IAEA-TECDOC-1135

Regulatory review of probabilistic safety assessment (PSA) Level 1

Prepared jointly by the International Atomic Energy Agency and the OECD Nuclear Energy Agency

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

February 2000

The originating Section of this publication in the IAEA was:

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

REGULATORY REVIEW OF PROBABILISTIC SAFETY ASSESSMENT (PSA)
LEVEL 1
IAEA, VIENNA, 2000
IAEA-TECDOC-1135
ISSN 1011–4289

Printed by the IAEA in Austria
February 2000

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 the PSAs are being used along with those from the deterministic analysis.

Many regulatory authorities consider that the current state of the art in 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 regulatory authorities to have a high degree of confidence in PSA. However, at the IAEA Technical Committee Meeting on 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 formal regulatory review guidance for PSA did not exist. The senior regulators noted that there was a need to produce some 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 technical document on the regulatory review of PSA.

This publication is intended to provide guidance to regulatory authorities 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 document gives guidance on how to set about reviewing a PSA and on the technical issues that need to be addressed.

This publication gives guidance for the review of Level 1 PSA for fault sequences occurring at full power only. It is intended that further work will be carried out in the future to extend the coverage of the document to fault sequences occurring at low power and shutdown states, and for Levels 2 and 3 PSA.

The IAEA appreciates 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 officers responsible for this publication were V. Ranguelova and F. Niehaus of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

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:

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

At present, over 200 PSAs have been produced worldwide. All of them have been done to Level 1 to provide an estimate of the core damage frequency. 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 between different countries. The emerging standard in the last few years is for performing Level 2 PSAs. At present, relatively few Level 3 PSAs have been completed.

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

— to provide insights from the risk analysis to supplement those obtained from the deterministic safety assessments,
— to identify weaknesses in the design and operation of the plant,
— to estimate the risk from the plant for comparison with risk criteria, and
— to provide an input into the plant specific applications such as the optimization of technical specifications and accident management, and operational uses such as maintenance planning.

The scope of the PSAs that have been carried out also vary. They have all addressed initiating events occurring at full power and, in some cases, this has been extended to address low power and shutdown states. In addition, they have all addressed internal events and, in some cases, this has been extended to address internal hazards such as fire and flood and external hazards such as earthquake and aircraft crash.

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

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 analysis which has traditionally been carried out. The insights gained from the PSA are being considered along with those from the deterministic analysis to make decisions about the safety of the plant. Additionally, many regulatory authorities consider that the current state of the art in 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 authority (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 consultants 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 authorities to move towards a more risk informed approach to their activities, it was found that there is 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 to a specific purpose — for example, the International Peer Review Service (IPERS) 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 was 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 conclusions reached are appropriate. This publication is the result of a co-operative arrangement between IAEA and NEA.

1.2. REGULATORY REVIEW OF PSA

The PSAs that are currently produced provide unique insights into the way initiating events and safety systems interact and give an overall picture of plant behaviour. These insights are of value to both the plant operators and the regulatory authority.

This increasing use of PSA has led to the realization that the production and use of a PSA requires substantial efforts by both the utility and the regulatory authority to carry out and review them. In addition, there is a need to provide knowledge and training to personnel in the use of these methods.

Inherent in the production and review of a PSA is the ability of those involved to determine what is acceptable. As industry further develops the use of PSA in justifying plant changes and modifications, the regulatory authority and other agencies need to understand how the PSA has been produced in order to be able to assess its applicability in the decision making process. The review process becomes an extremely important phase in determining the acceptability since this provides a degree of assurance of the scope, validity and limitations of the PSA, as well as a better understanding of the plant itself. This is becoming increasingly important with the advent of a risk-informed regulatory decision making environment.

Additionally, utility involvement is important, since the prime responsibility for the safety of the plant rests with the utility and not with the regulatory authority. Therefore, motivation exists on the part of both the regulatory authority and the utility to ensure that PSAs are performed adequately.

In preparing this report, it is recognized that differences exist between countries in the way that the nuclear industry is organized — including the utilities, operators, designers and manufacturers. In this report, the term "utility" is used and is taken to encompass the industry as a whole. In addition, there are differences in the way a regulatory authority operates in that, in some countries, it is completely within the governmental system while, in others, it is outside government but responsible to or licensed by it. These differences are reflected in the way that the PSAs are produced and reviewed in different countries.

The review of the PSA may be performed by the regulatory authority alone or with outside consultants or even in some cases with the help of international peer reviews. The guidance provided covers all these possibilities.

1.3. SCOPE OF THE REPORT

This publication provides recommendations on how to carry out the regulatory authority review of a PSA produced by a utility. By following the guidance given, the regulatory authority should be 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.

At this stage, detailed guidance is given for the review of Level 1 PSA only for event sequences occurring during full power operation. However, since most regulators would expect the Level 1 PSA to be continued into a Level 2, or at least to retain this option, the report also covers the Level 1/Level 2 PSA interface. This interface, in the form of plant damage states and their frequencies, would also provide the basis of a Level 1+ PSA, and can, of itself, give some useful insights into the safety of the plant, to supplement those from the Level 1 PSA. Thus the document assumes that a Level 2 PSA will subsequently be performed, but can, of course, be readily adapted to the case where only a Level 1 PSA is required or intended. It is intended that further work be carried out in the future to extend the coverage of the document to provide review guidance for event sequences occurring at low power and shutdown states, and for Level 2 and 3 PSA.

Recommendations are given on carrying out the review of a PSA throughout the PSA production process — that is, 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 in progress.

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

1.4. STRUCTURE OF THE REPORT

This report gives key recommendations for carrying out the regulatory review of a PSA.

Section 2 gives guidance how the regulatory authority should carry out the review of a PSA. This addresses issues such as when the review may be 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 the review of a Level 1 PSA for initiating events occurring at full power. This covers: the identification of initiating events, accident sequence analysis, human reliability assessment, data, quantification of the PSA, and sensitivity studies/uncertainty analysis.

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

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

2. THE REVIEW PROCESS

2.1. INTRODUCTION

This section gives recommendations on the way a regulatory authority may set about reviewing the 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 may be different in different countries. In addition, the approach may also be different depending on the purpose of the review — for example, the 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 review of the aims, objectives and scope of the PSA,
— the review of the methods and assumptions used in the PSA, and
— the review/ audit of the utility's PSA production process.

2.2. APPROACH TO THE REVIEW

2.2.1. Timing of the review

The review carried out by the regulatory authority can be an on-line review or an off-line review depending on the time when the review is carried out. An **on-line review** is when the review 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 in the PSA which would 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 starts after the PSA team has presented the final report to the regulatory authority. The advantage of this approach is that the PSA documents are reviewed 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 important to carry out the review in parallel with the production of the PSA (that is, on-line) whenever possible so that the regulatory authority can determine at an early stage that 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 give an earlier date for regulatory acceptance of the PSA (see Section 2.2.8).

