment of uncertainties in source term estimates

Quantitative evaluations of source term uncertainties are not usually made in Level 2 PSAs. However, a structured sensitivity analysis of source term calculations for major accident scenarios is expected to be available and to be reviewed. The reviewers should be satisfied that the major modelling assumptions are identified and their importance quantified. For example, the extent to which iodine is assumed to be permanently retained in water during late phases of an accident is highly uncertain. The effects of baseline modelling assumptions concerning iodine aqueous chemistry (and many other similar processes) need to be measured and incorporated in the Level 2 PSA results.

5.7.5. Presentation of the results

The presentation of source term results needs to conform to the prescriptions detailed in Ref. [9]. Where the reviewers have developed models for an independent estimate of the source terms, similar tables have to be derived and a comparison made with the results of the PSA. In addition, from these tables, cumulative complementary distribution functions may be constructed and then compared with the results of published Level 2 PSAs. This information is vital for the review process and can provide insights on several risk figures of merit (including the large early release frequency (LERF)).

5.8. RESULTS OF LEVEL 2 PSAs

The general statements made in Section 3 about the presentation of the results of Level 1 PSAs are also valid for Level 2 PSAs. This is particularly important for Level 2 PSAs in view of the complicated phenomena modelled and the uncertainties involved. Difficulties inevitably arise in the communication of the results of the analysis to non-specialists.

This places a more onerous requirement on analysts and reviewers to present the results of the PSA and the findings clearly and succinctly, in non-specialist language, so that they can be understood more widely. This is particularly important where the results have been used to indicate that changes need to be made to the design or operation of the plant to provide additional protection against severe accidents.

5.8.1. Review of PSA results

The presentation of the results of a Level 2 PSA depends on the aims and objectives of the analysis. For a full scope analysis, the results would be in the form of

source terms and their frequencies, where the source term specifies the quantity of each of the isotopes for each of the release groups included in the analysis. This information needs to be grouped to provide estimates of the frequency of a large (early) release, where this is required to allow a comparison to be made with probabilistic safety criteria.

The results should include sufficient information to give insights into the main contributors to risk and the uncertainties in these estimates of risk. This would result in identification of the weaknesses in the design or operation of the plant in relation to providing protection against severe accidents.

The reviewers need to be satisfied that the global results of the PSA are plausible, the interpretation and conclusions drawn from the results are logical and correct, and the overall objectives of the PSA and the PSA requirements and guidelines are met.

The reviewers need to check that a sufficient range of sensitivity studies have been carried out that relate to the aspects of the analysis which are most significant in determining the level of risk and those which have the highest uncertainty. The reviewers should also check that the results of the sensitivity studies demonstrate that the conclusion of the analysis and the insights derived from it are still valid.

It is necessary that the results of Level 2 PSAs be compared with those for plants with similar containment and containment systems design, and any differences identified. These need to be investigated since this may provide additional help to the reviewers in the identification of potential weaknesses of the PSA.

The reviewers need to check the assumptions made in the PSA carefully. This particularly applies to areas of the PSA that rely on expert judgement.

The reviewers should identify relevant experimental data which address processes represented in analytical models contained in the PSA, and satisfy themselves that these have been properly and adequately taken into account. The reviewers need to be satisfied that the benefits from carrying out accident management measures are reasonable in relation to the results of the PSA.

5.8.2. Use of PSA results

The reviewers should compare the results of the analysis with the probabilistic safety goals defined for the plant (if such goals have been defined). In some countries, risk criteria have been defined which relate to the frequency of a large release or a large early release of radioactivity.

The results of the PSA are used to determine whether there are any weaknesses in the design and operation of the plant. Where such weaknesses are identified, consideration may be given to identifying improvements which could be made to reduce the risk from severe accidents. This typically includes additional safety

systems to provide protection from some of the adverse consequences of a severe accident. In the past, such additional safety systems have included the following:

(a) The incorporation of hydrogen igniters or recombiners that have sufficient capacity to deal with the rate of hydrogen generation which would occur during a severe accident;
(b) The addition of a filtered containment venting system which would prevent failure of the containment due to overpressurization for longer.

The results of the PSA are used to determine whether there are additional accident management measures which could be incorporated to reduce the risk from severe accidents. This typically includes the use of existing equipment to provide protection from some of the adverse consequences of a severe accident. In the past, such accident management measures have included the following:

(1) The use of the primary relief valves to depressurize the primary circuit to prevent the possibility of high pressure melt ejection,
(2) The addition of water to the containment to help with core cooling.

The reviewers need to check that, where accident management measures have been identified which are effective in reducing the risk, they have been included explicitly in the emergency operating instructions.