The regulatory authority's reviewers may consider necessary to agree on a schedule of work with the utility's PSA team that fits the needs of both organizations, ensures that the review process is conducted efficiently and that any delays in completing the review are minimized. This schedule has to allow for sufficient time and effort to be given to the review of the results (see Sections 3.11 and 3.12), 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 hastened, due to the effort allocated to the review being used up, but it is an essential step

to confirm that the aims and objectives of the PSA have been met, and to provide the level of confidence that the regulatory authority is seeking.

2.2.2. Extent of the review

It is recommended to decide on the extent of the review to be carried out by the regulatory authority 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.

During an **extensive review**, the PSA would be reviewed in considerable detail to make sure that the models and data used are good representations of the actual plant design and operational practices. 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 authority 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 authority are not large enough.

During a **limited review**, the aim would be to ensure that all aspects of the event sequences leading to core damage are modelled adequately and the data used to determine the frequencies of the event sequences is 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 authority but leads to lower levels of learning and confidence. 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 IPERS of the IAEA, which needs to be a limited due to time constraints [3].

In a limited review there is the 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 (see Section 2.2.5).

It is recognized that the practice will be different in different countries. However, it is recommended that the extent of the review is chosen to be sufficient to provide the regulatory authority with the level of confidence it is seeking.

The review should consider whether the scope of the PSA is adequate in that it addresses an adequate range of internal and external initiating events, and operating modes of the plant. (The review recommendations given here only address full power operation).

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

The extent of the review will have to take into account important factors including the level of risk from the plant and the experience with that reactor system.

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

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

The extent of 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 authority may decide to reduce the extent of the review they would carry out, to avoid duplication. However, for many regulatory authorities, the review of the PSA is an excellent source of additional knowledge about the plant design, operation, and safety strengths and weaknesses that, by itself, may justify an extensive review in any case. An extensive review would likely be required if the regulatory authority intended to use the PSA as a basis for risk informed regulation.

2.2.3. Documentation for the review

The documentation for the 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 authority and is the basis for the regulatory review and any uses made of the PSA.

The starting point for the production and review of the PSA is a clear definition of the design of the plant and how it will be operated. This will normally be a frozen 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. It is recommended, in such cases, that a PSA be performed for both the states, before and after, so that the reduction in risk can be evaluated. Sufficient information available is essential to allow the reviewers to become familiar with the design and operation of the plant and this may be combined with plant visits as required. This would include systems descriptions, operating procedures, test and maintenance procedures, accident management procedures, etc. Sources of plant information which are typically used for plant familiarization are given in Table III of Ref. [4].

Sufficient documentation is to be provided/made available to the reviewers to describe the PSA, including the analysis methods and data, supporting analysis (such as the transient analysis to support the safety system success criteria). It is important that this is in sufficient detail to allow the analysis to be traced (or repeated, if necessary). A more detailed information on the content of a PSA report can be found in Appendix VIII of Ref. [4]. Further information on typical documentation to be included for each task of the PSA can also be found in Ref. [5].

It is recommended that the regulatory authority agree with the utility on the format and content of the PSA documentation before the start of the PSA. This will ensure that quality assurance (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 is to be used for many applications and will require updating. The documentation should be completely traceable.

One of the reviewers' first tasks is to check that the PSA documentation submitted generally corresponds to the items described in the above references. 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:

— the information on the design and operation of the plant has been clearly documented,
— the methodologies used for performing the different PSA tasks (as identified in Section 3) have been clearly documented and would allow the analysis to be repeated without additional information from the PSA team,
— the supporting analyses (including thermal-hydraulic analyses for justifying system success criteria) are either included in the PSA documentation or are available for consultation by the reviewers,
— all tables, figures and appendices have been provided,
— there are adequate references to supporting literature, and
— all the information provided is consistent with the PSA freeze date.

The reviewers have to confirm that the utility has documented the PSA in a manner that helps the comprehension and review of the PSA.

It is considered a 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 would allow the reviewers:

— to use the PSA as a basis for risk informed regulation,
— to search for specific information in the model,
— to perform spot checks on the model and its quantification,
— to carry out importance analysis to identify the areas of the PSA on which the review should be focused, and
— to carry out their own sensitivity studies to determine how changes in assumptions can affect the results of the PSA.

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

2.2.4. Setting up the review team

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

It is important that the review team be experienced in the techniques for carrying out state of the art-the-art PSAs. The range of expertise should 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 authority. Where necessary, additional training may be required and provided.

It is good practice that the review team includes experts with experience of deterministic analysis. This offers the advantage of aiding the regulatory authority 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 the free exchange of documentation and easy discussions. However, in setting up and carrying out the review, care has to be taken to ensure that the independence of the regulatory authority is not compromised.

2.2.5. Identification of/focus on important issues

It is highly recommended to focus the work of the reviewers on the areas of the PSA which have the most significant impact on the results of the PSA. This would include the PSA topics addressed in Section 3 and the initiating events, system/component failures, etc. which have the highest risk significance.

The reviewers should 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 analysis 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.

2.2.6. Comparison with other PSAs

The review carried out may include a comparison of the methods used and the results of the PSA with other PSAs for similar plants where possible. It is the practice in many countries to use a previous, state of the art, PSA as a reference for the review of a new PSA.

The reviewers may consider useful to compare the results of the PSA — that is, core damage frequency, dominant sequences and their initiators, dominant systems, etc., with the results of the PSAs of similar plants. However, if there are differences in design among the plants compared, neither the similarity, nor the lack of similarity, of the results is a clear indication of correctness or incorrectness of the PSA, but it can stimulate the thinking about areas to review in more detail.

Where there are several methodologies available to carry out the same part of the analysis, it is important that the regulatory authority clearly point out to the PSA team which of them it would consider to be totally or partially unacceptable to avoid resources being used in carrying out work that would be considered inadequate later on.

2.2.7. Reworking of the analysis by the regulatory authority

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

The practice varies between the regulatory authorities in different countries from doing virtually no reworking of the analysis to carrying out whole PSAs themselves — either in-house or by using consultants. If consultants option is retained, it is important that the consultants work in close consultation with the 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 — should be considered to give the reviewers confidence that the mechanics of the PSA have been correctly handled.

2.2.8. Documentation of the review findings

The reviewers are advised to document the findings of the work they have carried out in a final PSA review report. The format, content and structure of this report will depend to a great extent on the national practices and the scope of the review. Some general recommendations are given below on items and issues to be included in a final report.

The final PSA review report usually contains 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 final PSA review report also contain 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 is also to be provided. This would include all issue lists (questions, answers and resolutions) if they were used in the review process and would highlight any issues still open.

The final PSA review report will contain final conclusions on the adequacy of the PSA including the PSA results, uncertainties and sensitivity studies. Problem areas should be identified and explained.

The final PSA review report may contain recommendations, if any, 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. This 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 final PSA review 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 complete the review in a short time after the presentation of the PSA report. If the review process is offline, 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 should be done in accordance with the QA requirements.

2.2.9. Interactions with the utility

It is important that the reviewers agree with the utility on how to conduct the interactions between the two parties and with 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 sanctions of the law in the background. The reviewers, with their regulatory role in mind, are recommended 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 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. The reviewers should also avoid, as a general rule, proposing specific means of resolving their concerns: that is the job of the utility and is part of the process whereby the utility "owns" 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 should, however, be formally confirmed in writing.

The aim of all parties is for a final PSA report for which the utility is content to take full responsibility and which the regulatory authority 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 should ensure that all the significant impacts of the change are reflected throughout the PSA and its documentation, so that it is all consistent, even if this means repeating the whole of the numerical evaluation and the review of the dominant components, sequences etc. It is necessary also to ensure that all points of clarification, including those dealt with informally, have been satisfactorily incorporated into the final PSA report; one should bear in mind that this report, or its future updates, will be expected to 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 to communicate the reviewers' 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 them a copy of the review report. They may send only the findings, extracted from the report, 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 should be careful to distinguish their role in these activities from that as PSA reviewers. It is the job of the utility to formulate the programme of plant changes, to obtain regulatory approval and to implement it, ensuring that the changes have no negative impacts on the deterministic safety analysis. It is necessary for the utility to evaluate also 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 authority will review the utility's safety assessments of the changes, which will include reviewing the PSA aspects, and will monitor their implementation.

The regulatory authority usually encourages the utility to use the PSA as widely as possible during the operation of the plant (see Section 2.3.3), to maintain a PSA team which is capable of doing this, and to keep the PSA up to date.

2.2.10. Research

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, reducing conservatism. This would include the research to support the development of PSAs in general (for example, to improve the modelling capabilities of the PSA) and the research to investigate the issues which arise out of the review of a particular PSA (for example, to provide better information on particular event sequences which allows some of the conservatisms to be removed from the PSA). The reviewers usually draw any such research topics to the attention of the regulatory authority 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 authority and the utility which aims to identify technical areas that may be controversial and fund research or pilot activities aiming at developing the criteria or methods to be used.

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

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 authority, in terms of a requirement or recommendation, a voluntary decision by the utility, or may arise by some other means — for example, as a result of a government inquiry. Either way, if the PSA is going to be presented to the regulatory authority 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 the PSA

It is recommended that the regulatory authority set down the standards which will be used to assess the acceptability of the PSA and make these clear to the utility.

It is considered very important that, before the start of the PSA, both the regulatory authority and the utility be 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 documents covering the performance of Level 1, Level 2 and Level 3 PSAs [4, 6, 7] and documents covering specific aspects of PSA including the treatment of external events [8], PSA for seismic events [9], common cause failure analysis [10], defining initiating events [11, 12] and human reliability analysis [13].

2.3.2. Aims and objectives of the PSA

The regulatory authority may find useful to set down what it considers the aims and objectives of the PSA. These should 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, these may be set down and their interpretation and implications for the PSA agreed. A target for large release frequency will demand a Level 2 PSA. If the criteria are based on non-nuclear risks in society, they will be absolute values and the PSA will need to be as complete as possible (for example, it will include all hazards and all plant states) for a valid comparison to be made. If there are targets aimed at showing that the risk has been reduced from the levels determined by previous PSAs, then they will be relative values and a more limited scope of PSA may suffice. In this publication, it is assumed that the aim is to produce a state of the art Level 1 PSA which is to be continued eventually as a Level 2 PSA. (Proceeding to Level 3 does not affect the Level 1 PSA.)

As with any review of the design, it is recognized that the PSA and its review may lead to requirements for changes in the design — and the project schedule should allow for this possibility. The PSA is not to be regarded as simply providing confirmation that the design as put forward is acceptable from a risk point of view.

2.3.3. Scope and applications of the PSA

It is good practice for the regulatory authority to set down the scope of the PSA that it would expect the utility to carry out. This should be compared with what the utility has proposed and an agreement reached.

The specification for the scope of the PSA usually includes:

— the range of internal and external initiating events to be addressed by the analysis (internal initiators such as transients and LOCA, internal hazards such as fire and flood, and external hazards such as earthquake and aircraft crash),
— the modes of operation of the plant to be addressed by the analysis (full power operation, low power operation, shutdown states),
— whether modelling of cognitive errors will be attempted in the human reliability analysis,

— whether recovery actions and accident management measures (to prevent core damage) are to be taken into account for accident situations beyond the design basis,
— whether post-trip repair and return to service of failed systems/components is to be taken into account,
— 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,
— the range of sensitivity studies that need to be carried out (data, modelling assumptions),
— whether an uncertainty analysis is required,
— the level of the PSA required (Levels 1, 2 and 3 are defined in Section 1; only Level 1 is addressed in this report), and
— the main results of the PSA that are to be presented — for example, core damage frequency, dominant accident sequences or cut-sets, importance measures.

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

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 address the scope of the analysis. The detailed review of the technical issues is addressed 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.

A PSA has many potential applications beyond satisfying the immediate objectives of identifying design weaknesses and addressing risk targets/criteria, referred to in the preceding section. The regulatory authority 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 “standard” PSA, as covered in this guidance, but others, particularly operational uses such as maintenance planning, require the special characteristics of a living PSA [14], such as explicit modelling of each train and separate initiating events for each loop. The range of PSA applications could include, for example:

— optimization of the technical specifications,
— identification of accident management measures,
— determining the change to the risk from the effects of ageing,
— control of equipment outages for maintenance,
— support for plant modifications,
— risk-based evaluation of operational events, or
— graded QA.

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, and the level of detail in the component modelling. The reviewers are advised to check that the scope is adequate for the intended applications. Approximations and simplifications which are acceptable for the standard 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.

2.4. REVIEW OF METHODS AND ASSUMPTIONS

2.4.1. State of the art

The reviewers usually determine the standard of the PSA that the regulatory authority 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 reasonable improvements over previously existing methods.

It is recognized that PSA methods are evolving. However, it is important that both the regulatory authority and the utility determine what the state of the art is in PSA and this should be agreed between both parties. A review of the state of the art in Level 1 PSA (1993) was carried out by the Committee on the Safety of Nuclear Installations (CSNI) [15].

2.4.2. Level of detail

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

The reviewers should 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 (for example, 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 will 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 should be structured so that it can be readily adapted.

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 dependencies may be missed if the level of detail is not enough to uncover them. It is a good practice to reach a level that provides assurance that all significant dependencies are included in the model.

It is necessary for the reviewers to determine the level of detail that the regulatory authority 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

It is necessary for the reviewers 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 Section 3 on the various aspects of the PSA.

The reviewers will ideally identify the state of the art methods and tools for each task, and then will 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 significantly underestimating the risk or to invalidating the PSA for one of its uses.