5.9. AUDIT OF PSA QUALITY ASSURANCE

As discussed in Sections 2.2–2.4, it is good practice for the QA procedures used in performing a PSA (including technical procedures) to be reviewed and approved by the regulatory body at an early stage of the PSA (ideally, before the start of the analysis). Whether or not this is done, the regulatory body may conduct audits during the process of the PSA development to ensure that the QA procedures are indeed followed, and that the process for performing the PSA is being properly managed. The frequency of audits can be determined to meet specific needs. To receive the maximum benefit from audits, it is important that the first audit be carried out at an early stage in the PSA development, so that any deficiencies identified in the audit can be corrected then.

6. REVIEW OF LEVEL 3 PSAs

The radiological source terms and frequencies identified in Level 2 PSAs are used in Level 3 PSAs to determine the risk to the public. This includes the risks to

health and other societal risks such as contamination of land, air, water or food. This is done by modelling how the radionuclides released from the plant are transported through the environment and lead to the these risks. This section provides guidance on the technical issues that need to be addressed in carrying out the review of a Level 3 PSA.

The exposure of individuals to ionizing radiation can lead to health effects which are generally classified as either 'deterministic' or 'stochastic'. Deterministic effects result from exposure of the whole or part of the body to high doses of radiation. Their severity is observed to increase with dose, and there is usually a threshold dose below which effects are not induced. Stochastic effects of radiation include an increased incidence of cancer among the exposed population and of hereditary disease in their descendants. For stochastic effects, the probability of occurrence, but not the severity, depends on the radiation dose. Effects observed in exposed individuals, i.e. deterministic effects and cancers, are termed 'somatic' effects, while those observed in their descendants are known as 'hereditary' effects. Deterministic and stochastic effects are often referred to as 'early' and 'late' effects, respectively.

Level 3 PSAs provide insights into the relative importance of accident prevention and mitigation measures expressed in terms of the risk to the public and the relative effectiveness of the off-site emergency plans and countermeasures for the site.

This section addresses:

- The aims of Level 3 PSAs,
- Source term characterization and grouping,
- The choice of a consequence analysis code,
- The data requirements for the consequence analysis,
- Atmospheric dispersion modelling,
- Identification and modelling of emergency planning and countermeasures,
- Quantification and use of the results of Level 3 PSAs.

6.1. AIMS OF LEVEL 3 PSAs

The aims of Level 3 PSAs can range from carrying out a analysis to determine the health effects on people close to the site to carrying out a more sophisticated analysis to provide estimates for a wide range of societal health and economic risks.

The reviewers need to be satisfied that the Level 3 PSA aims have been clearly defined. In particular, this relates to the range of societal risks that need to be addressed by the Level 3 PSA and the risk criteria that will be used to determine whether the results produced by the analysis are acceptable. This will influence the choice made for the consequence analysis code and the amount of data required.

6.2. RADIOLOGICAL SOURCE TERM CHARACTERIZATION AND GROUPING

The starting points for the consequence analysis carried out for a Level 3 PSA are the radiological source terms and frequencies produced by the corresponding Level 2 PSA. In general, this identifies a large number of accident sequences, each with characteristic source terms, which should be grouped to limit the consequence analysis that needs to be carried out to a manageable size.

The radiological source terms include a range of different radionuclides in different physical and chemical forms, which behave differently in the way that they are transported through the environment and contribute to the societal risks.

The reviewers should check that the radiological source term groups have been fully specified in terms of the quantity of each of the radionuclides in the group, and that their physical and chemical forms are adequately determined.

The magnitude of the radiological source term is usually specified by defining groups of elements which have the same physical and chemical properties. The magnitude of the release is specified by defining the fraction of the reactor inventory of each group of elements that is released to the atmosphere. The reviewers need to be satisfied that the way the magnitude of the radiological source terms has been defined is consistent with current best practice.

The reviewers should be satisfied that all the accident sequences identified in the Level 2 PSA have been mapped correctly into the radiological source term groups used in the Level 3 PSA.

The reviewers must also be satisfied that the time dependent characteristics of the release of the radionuclides from the plant are fully specified for each of the source term groups. This is usually done by specifying:

- The time that the release starts,
- The duration of the release,
- The amount of energy associated with the release,
- The height of the release and the building dimensions,
- The warning time (for the initiation of off-site countermeasures).

Where accident sequences identified from the Level 2 PSA are included in radiological source term groups, the reviewers need to be satisfied that the members of the group have similar characteristics and that the group is defined in a way that bounds the characteristics of the individual members of the group.

Where the data on the radiological source terms produced by the Level 2 PSA are imprecise, for example information on the particle size of aerosols, the reviewers should be satisfied that reasonably conservative assumptions have been made.

6.3. CONSEQUENCE ANALYSIS CODES

The aim of the consequence analysis is to model the transport of the radionuclide releases from a plant through the environment and to determine the resulting risks to public health and the economic consequences of an accident. For a nuclear power plant, the main contribution is likely to be from the atmospheric release and dispersion of radionuclides. However, other pathways such as the migration of radionuclides in groundwater may also need to be considered.

The basic elements of a consequence analysis are as follows (see Section 2.1.1 of Ref. [10]):

— sampling of meteorological data
— atmospheric dispersion and deposition modelling
— dose evaluation for each exposure pathway
— accounting for countermeasures
— estimation of health effects
— estimation of economic consequences.

The consequence analysis software codes which have been developed usually model:

- The different phenomena that can occur (air mixing, atmospheric dispersion, wet and dry deposition of airborne material, resuspension, migration through food chains, etc.);
- The characteristics of the terrain surrounding the site;
- The weather patterns in the area of the site;
- Human habits (population distribution, food consumption patterns, etc.).

Hence these codes determine:

- The health effects on the public;
- The economic consequences (area evacuated, area of land contaminated, etc.).

The consequence analysis needs to take into account the exposure pathways:

(a) External radiation from radioactive material in the passing plume or cloud — *cloud shine*,
(b) External irradiation from radioactive material deposited on the ground — *ground shine*,
(c) External irradiation from radioactive material deposited on skin and clothing — *deposition*,

(d) Internal irradiation from radioactive material inhaled directly from the passing plume — *inhalation*,
(e) Internal irradiation from radioactive material inhaled following resuspension of the ground deposit — *resuspension*,
(f) Internal irradiation from radioactive material ingested following the contamination of foodstuffs by radioactive material deposited from the plume — *contamination of foodstuffs*.

The consequence analysis codes contain models that convert the concentration of radionuclides in the atmosphere, on the ground, in foodstuffs or on the skin and clothing to the dose to humans.

Many of the consequence analysis codes are probabilistic codes in that they calculate averages over the range of weather conditions that can occur. These are based on a scheme which samples the meteorological data provided for the site.

There are a number of consequence analysis codes currently in use; these include ARANO, CONDOR, COSYMA, LENA, MACCS, MECA2 and OSCAAR. Some information on these codes and their capabilities is given in the Annexes to Ref. [10]. Work has also been carried out internationally to compare these codes. The conclusion drawn was that the predictions made by the codes were in reasonable agreement, i.e. the spread of variation between the code predictions was within a narrow range which was small in comparison with the overall uncertainty associated with the estimation of the risk from a nuclear power plant.

The reviewers should determine the basis on which the computer code used for the consequence analysis has been selected and be satisfied that it is suitable for the aims of the Level 3 PSA. This needs to be a state of the art code which incorporates currently acceptable models, calculational methods and databases. The code needs to have been fully validated and verified.

In addition, the reviewers should be satisfied that the analysis is being carried out by experienced analysts who understand the models and data included in the code, understand the default parameter settings and are using the code within its limits of applicability. This is particularly important for consequence analysis codes since they generally have a range of modelling options and a large number of parameters which the users can either set themselves or for which they can use default values.

The reviewers have to be satisfied that all the relevant exposure pathways are included in the code.

6.4. DATA REQUIREMENTS FOR CONSEQUENCE ANALYSES

This section is related to the data that are required to carry out a consequence analysis, which include meteorological data, and population, agricultural and

economic data. The modelling of countermeasures and the data required for this are covered in Section 6.5.

6.4.1. Meteorological data

Meteorological data are required for the whole of the area covered by the consequence analysis. This would include data which are specific to the site and national data if the consequence analysis needs to extend beyond this region.

The meteorological data typically include:

— wind direction
— wind speed
— stability category
— rainfall
— mixing layer depth.

Consequence analysis codes typically require this information to be specified at regular intervals (normally hourly) for a prolonged period of time. Ideally, a long enough period, for example ten years, should be covered to ensure that rare weather conditions have been included. However, a shorter time might be acceptable, but would need to be at least one year.

The reviewers need to understand the basis on which the meteorological data have been specified for the consequence analysis and be satisfied that it is representative of the area over which the consequence analysis is to be carried out. For the region close to the site, this would normally be data recorded at the nearest meteorological station. For the region further from the site, this would normally be based on national meteorological data.

Some of the meteorological data may not be complete. In addition, some of these parameters, for example, stability category and mixing layer depth, may not have been routinely measured and may need to be derived from other measurements. Where the data available are incomplete or inconsistent, the reviewers need to be satisfied that the way that the data have been processed or added to is satisfactory.