2.4.4. Sources of data

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

The reviewers should 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 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 is acceptable. The data should preferably be best estimate, appropriate for the use made of it in the PSA and cover all the causes of the failure which could occur, with the uncertainties identified. Further guidance on data is given in Section 3.

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

With the aim of best estimates throughout the PSA, it is important to check that the conservatisms present are not so great that they lead to an unacceptable bias and distortion in the results of the PSA. This will be largely 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 — that is, where the PSA is based on point values alone, all the values and assumptions input should represent best estimates of the mean values, and not, for example, of the median, 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 and percentiles) should always 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.

2.4.6. Validation and verification of computer codes

The computer codes used in the PSA are to be validated and verified. In this context, **validation** is defined as providing the theoretical examination to demonstrate that the calculational methods used in the computer code are fit for purpose and **verification** is defined as ensuring that the controlling physical and logical equations have been correctly translated into computer code.

It is necessary for the reviewers to determine whether the codes which have been selected by the PSA team are fit for purpose and that the users of the codes are experienced in their use and fully understand their limitations. It is recommended that the regulatory authority 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 authority may also carry out a review/audit of the utility's PSA production process and the procedures being used. The reason for this is 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 are recommended 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 Section 3, 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 usually 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 authority. Alternatively, the procedures followed for an already approved PSA can be used.

2.5.2. Quality assurance

One of the reviewers' tasks is to determine whether the utility has QA arrangements in place for the production of the PSA. Some guidance on QA procedures for a PSA are given by the IAEA [4] and the United States Nuclear Regulatory Commission [16]. In addition, the IAEA is preparing a technical document on a framework for a quality assurance programme for PSA.

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 to be carried out. The existence of such an independent peer review may allow for a reduction of the extent of the review carried out by the regulatory authority.

2.5.3. Organization of the PSA production team

In connection with the organization of the PSA production team, the reviewers usually determine whether:

— the utility has assembled a team with sufficient depth and breadth of experience to enable the efficient production of the PSA,
— the composition of the utility PSA team is in line with the PSA procedures established by the utility,
— the PSA team is under the direction of utility personnel,
— the PSA team includes representatives from the plant operating staff,
— where external consultants are used, they are fully integrated into the PSA team,
— the utility personnel are fully aware of the PSA methods and techniques being used and of their strengths and limitations,
— training is provided for the less experienced members of the PSA team,
— all the members of the PSA team work within the procedures provided and the QA arrangements, and
— the arrangements are in place to check the PSA as it is being produced and to carry out an independent peer review of the PSA.

2.5.4. Future updating/development of the PSA

It is necessary for the reviewers to check that the PSA is being produced and documented in a way that makes it easy to update and to extend its use to other applications. The PSA report should 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 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 authority.

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

3. CONDUCTING THE LEVEL 1 REVIEW

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 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, and
— 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 communicates with 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. [4].

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 should occur.

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

— analytical methods such as hazards and operability studies (HAZOP) or failure modes and effects analysis (FMEA),
— deductive analyses such as master logic diagrams,
— comparison with the lists of initiating events developed for the PSAs for similar plants and with existing guidelines, and
— 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 (see Section 2.3.3) the set of initiating events identified will include internal initiating events (such as loss of coolant accidents (LOCAs), and transients), internal hazards (such as fire, explosion and flooding of internal origin) and external hazards (such as earthquake, aircraft crash and flooding of external origin). (The identification of internal and external hazards is discussed in Section 3.9). Loss of grid (off-site AC power) should always be included, conventionally classed as an internal event, and specified stepwise in terms of the duration of loss.

The set of initiating events identified should be 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 should be 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 use of operational experience) addressed in the PSA, together with some analytical approach. The reviewers are recommended to 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 is supposed to be 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 (for example, rupture of the reactor pressure vessel) it is recommended 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 is also to be paid to the potential radiological consequences; low frequency events with potentially high consequences should not be screened out.

For twin or multiple unit sites, some safety systems may be shared or cross-tied. In this case, the reviewers should check that those initiating events that can affect both units (for example, loss of grid and most external events) have been identified and the PSA takes account of the shared systems that 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, and this event should have been identified, even though it may be screened out later after analysis. It is possible that interconnections between units could be a mean of an accident on one unit giving rise to an initiating event on another. This is unlikely to be the case on a well engineered plant, but the reviewers may consider it necessary to check this point.

The set of initiating events considered in the PSA may be compared with that for similar plants to ensure that any relevant initiating events have been included. Where differences are identified, additional initiating events may be defined or justification provided on 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 (see Section 3.2), some initiating events can be grouped together for further analysis in the same event tree.

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

Where initiating events with slightly different accident progression and/or success criteria for the mitigating systems have been grouped together, the reviewers need to 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 should satisfy themselves that this does not introduce undue conservatism into the analysis.

The initiating events which cause a containment bypass (for example, steam generator tube rupture) should 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 would typically include the following:

— increase in reactor heat removal (for example, opening of secondary relief valves or steam line breaks),
— decrease in reactor heat removal (for example, loss of main feed or feed line breaks),
— decrease in reactor coolant system flow rate (for example, reactor coolant pump trip, pump seizure or shaft break),
— reactivity and power distribution anomalies (for example, uncontrolled control rod withdrawal, control rod ejection or boron dilution),
— increase in reactor coolant inventory (for example, inadvertent operation of the emergency coolant injection system), and
— decrease in reactor coolant inventory (for example, LOCAs due to primary relief valves opening or primary pipework leakages and including interfacing systems LOCAs).

The reviewers are recommended to look for the lesser events within any category as well as the extreme ones, since these are often much more frequent and can make a greater contribution to the risk. In the first two categories above, for example, a turbine control malfunction or trip would be more frequent than a major line break.

LOCAs

For 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. This is based on actual design and layout of the plant and includes failures of valves and, in particular, relief valves.

The LOCAs identified are usually categorized and grouped according to the success criteria of the safety systems required to operate to prevent or limit core damage.

For LOCAs in the reactor coolant system piping, the reviewers should 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 for very small LOCAs such as reactor coolant pump seal failure.

The success criteria for the LOCA groups are to 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 systems 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.

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:

— steam generator tube ruptures,
— loss of secondary cooling through loss of feedwater, loss of condenser vacuum,
— spurious operation of systems which are not present in other plants of the same, and
— loss of the main heat sink (for example, 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 feedwater line breaks, should be considered as special types of transients.

Plant specific operating experience needs consideration to identify any plant specific transients which need to be considered in the PSA.

Loss of a support or a supply systems should 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 awareness 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 (alternating current) or DC (direct current) bus,
— loss of instrument air,
— loss of component cooling and service water, and
— loss of room cooling.

The identification of events related to loss of support systems should not only consider support functions to mechanical components, but also to instrumentation and control (I&C) systems (solid state components), including the reactor protection system.