If a probabilistic consequence analysis code is used, the reviewers should be satisfied that the meteorological data are provided in a form that is suitable for the sampling scheme used in the code.

6.4.2. Population, agricultural and economic data

Consequence analysis codes typically require information on the spatial distributions of:

— population data
— land use and agricultural production data
— food distribution data
— economic assets.

These data are needed to determine the radiation doses arising from the external exposure, inhalation and ingestion pathways, and to calculate the impact of implementing countermeasures such as relocation and food bans.

These data normally need to be specified in annular segments centred on the site and segmented by radial lines, i.e. an (r, θ) grid with a spatial resolution finer near the site than further away from it. This should be consistent with the way that the meteorological data are specified. Since the available data are not specified in this form, a conversion process will usually be necessary to map them to the (r, θ) grid.

The reviewers must be satisfied that the land data specified are acceptable. This is usually done by defining the fraction of each spatial element in the (r, θ) grid that is land, lakes or sea, and the fraction of the land that is urban or rural. This information is usually derived from large scale maps.

The reviewers should be satisfied that the population data are acceptable for the purposes of the consequence analysis. Census data, which need to be sufficiently up to date to represent the current population distribution, would normally be used. These data need to be supplemented where appropriate by local surveys in the immediate vicinity of the plant and have to take account of daily and yearly variations in the population distribution.

The land use and agricultural data relate to agricultural production and distribution. They are required to calculate the collective dose due to ingestion. The precise agricultural data required depend on the aims of the Level 3 PSA and the consequence analysis code but typically include the number and type of livestock, the milk production and the type of crops grown. If food distribution is taken into account, it is necessary to specify the regions of food production and consumption. Agricultural data are usually based on government information and need to be mapped onto the (r, θ) grid being used by the consequence analysis code. The reviewers should be satisfied that these data have been derived and used in an acceptable way.

The economic data required relate to, for example, the gross domestic product, the value of land and the value of housing for each of the sectors defined in the consequence code. These are usually based on government economic data which need to be mapped onto the (r, θ) grid being used by the consequence analysis code. This could also include the cost of countermeasures (evacuation, relocation, food restrictions and decontamination) and the costs of the health effects on the exposed population. The reviewers should be satisfied that these data have been derived and used in an acceptable way.

6.5. EMERGENCY PLANNING AND COUNTERMEASURES

6.5.1. Emergency planning and countermeasures options

In the event of a release of radioactive material from a nuclear power plant, there are a number of countermeasures which can be applied to reduce the risk to the public. These include the following short term countermeasures:

— sheltering the affected population
— issue of stable iodine tablets
— evacuation
— human decontamination

which are undertaken to limit the exposure of the public to both internal and external radiation with the aim of preventing deterministic effects and minimizing stochastic effects.

There are also long term countermeasures, which include:

— relocation
— food bans
— land decontamination

which are undertaken to reduce chronic exposure to radiation, both externally from deposited material and internally from ingestion of contaminated food, with the intention of reducing the incidence of late health effects.

Account needs to be taken of these countermeasures to get a realistic estimate of the risk to the public. The consequence analysis codes typically allow a wide range of off-site emergency actions to be modelled and the user has considerable flexibility in setting the criteria for these countermeasures. These can be set in terms of the dose levels at which actions are assumed to be taken or the time at which the countermeasures are implemented in relation to the developing accident scenario. The reviewers need to be satisfied that a sufficient set of countermeasures has been identified and addressed in the analysis (consistent with the agreed scope of the Level 3 PSA).

The reviewers have also to be satisfied that the countermeasures strategies modelled in the consequence analysis are feasible and correspond to national requirements; in particular that the trigger levels set for the implementation of these countermeasures and the time taken to implement them are realistic. The trigger levels can be based on the plant condition, an estimate of the potential off-site dose, an estimate of the dose that is likely to be averted by implementing the countermeasure, or actual off-site radiation measurements. National criteria are usually set for the trigger levels at which stable iodine tablets are issued, evacuation is required and food bans are implemented.

6.5.2. Emergency planning and countermeasures data

Data are required for the modelling of the countermeasures in the consequence analysis. This relates to the effectiveness of countermeasures in reducing the dose received by individual members of the public. The data required include the trigger levels at which the countermeasures would be carried out and their effectiveness.

The trigger levels at which particular countermeasures are carried out normally relate to plant conditions or off-site dose levels. The plant conditions can be that a release of radioactivity has actually occurred or that the accident sequence is developing in such a way that a release is likely to occur which would exceed the dose levels at which countermeasures would be required.

These dose trigger levels relate to the dose at which it would be beneficial to take the appropriate countermeasure. For example, dose levels may be defined for the issue of stable iodine tablets, evacuation and imposition of food bans. These are often defined at a government level.

The reviewers need to be satisfied that the countermeasures strategies which are modelled in the consequence analysis are realistic and that the trigger levels defined are consistent with national requirements. This is important since experience with consequence analysis has shown that the results can be sensitive to the timing of the countermeasures in relation to the release.

The data relating to the effectiveness of stable iodine tablets are normally included in the consequence analysis code. For sheltering, the data required relate to the degree of shielding and air filtration provided by the building structure, which depend on the types of building in the region close to the site. For evacuation, the data required relate to the time taken to start the evacuation, its duration, its effectiveness and the route taken.

The reviewers need to be satisfied that the basis for selecting the data is acceptable. Where default values in the consequence analysis code are used, these should be checked to determine their applicability.

6.6. RESULTS OF LEVEL 3 PSAs

6.6.1. Quantification of the analysis

The results of Level 3 PSAs are normally presented as complementary cumulative distribution functions (CCDFs) which give the overall frequency of occurrence of a number of consequences, for example the number of early or late deaths and the area of land contaminated.

The codes available are generally used to carry out a consequence analysis for one of the radiological source term groups and to provide information on the spatial

distribution of the public risks averaged over the weather conditions which could occur at the time of the release. This information then needs to be weighted by the frequency of the source term group and combined to form the CCDFs. This part of the analysis is usually done by a separate computer code or a spreadsheet into which the results of the consequence analysis code are fed. More detail on the way that the results of the consequence analysis are used to form the CCDFs is given in Ref. [10].

The CCDFs should be presented for each of the public health and economic risks addressed by the Level 3 PSA. The reviewers need to be satisfied that the results of the consequence analysis have been used correctly in the construction of these CCDFs.

6.6.2. Sensitivity studies and uncertainty analysis

The aims of carrying out sensitivity studies and uncertainty analysis for Level 3 PSAs are broadly the same as those for Level 1 PSAs (Sections 3.11.1 and 3.11.2).

The reviewers have to be satisfied that a sufficient range of sensitivity studies have been carried out to address the main modelling assumptions made and the data used in the consequence analysis. In particular, reviewers need to address the way that off-site countermeasures have been modelled in the analysis, since this is an area of significant uncertainty.

In addition, where an uncertainty analysis is required as part of the scope of the Level 3 PSA, the reviewers should check that this has been carried out in an acceptable way.

6.6.3. Use of results

The reviewers need to be satisfied that the results of the Level 3 PSA have been used to identify where the weaknesses are in the design, operation and accident management measures for the nuclear power plant. In addition, they need to be satisfied that the results have been used as an input into planning the emergency countermeasures for the plant.

The results of the Level 3 PSA should be compared with probabilistic safety criteria where such criteria have been established. The safety criteria which relate to societal risk are usually defined in terms of:

- The risk of death (early or late) for individual members of the public;
- The number of deaths (early or late) in the public as a whole;
- The economic consequences (area evacuated, area of land contaminated, etc.).

The reviewers need to be satisfied that these criteria have been met.

Appendix

ACCIDENT PHENOMENA TO BE ADDRESSED WITH ACCIDENT PROGRESSION MODELS

The phenomena that need to be addressed in each of the time domains are as follows.

RCS thermohydraulic behaviour prior to core damage

- Depletion of primary coolant inventory;
- Temporal changes in core power;
- Reduction in reactor vessel level;
- Thermodynamic effects of steam generator, relief valve and coolant injection system operation (along with other systems represented in PDS definitions);
- Asymmetric RCS coolant flow and heat transfer associated with pipe breaks (LOCAs), pressurizer behaviour or non-uniform steam generator operation.

In-vessel core degradation

- Fuel heat-up, and heat transfer to neighbouring structures;
- Metal–water reactions and accompanying hydrogen generation;
- Eutectic material formation and associated changes in thermophysical properties;
- Control material melting and relocation;
- Ballooning, failure, melting and relocation of cladding;
- Dissolution of fuel and relocation with molten metals;
- Re-freezing of previously molten material on cooler surfaces;
- Formation of local and/or core-wide blockages;
- Accumulation of molten materials above large scale blockages;
- Enhanced steam/hydrogen generation accompanying the water introduced to the core debris (e.g. from midperiod accumulator operation);
- Structural collapse of fuel rods (formation of particulate) and other structures;
- Relocation of molten material (via pouring) and/or regional collapse of core debris into the lower plenum of the reactor vessel;
- Quenching of core debris in the lower plenum and debris formation on the lower head surface.