Loss of grid/station blackout

Loss of grid (loss of 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 (for example, the frequency of loss of grid should exclude the frequency of blackout) and no omission.

The duration of loss of grid (and more particularly of station blackout) can be critical to the development of the accident sequences, since some plants may have weak defences against a prolonged blackout. The frequency of loss of grid should therefore 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, based on records of grid loss in the area and taking account of any site specific factors such as redundancy of grid lines or susceptibility to storm damage. The different durations of loss may be treated in the PSA as different initiating events (analogous to different LOCA sizes) or, alternatively, the restoration of AC power at the 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 must 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 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 should be clear interfaces between the structure of the event trees and the database analyses. There should also be clear connections in the event trees between the duration of blackout and 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. This identifies the event sequences 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. It is helpful if this information is tabulated (see Section 3.3.1).

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

It is necessary for the reviewers to 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 core uncovery, to the top of the core or overpressurization and these need to be differentiated for comprehensive analysis. Core uncovery is an acceptable surrogate for core damage if only limited possibilities exist to mitigate core damage after core uncovery 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 core uncovery, then this should be taken into account in framing a realistic definition of core damage.

The safety functions that need to be performed to prevent core damage are 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, containment protection, etc. depending on the nature of the initiating event.

The safety systems available to perform each of these safety functions have to be identified. The success criterion for each system is then determined, as the minimum level of performance required from the system, and 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 or reclose. 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 should identify the operator actions that are required to bring the plant to a safe, stable shutdown state. These are usually identified from the emergency procedures, which should be available at least in outline, or by using an analysis technique such as event sequence diagrams. Good practice is to do this as a co-operative effort between the systems analysts and the 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 which would fail as a result of the initiating event should be identified and this should be 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, electrical power, cooling water, etc. — 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, it is recommended to define realistic success criteria to be used in the PSA based on best estimate transient analysis. This should be preferred to using the conservative success criteria which are addressed in the 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 should be clearly indicated and justified. In addition, the results warrant careful review to ensure that such conservatisms do not 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, it is recommended that the reviewers check the quality of these analyses.

Regarding the computer codes used to define the success criteria, the reviewers may consider necessary to check that:

— 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,
— both the computer codes and the code users have been subject to quality assurance procedures. The analyses have been performed only by qualified code users. A record documenting the qualification is available,
— 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. The codes used contain at least the modelling detail present in codes such as RELAP [17], TRAC [18], CATHARE [19], ATHLET [20] and DYN 3D/M2 [21],
— 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, check and verification,
— for each case analysed, a sufficient description of input data, basic assumptions, safety system set points and capabilities is provided, and
— all calculations are well documented and the analysis results which are to be used further in the PSA study are well identified.

3.2.2. Event tree analysis

It is necessary for the reviewers to check that the event tree analysis for each of the initiating event groups addresses 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) should form the headings on the event tree, to which should

be added any operator actions, particularly recovery actions, which would directly affect the course of the 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 dependencies 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 should 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 so long as the dependencies are correctly observed. If this cannot be done, an event can appear in two headings, with branching at the appropriate one.

Event tree analyses usually identify and model all the dependencies that can occur due to equipment failures and operator errors. Dependencies 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. Dependencies due to operator errors can occur where an operator action is required before a safety system is able to operate. For example, in particular accident sequences for a PWR, the operator needs to carry out an intentional depressurization of the primary circuit by opening the PORVs before the low pressure ECCS can inject water into the primary circuit. In addition, dependencies can arise due to the operator making mistakes in carrying out the accident management procedures.

The 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 need to 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.

It is important that the PSA documentation contain detailed descriptions of the event trees, the assumptions made, descriptions of the conditions created by the initiating event and the safety system requirements for the different event tree branches. The event tree diagram itself gives no reasoning, only the results of reasoning, and hence cannot be understood completely without reference to an accompanying text. It is necessary for the reviewers 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 where a complex event (such as performing a recovery procedure), or more than one event, are lumped together 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, it is recommended that the reviewers 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 is expected to be determined based on plant specific best estimate thermal-hydraulic 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 operations organization of the plant should have taken part in the estimation process.

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

An example of where a detailed review would be worthwhile is for reactor coolant pump (RCP) seal LOCA for a PWR. This can occur due to the loss of cooling and water injection systems and has been shown to be an important contributor to the risk for some PWR plants. Further guidance on RCP seal LOCA modelling in PSA can be found in Section 2.1.2.1 of Ref. [5].

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

It is necessary for the reviewers to 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 (see Section 3.3.1), the house event descriptions should be reviewed and the interfaces with the respective event trees should be checked.

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

3.2.3. Plant damage states

The next stage of the analysis is that the event sequences identified as leading to core damage need to be grouped into plant damage states (PDSs) which form the interface between the Level 1 PSA and the Level 2 PSA. To do 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 should 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:

— the type of initiating event that has occurred (intact primary circuit or LOCA),
— the safety systems failures which have occurred leading to core damage (reactor protection system, residual heat removal system, ECCS), 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 if the system is rendered non-functional due to high primary circuit pressure; however, there is a big difference in these two cases from a Level 2 perspective,
— the state of the primary circuit pressure (high or low) at the time of core damage,
— 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, bypassed due to a SGTR or an interfacing systems LOCA),
— LOCA with or without pressure suppression (BWRs),
— pool subcooled or saturated when core damage occurs (BWRs),
— the availability of the containment protection systems (containment sprays, heat removal systems, hydrogen mixing/recombiners),
— the availability of AC/DC power and recovery times, and
— the operator actions which have been attempted and failed.

This grouping of event sequences into PDSs is usually done as a co-operative effort between the 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 dependencies 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 timing, pressure etc., giving the frequency of each PDS as output, ready for the Level 2 analysis. Where this approach is taken, the reviewers are recommended to check that the assumptions, simplifications and dependencies 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 should be chosen to present the most severe challenge to the containment, but the variation in severity within the PDS should not be so great that it introduces undue conservatism.

It is necessary for the reviewers to 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. [6].

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, component unavailabilities during periods of maintenance or test, common cause failures of redundant components and operator errors.

3.3.1. Fault tree analysis

It is necessary for the reviewers to 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 should be 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 should describe the dependency 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 fault trees should 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 should be identified by a systematic analysis — for example, a failure modes and effects analysis (FMEA) which may have been carried out as part of the design assessment to identify the important component failure modes, a review of operator actions supported by task analysis to identify potential errors, etc.

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

The hardware dependencies, including the functional dependencies which could arise within systems, are usually identified and modelled explicitly in the fault tree analysis (see Section 3.4.1). It is good practice for the analysts to tabulate all these dependencies in a dependency matrix, which can be used as a basis for constructing the fault trees, and is helpful to the reviewers in checking them. Such dependencies should *not* be included as part of the component failure dependencies included in the common cause failure probabilities of the system. These are reserved for the more uncertain dependencies which have not been explicitly identified and which are quantified by means of beta factors and similar approaches.