RCS pressure boundary failure

- Buoyancy driven natural circulation flow within the reactor vessel;
- Counter-current natural circulation flow within RCS piping and steam generators (PWRs);
- Heat transfer to the RCS pressure boundary including cumulative damage leading to creep rupture (at locations such as hot leg nozzles, pressurizer surge lines and steam generator tubes).

Reactor vessel failure and debris relocation to containment

- Energetic fuel–coolant interactions within the reactor vessel lower head (an alternative to quenching), resulting in steam explosion;
- Reheating of quenched core debris in lower head and molten pool formation;
- Cumulative thermal damage to reactor vessel lower head leading to creep rupture;
- Local pouring of molten material onto lower head surface leading to jet impingement, possible plugging and failure of lower head penetration;
- Relocation of molten materials and particulate debris from lower head to containment floor;
- In-vessel debris configuration and coolability.

Energetic phenomena accompanying vessel failure

- High pressure melt ejection, debris fragmentation and dispersal in the containment atmosphere;
- Hydrogen generation, ignition and combustion;
- Direct containment heating;
- Energetic fuel–coolant interaction on containment floor and ex-vessel steam explosion;
- Direct impingement of ejected core debris on thin (steel) containment boundary structures;
- Reactor pressure vessel reaction forces and movement accompanying vessel failure.

Ex-vessel behaviour of core debris (long term)

- Corium–concrete interactions (non-condensable gas and steam generation, concrete ablation and accompanying changes to corium properties);
- Heat transfer and damage to containment pressure boundary due to direct contact with debris;

- Basemat penetration;
- Ex-vessel debris configuration and coolability.

Containment response

- Steam and non-condensable gas accumulation and resulting changes in containment pressure;
- Hydrogen stratification or mixing, as appropriate;
- Thermodynamic effects of operation of containment sprays, coolers and pressure suppression systems (along with other systems represented in the PDS definitions);
- Ignition and burning of combustible gases (including diffusion flames, deflagrations and detonations, as appropriate);
- Containment failure due to overpressure or overtemperature conditions.

REFERENCES

[1] OECD NUCLEAR ENERGY AGENCY, Regulatory Approaches to PSA, Report of a Survey of National Practices, Rep. NEA/CNRA/R(95)2, OECD/NEA, Paris (1995).

[2] OECD NUCLEAR ENERGY AGENCY, Review Procedures and Criteria for Different Regulatory Applications of PSA, Rep. NEA/CNRA/R(97)5, OECD/NEA, Paris (1997).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, IPERS Guidelines for the International Peer Review Service, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, IAEA-TECDOC-832, Vienna (1995).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) — Level 1, IAEA-TECDOC-1135, Vienna (2000).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulatory Review of Probabilistic Safety Assessment (PSA) Level 2, IAEA-TECDOC-1229, Vienna (2001).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Review and Assessment of Nuclear Facilities by the Regulatory Body, Safety Standards Series No. GS-G-1.2, IAEA, Vienna (2002).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2002).

[8] 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).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, Vienna (1993).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA-TECDOC-648, Vienna (1992).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Defining Initiating Events for Purposes of Probabilistic Safety Assessment, IAEA-TECDOC-719, Vienna (1993).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Initiating Events for PSA for WWER Reactors, IAEA-TECDOC-749, Vienna (1994).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Living Probabilistic Safety Assessment (LPSA), IAEA-TECDOC-1106, Vienna (1999).
[18] OECD NUCLEAR ENERGY AGENCY, State of the Art of Level-1 PSA Methodology, Rep. NEA/CSNI/R(92)18, OECD/NEA, Paris (1993).
[19] UNITED STATES NUCLEAR REGULATORY COMMISSION, Probabilistic Safety Analysis: Procedures Guide, Rep. NUREG/CR-2815 BNL-NUREG-51559, Rev. 1 (2 Vols), Brookhaven Natl Lab., USNRC, Washington, DC (1985).
[20] NYMAN, R., HEGEDUS, D., TOMIC, B., LYDELL, B., "Reliability of piping system components", Framework for Estimating Failure Parameters from Service Data, SKI Rep. 97:26, Swedish Nuclear Power Inspectorate, Stockholm (1997).
[21] UNITED STATES NUCLEAR REGULATORY COMMISSION, An Approach for Plant-Specific Risk-Informed Decision Making Inservice Inspection of Piping, USNRC, Washington, DC (1998).
[22] OECD NUCLEAR ENERGY AGENCY, Critical Operator Actions: Human Reliability Modeling and Data Issues, Rep. NEA-CSNI-R(98)1, OECD/NEA, Paris (1998).
[23] HANNAMAN, G.W., SPURGIN, A.J., Systematic Human Action Reliability Procedure (SHARP), Rep. EPRI-NP-3583, Electric Power Research Institute, Palo Alto, CA (1984).
[24] SWAIN, A.D., GUTTMAN, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Rep. NUREG/CR-1278, United States Nuclear Regulatory Commission, Washington, DC (1983).
[25] HANNAMAN, G.W., SPURGIN, A.J., LUKIC, Y.D., JOKSIMOVICH, V., WREATHALL, J., Human Cognitive Reliability Model for PRA Analysis, NUS Rep. (Draft) NUS–4531, Electric Power Research Institute, Palo Alto, CA (1984).
[26] EMBREY, D.E., et al., SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement, Rep. NUREG/CR-3518, United States Nuclear Regulatory Commission, Washington, DC (1984).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Modelling and Data Prerequisites for Specific Applications of PSA in the Management of Nuclear Plant Safety, IAEA-TECDOC-740, Vienna (1994).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-508, Vienna (1989).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Implications of Computerized Process Control in Nuclear Power Plants, IAEA-TECDOC-581, Vienna (1991).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Computerized Control and Protection Systems, IAEA-TECDOC-780, Vienna (1994).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Reliability of Computerized Safety Systems at Nuclear Power Plants, IAEA-TECDOC-790, Vienna (1995).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues for Advanced Protection, Control and Human–Machine Interface Systems in Operating Nuclear Power Plants, Safety Reports Series No. 6, IAEA, Vienna (1998).
[33] HEALTH AND SAFETY EXECUTIVE, The Use of Computers in Safety-critical Applications, Final Report of a Study Group on the Safety of Operational Computer Systems, HSE Books, London (1998).