The inter-system dependencies which could arise due to shared components are usually 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 should 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 are to be consistent with the available component reliability data. The component boundaries and component failure modes should 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 has to be sufficient to ensure that all the hardware dependencies can be modelled. For example, pump cooling water systems are expected to be explicitly modelled in the fault tree to ensure that the dependencies 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 is available on the whole system and it can be fairly regarded as being independent of other equipment on the plant.

Where components are grouped together into super components, the failure modes of each of the elements should have the same effect on the system. In addition, all the super components should be functionally independent in that no component appears in more than one super component, or elsewhere as a basic event.

The support systems for components and subcomponents are usually identified and modelled in the fault trees to ensure that all hardware dependencies 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 to components in the support systems.

The operator errors which can contribute to safety system failure should have been identified and are usually modelled explicitly in the fault trees. The review of the human reliability assessment is discussed in Section 3.6.

The common cause failures which can affect groups of redundant components are usually 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 are usually modelled in the fault trees (see Section 3.4).

The unavailability of individual components or trains of equipment which are taken out of service for periods during the lifetime of the plant for test, maintenance or repair are usually 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 maintenance unavailability should be consistent with the way the system is actually taken out of service for maintenance and with the maintenance unavailability data that is 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 are recommended 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.

One of the tasks of the reviewers is to ensure themselves 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 (see Ref. [4]).

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:

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

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

— all the system components modelled in the fault trees,
— the normal configurations of the components,
— the pipe segments or wiring segments connecting the components, and
— the support system interfaces (power, electrical, cooling, etc.).

The functional descriptions and schematics provided of the safety system need to be sufficiently clear to allow the fault tree 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 identification tables for the instrumentation in each system that identifies 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 are recommended to pay special attention to the treatment of dependencies.

3.4.1. Types of dependencies that can occur

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

— functional dependencies,
— physical dependencies,
— human interaction dependencies, and
— component failure dependencies.

Functional dependencies between safety systems or components can arise when the function of one system or group of components depends on the function of another system or component. These can arise due to a number of causes including the following:

— shared component,
— common actuation systems,
— common isolation requirements, and
— common support systems — power, cooling, indication and control, ventilation.

Functional dependencies 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 trace heating on a section of pipe allows it to freeze in cold weather.

Physical dependencies can arise in two ways. Firstly, an initiating event can cause the failure of a safety system or component and 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 air 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 a consequence of pipe whip, missile impact, jet impingement, environmental effects, etc.

Human interaction dependencies 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.

Component failure dependencies cover those failures of usually identical components which are otherwise not analysed. Such failures may be caused by errors in design, manufacturing, installation, calibration or 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. [10].

3.4.2. Inclusion of dependencies in the PSA

It is necessary for the reviewers to check that a systematic analysis has been carried out to identify all the potential dependencies 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 were not omitted. In addition, some of these dependencies which are important in the PSA may be selected for a detailed review.

Human interaction dependencies include:

— test or maintenance activities that require multiple components to be reconfigured,
— multiple calibrations performed by the same personnel, and
— post-accident, manual initiation (or backup initiation) of components that require the operator to interact with multiple components.

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

Adequate justification is to be provided for the common cause failure probabilities used in the PSA. Where possible, they are 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 (APWR, ABWR, etc.) 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 in station blackout. 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 thermal-hydraulic analysis and by extensive tests. This deterministic demonstration of effectiveness should cover the full range of accident conditions for which they are claimed. Passive systems tend to work with much lower pressure heads than do active systems so that the thermal-hydraulic performance predictions may be more difficult.

The successful performance of passive systems will have been demonstrated within a set of boundary conditions (for example coolant temperature, pressure, 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 right 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 — that is, that the system set-up is incorrect. This can be done by standard fault tree analysis, but the reviewers need to check that this takes full account of the potential for human error in leaving the system in the proper condition, as well as of all necessary valves (for example, check valves) which are required to act and any active initiation signals.

3.5.2. Passive components and structures

These items may be considered as **structures**, such as walls, floors, supports, etc., and high energy **pipework and vessels**.

Structures. Failure of structures as a consequence of certain energetic 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 (see Section 3.9), and the detailed review of the conditional failure probabilities (fragilities) requires assessment by specialists in these areas. Otherwise, the failure of a properly engineered structure is generally taken to be of such a low probability that it need not be considered in the PSA. The reviewers may accept this approach, provided that the regulatory authority has accepted the deterministic safety case for the structures, and that there is nothing in the operating experience of the plant which casts doubt on particular items.

Pipework and vessels. The significance of these in PSA is twofold. First, an unprovoked failure will constitute an initiating event, and an estimate of its frequency will be needed. 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 break, feedline break). For some plants, the utility may claim that certain components in the primary and secondary circuits (for example, 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 — that is, it is outside the design basis of the plant, and no specific protection needs to be provided. If the regulatory authority 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 rest, it has to be recognized that the estimation of failure rates is subject to large uncertainty, due to the scarcity of relevant experience 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 have 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 [22, 23]. 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, first, 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 the code produces as output. 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 should 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 experience data. 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 the unreliability of the system, and so 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 the PSA is the human reliability assessment (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 (see Ref. [24]).

3.6.1. Framework for the HRA

It is necessary for the reviewers to 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 HRA methods selected is a critical factor in a successful HRA.

The framework used for guiding the HRA should 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 (see Ref. [25]).

The HRA procedure used usually include the following important steps:

— identification of human interactions,
— establishment of the importance of the human interactions (qualitative and quantitative screening),
— incorporation of the actions into the appropriate parts of the logic model,
— selection of suitable HRA methods,
— quantification of the human interaction events, and
— documentation of the analysis performed.

The reviewers need to compare the HRA process used to the SHARP steps in order to check that all the necessary steps are included in the PSA.

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). The HEPs may be derived by using the technique for human error rate prediction (THERP) method [26], the human cognitive reliability method (HCR) [27] method or the success likelihood index method (SLIM) [28], which are some of the commonly used methods. Other methods are also available and can be used where appropriate.

The reviewers need to 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. This would include:

— the timing of the action,
— the information available, and
— the influence of prior actions.

The reviewers should 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 only done 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 three types:

— **Type A** — human interactions occurring before the initiating event affecting system or component unavailability,
— **Type B** — human interactions that cause an initiating event, and
— **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 called upon. 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. 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's maintenance, testing, and calibration procedures to identify these actions for the systems modelled in the PSA.