[34] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, IEC 880, IEC, Geneva (1986).
[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Reports Series No. 10, IAEA, Vienna (1998).
[36] UNITED STATES NUCLEAR REGULATORY COMMISSION, PRA Procedures Guide — A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants, Rep. NUREG/CR-2300 (2 Vols), USNRC, Washington, DC (1983).
[37] ELECTRIC POWER RESEARCH INSTITUTE, MAAP 3.0B Computer Code Manual, Vols 1 and 2, EPRI-NP-7071-CCML, Palo Alto, CA (1990).
[38] GAUNTT, R.O., et al., MELCOR Computer Code Manuals: Version 1.8.4, Rep. NUREG/CR-6119, Vols 1 and 2, Rev. 1, SAND97-2398, Sandia Natl Labs, Albuquerque, NM (1997).
[39] GAUVAIN, J., et al., ESCADRE Mod 1.0 — JERICHO: Reactor Containment Thermal-hydraulics During a Severe Accident — Reference Document, Rep. IPSN/DRS/SEMAR/96-06, Fontenay-aux-Roses (1996).
[40] KAJIMOTO, M., et al., "Development of THALES-2, a computer code for coupled thermal-hydraulics and fission product transport analysis for severe accidents at LWRs and its application to analysis of fission product revaporization phenomena", paper presented at Int. Top. Mtg on Safety of Thermal Reactors, Portland, 1991.
[41] BRINSON, D.A., et al., Evaluation of Seals for Mechanical Penetrations of Containment Buildings, Rep. NUREG/CR-5096, SAND88-7016, Sandia Natl Labs, Albuquerque, NM (1988).
[42] UNITED STATES NUCLEAR REGULATORY COMMISSION, Reassessment of the Potential for an α-Mode Failure and Review of the Current Understanding of other FCI Issues, Rep. NUREG-1529, USNRC, Washington, DC (1996).
[43] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, Rep. NUREG-1150 (Vols 1 and 2), USNRC, Washington, DC (1990).
[44] PILTCH, M.M., YAN, H., THEOFANOS, T., The Probability of Containment Failure by Direct Containment Heating in Zion, Rep. NUREG/CR-6075, Sandia Natl Labs, Albuquerque, NM (1994).
[45] SOFFER, L., et al., Accident Source Terms for Light Water Nuclear Power Plants, Rep. NUREG-1465, United States Nuclear Regulatory Commission, Washington, DC (1995).