The reviewers need to check that the maintenance and test department practices to minimize human induced dependencies, 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 was done correctly. It is also helpful to review plant experience for Type A human errors. The reviewers should pay particular attention to plant configurations in which valves are isolated (actuated, closed/opened) for test and maintenance purposes or calibration processes which can defeat key instrumentation for either operator information or automatic action by 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 need 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 to analyse these actions, such as the HCR method, THERP, SLIM and others. 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 may be performed. The aim is to check that:

— the process for identifying Type C actions to be analysed is thorough and comprehensive,
— the quantification process was performed accurately and consistently, and
— 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

It is necessary that the reviewers 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 like:

— description of human actions,
— precise indication of relevant part/subpart/paragraph of operational documentation, if they exist,
— modelling in system functions, event sequences (together with a description of previous failures), and
— necessity/feasibility/entry and/or transfer criteria of considered human actions referring to the modelled position in the PSA (boundary conditions, assumptions, 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 has to be addressed. Finally, it is necessary to pay attention to a coherent HRA and PSA modelling in the framework of a static assessment. That means, for example, the interconnections between human actions have to be examined along an event path (sequence).

Thus a detailed HRA is necessary to 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 dependencies have usually not been considered at this point. Often in screening, the dependency between human interactions is set to 1.0 to ensure that the related human action dependency 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 validity, the PSA should have clearly identified and documented all the following:

— the components with which the operator or other personnel interacts,
— the tasks and restoration actions that are specifically involved in each interaction,
— the relative locations of the different components when the operator interacts with multiple components,
— the components that need to be restored and that are alarmed in the control room if not restored,
— 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 should be reviewed to assess the data and quantification techniques used.

In order to assess post-accident (Type C) operator actions validity, the PSA should have clearly identified and documented two sets of actions:

— post-accident operator actions required for systems to operate successfully, and
— 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. The PSA should clearly identify and document all these operator actions, 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 be checked using appropriate techniques — for example, walk-talk through procedures.

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

Checks may be needed to see whether the estimated probabilities are sensible with regard to influences and assumptions made. The involvement of plant personnel should 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 dependencies between the actions have been accounted for.

If expert judgement methods, such as the direct estimation approach, are used, the reviewers need to examine the process carefully as to how the process 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, include 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. Modelling of the human interactions is to be thoroughly documented. The PSA should clearly identify 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 it is to be verified that if their probabilities are independent there are no dependencies between the actions, or if they are dependent then that the dependency 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 in which the recovery can be performed (MCR or locally), the environment in 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 should 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 need to check the coherence of the modelling of the HRA and the systemic analyses in the overall PSA model — that is, the incorporation of the results of HRA into the PSA has to be assessed.

3.7. DATA REQUIRED FOR THE PSA

This section addresses the data required for the following items:

— initiating event frequencies,
— component failure probabilities, and
— 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 should 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 should ensure that the maximum use has been made of plant specific data, but should compare this with the generic data and 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 are recommended 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 that from all PWRs, but may not have been readily available to the PSA analysts. For a new plant, the designers may have supplied them with data for 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 data used should be sufficiently well justified in the PSA documentation and should be 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 ensure themselves that bases for the judgements on these numerical estimates have been given and are acceptable.

3.7.1. Initiating event frequencies

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

For an operating plant, the reviewers are recommended to check that an analysis has been performed of all 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 this 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. This kind of analysis is described in Section 5.2.2 of Ref. [4] and Section 6.6 of Ref. [3], which give some guidance on modelling aspects.

3.7.2. Component failure probabilities

Selection of generic data for each type of component and the transferability to the plant under consideration should be justified in the PSA documentation. Plant specific data is preferable, if available.

If a combination of generic references is used, the methods used for selection of the specific references or for integration of the references are 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 expect 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 should 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 should 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 are recommended also 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 should 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 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. [29] and in Section 5.3 of Ref. [4]. 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. [30].

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. It is recommended that this data be a realistic reflection of the practices in use on, 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 contribution to 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 were performed correctly. If generic data is used, the reviewers should verify that the source is recent and is recognized as an acceptable source.

Further guidance can be found in Section 5.3 of Ref. [4].

3.8. ANALYSIS OF COMPUTER BASED SYSTEMS

Increasingly, protection and control systems are being based on programmable computers and it is expected that all future designs will be computer based, whether they are for new plant or for major upgrades of existing plant. Computer based systems present problems for the designer, assessor and reviewers which are distinctly different to those of traditional hard-wired systems, particularly as regards the estimation of reliability values for the systems.

The reliability analysis of a hard-wired system is generally based on the assumption that the 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. That is, 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 subcooling 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.

It is important for the reviewers 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 [31–36].

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 bound 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 unsafe errors, 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.

In the reliability analysis, the computer based system is usually first decomposed into parts which can be treated separately and where the dependencies between the parts can be identified clearly, as for the analysis of a conventional system. If the system is integrated, the dependencies 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 sub-systems each of which performs a fairly simple safety function, as may happen 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 will expect to see an analysis of the reliability of the hardware. This usually follows a standard approach, as described in Section 3.3, taking account of both random and common cause hardware failures. It should also take into account the self-checking facilities which are usually built into such computer systems, since these are to reveal any hardware failures. If the system has adequate redundancy of trains (say three or fourfold) and is otherwise well designed, the unreliability calculated for the hardware is usually relatively low, say 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 rate should take account of all relevant factors, which would include:

— the size and complexity of the system (the number of lines of code is an indication),
— the novelty of any of its features,
— whether it identifies a safety kernel,
— the degree of conformance with procedures and standards in the production, checking and testing processes,
— the independence of the teams performing the static analysis and the dynamic testing,
— the number of errors found in these two processes,
— the extent of the use of formal analysis tools in the static analysis,
— the number of dynamic tests carried out,
— the experience of the designers of the system, and
— experience with similar systems in service.

As regards the last item, it can, of course be very helpful to compare the system with a similar system (perhaps non-nuclear) for which there is some history of reliability, 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 rate 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 it is claimed to be much lower than this, the reviewers are recommended 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.

SOFTWARE DEPENDENCIES

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 different teams, programming languages, manufacturers, etc., and may then claim complete independence. It is recommended to not accept such a claim: 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 protection system are both computer based, consideration is to be given to software dependencies 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 against that fault. Also, where the control and protection systems both appear on an event tree, some dependence should be assumed.

SENSITIVITY STUDIES

As will be clear from the comments above, there will be a substantial uncertainty in the reliability assigned to a computer-based system. This is usually addressed in the PSA documentation by sensitivity studies on the overall PSA. If the unreliability has been judged, for example, to be 10^{-4} failures per demand, then the effect of changing this to, say, 10^{-3} should be determined, taking account of any implied changes in a diverse system due to dependencies.

FURTHER POINTS

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 need to check that it has been modelled in the appropriate event trees.

Computer components are also liable to be vulnerable to electromagnetic interference — for example, from mobile phones. The reviewers should 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 change procedure. This may not have any direct effect on the PSA but the reviewers should 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 for 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 on the same footing as initiating events caused by internal plant faults (transients and LOCAs). The section addresses the identification of internal and external hazards and the screening of them 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. This guidance illustrates the general approach, which can be adapted to the review of the analysis of other hazards, but further guidance can be found in Refs [8, 9, 37].