LIST OF ABBREVIATIONS

ABWR	Advanced boiling water reactor
APETs	Accident progresssion event trees
APWR	Advanced pressurized water reactor
BWR	Boiling water reactor
CCDFs	Complementary cumulative distribution functions
CDF	Core damage frequency
CETs	Containment event trees
ECCS	Emergency core cooling system
EOPs	Emergency operating procedures
FMEA	Failure modes and effects analysis
HAZOP	Hazards and operability studies
HCR	Human cognitive reliability
HEP	Human error probability
HHSI	High head safety injection
HRA	Human reliability assessment
I&C	Instrumentation and control
LERF	Large early release frequency
LOCA	Loss of coolant accident
LPIS	Low pressure injection system

MCR	Main control room
MGL	Multiple Greek letter
PDS	Plant damage state
pga	Peak ground acceleration
PORV	Power operated relief valve
POS	Plant operating state
PRA	Probabilistic risk analysis/assessment
PSA	Probabilistic safety assessment
PWR	Pressurized water reactor
QA	Quality assurance
RCP	Reactor coolant pump
RCS	Reactor coolant system
RHR	Residual heat removal
SGTR	Steam generator tube rupture
SHARP	Systematic human actions reliability procedure
SLIM	Success likelihood index method
SPSA	Shutdown PSA
THERP	Technique for human error rate prediction
WWER	Water moderated, water cooled reactor

CONTRIBUTORS TO DRAFTING AND REVIEW

Areia Capitão, J.J.	European Commission, Belgium
Blackburn, T.	Battelle, United States of America
Boneham, P.	Enconet Ltd, Austria
Campbell, J.F.	Nuclear Installations Inspectorate, United Kingdom
Castillo Álvarez, J.P.	National Centre for Nuclear Safety, Cuba
Cazzoli, E.G.	ERI Consulting and Co., Switzerland
Choi, J.S.	Korea Institute of Nuclear Safety, Republic of Korea
Choubeiko, E.	Scientific and Engineering Centre on Nuclear and Radiation Safety of the Regulatory Authority of Russia, Russian Federation
Gómez Cobo, A.	International Atomic Energy Agency
Gryffroy, D.G.J.M.	AIB-Vincotte Nuclear, Belgium
Hajra, P.	Atomic Energy Regulatory Board, India
Hirano, M.	Nuclear Power Engineering Corporation, Japan
Jordan Cizelj, R.	Jožef Stefan Institute, Slovenia
Kafka, P.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Kajimoto, M.	Nuclear Power Engineering Corporation, Japan
Kaufer, B.	OECD Nuclear Energy Agency
Koley, J.	Atomic Energy Regulatory Board, India
Kopustinskas, V.	Lithuanian Energy Institute, Lithuania
Kornfeld, C.	Nuclear Research Center — Negev, Israel
Kovács, Z.	Relko Ltd, Slovakia

Labatut, M.	Commissariat à l'énergie atomique, France
Landelius, M.	OKG AG, Sweden
Lantarón, J.A.	Consejo de Seguridad Nuclear, Spain
Lederman, L.	International Atomic Energy Agency
Lele, H.G.L.	Bhabha Atomic Research Centre, India
Leonard, M.	Dycoda Consulting, United States of America
López-Morones, R.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Mexico
Niehaus, F.	International Atomic Energy Agency
Patrik, M.	Nuclear Research Institute Řež plc, Czech Republic
Prior, R.P.	Westinghouse Electric Europe, Belgium
Pschowski, J.	ESI Energie–Sicherheit–Inspektion GmbH, Germany
Ranguelova, V.	International Atomic Energy Agency
Reer, B.	Paul Scherrer Institute, Switzerland
Rogers, P.	Rolls Royce plc, United Kingdom
Schueller, G.I.	Institute of Engineering Mechanics, Austria
Sepanloo, K.	Atomic Energy Organization, Islamic Republic of Iran
Serbanescu, D.	National Commission for Nuclear Activities Control, Romania
Serrano, C.	Iberdrola Ingeniería Consultoría, Spain
Shapiro, H.	Atomic Energy of Canada Ltd, Canada
Shepherd, C.H.	Nuclear Installations Inspectorate, United Kingdom
Sholly, S.	Institute of Risk Research, Austria

Spitzer, C.	TÜV Energy and Systems Technology, Germany
Svirmickas, S.	Lithuanian State Nuclear Power Safety Inspectorate, Lithuania
Szirmai, S.	Hungarian Atomic Energy Authority, Hungary
Talieu, F.P.D.	Electricité de France, France
Vallerga, H.R.	Autoridad Regulatoria Nuclear, Argentina
Villadoniga, J.	Consejo de Seguridad Nuclear, Spain
Vitazkova, J.	Nuclear Regulatory Authority, Slovakia
Vojnovic, D.	Slovenian Nuclear Safety Administration, Slovenia
Willers, A.	Australian Nuclear Science and Technology Organisation, Australia
Yllera, J.	Consejo de Seguridad Nuclear, Spain
Zeng, Y.	Atomic Energy Control Board, Canada

Technical Committee Meeting

Vienna, Austria: 26–30 June 2000

Consultants Meeting

Vienna, Austria: 5–9 February 2001