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 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 dependencies are usually important in hazards analysis, the reviewers need to pay particular attention to the way they are modelled. One approach is to model each dependency 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 hazards related dependencies to be integrated with that of the random and common cause failures, human errors, etc, and so may be preferred. Another approach is to evaluate the fault and event trees without the hazards related dependencies, and then to account for them 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 Ref. [38] or in other PSAs. The hazards are normally categorized by some such scheme as:

Internal hazards:	Fire. Flooding. Missiles. Dropped loads.
Natural external hazards:	Earthquake. High winds. Extreme temperatures (air and sea water). Floods. Lightning. Meteorites.
Man made external hazards:	Aircraft crash. Explosion. Toxic gases.

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

— are inapplicable to the site/plant (for example, volcanoes for most sites),
— are of negligible frequency (for example, relative to the core damage frequency (CDF) from internal plant faults), or
— 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. [8]. It is good practice to see 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 should be accounted for in the PSA. Some will need detailed analysis with specialist input — for example, earthquakes, internal fire, aircraft crash. Others, 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 (for example, wind speed). It is also generally subdivided into bands or ranges as follows:

— seismic event — bands/ranges of earthquake severity/ peak ground acceleration,
— wind — bands/ranges of wind speed,
— internal fires — each room with combustible material,
— aircraft crash — type of aircraft: military, light aircraft, airliner, helicopter, and
— internal flood — specific sources: pipe breaks, 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 are recommended 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 peak ground acceleration (pga), those of relatively high frequency, with pga just above the design basis level, may cause relatively little damage, those in the highest pga band may be very likely to lead to core damage but be of a 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 the hazard analyses. For the 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 — that is, that all the risk comes from hazards which are beyond the design basis. The reviewers have 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 [8, 9]. The analysis in general, includes the following steps:

— estimation of the frequency of seismic events as a function of their severity at the plant, which is often characterized by the peak ground acceleration — often referred to as the seismic hazard curve,
— estimation of component and structural failure probabilities (fragilities) as a function of seismic severity,
— evaluation of physical and systematic dependencies between components due to the seismic event,
— estimation of the effects of the seismic event on the possibilities for and probabilities of human error. This should cover psychological factors, like increased stress as well as confusion because of loss of equipment and spurious indications,
— 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, and
— uncertainties.

The reviewers need to assess 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 are usually based on relevant historical experience for the regions around the plant or for regions of similar seismicity. The estimation of the curve should consist of a parametric fit to data, with associated uncertainty distribution. The maximum severity cut-off for the curve should be identified and justified.

Soil failures as a direct result of the earthquake — for example, liquefaction and slope instability are supposed to 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 (for example, 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 should be given, 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 should be documented.

Evaluation of physical dependencies 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 failure contributors 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 the seismic event and cause the failure of critical components.

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

The calculation of the core damage frequency should 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 should 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 are recommended to 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 should 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:

— initial screening to eliminate fire scenarios in rooms that are small contributors to plant risk,
— estimation of the frequency of fires of different size starting in different rooms of the plant,
— assessment of the type of plant disturbance potentially caused by a fire,
— calculation of the propagation of the initiated fire and propagation of fire effects to affected components and operators,
— estimation of non-detection and non-suppression probabilities for the initiated, propagating fire,
— evaluation of component dependencies and component failure probabilities due to fire effects,
— estimation of the effects of the fire on human actions and possibilities for increasing the probabilities of identified human errors, and
— 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 that each of these steps has been clearly documented and that the basis and assumptions for the data and models is given. Specific points to address in the review include the following:

The documentation is expected 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 should describe the basis for the differentiation.

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, is to be assessed for its validity.

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.

Databases used for the fire initiation frequencies have to be referenced so that the reviewers can check for consistency between the databases and the data for the plant analysed.

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

Plant specific data or data from plants similar to the one in question should 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.

The propagation of the effects of the fire should 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. These parameters to be reviewed should 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.

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.

The evaluation of multiple components that can simultaneously fail owing to the fire should include consideration of heat effects, smoke effects and water effects due to the working of fire suppression systems.

The evaluation of operator actions related to the fire has to 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 should include effects of fire on the availability of instrumentation and related equipment.

The quantification of fire barrier efficiency has to be documented by the PSA. It is necessary for the reviewers to check whether penetrations in the barriers, such as doors that may have been left open, have been taken into account in probability assignments.

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 should be revealed in the PSA.

If fault trees are developed for fire suppression systems, the treatment of dependencies caused by the fire need to be reviewed.

The results of the fire analysis are to be as clearly presented and structured as the rest of the PSA analysis. It is good practice to perform sensitivity analyses on the areas of the analysis where especially questionable assumptions have been made.

Further guidance on internal fires PSA can be found in Ref. [37].

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:

— initial screening to eliminate flooding scenarios in rooms that are small contributors to plant risk,
— identification of the possible water and steam sources,

— assessment of the type of plant disturbance potentially caused by the flooding,
— evaluation of the frequency of occurrence of an initiating event caused by these sources,
— estimation of the likelihood that the operator does not detect and control the flood,
— identification of the components that are affected by the flooding.
— 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.

It is necessary for the reviewers to check that all these steps are clearly identified, that the data used are documented and that 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 frequencies of 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 should 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 are to be evaluated in terms of the means of detecting and controlling the event. The means should then 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 electrical 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 sequences frequencies are then calculated using the data for initiating event frequencies, component failure probabilities, component outage frequencies and durations, common cause failure probabilities, human error probabilities, etc. 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 dependencies are correctly accounted for in the quantification process.

The quantification process should have been carried out using a suitable computer code which has been fully validated and verified. In addition, the users of the codes should 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 a core damage. This is recommended to be done 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 need to check that they have been set at a sufficiently low level such that they would not lead to a significant underestimate of the frequency of core.

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, that is, 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 to the mean for a skewed distribution. In a point value calculation, the reviewers should 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 are recommended to follow the policy of their regulatory authority, 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 should 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 need to 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 production of the core damage frequency should be complemented by sensitivity studies to explore the major uncertainties separately. In addition, importance analysis are required to be performed to identify the significant initiating event groups, system and basic events that contribute to the risk.

These three areas are discussed below.

3.11.1. Sensitivity analysis

The aim of carrying out 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 means in the data listing.

Throughout their review, the reviewers should have identified and noted items of data or assumptions which are candidates for sensitivity studies, due to their uncertainty or their reliance on judgement. Some of these may later be weeded out on the basis of their importance factors, and others added which significantly impact 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 assumption 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 re-running the PSA evaluation. The reviewers are recommended to check that sensitivity studies have been performed on all the appropriate assumptions and data.

Section 6.5.2 of Ref. [4] 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 uncertainty analysis is to provide quantitative measures and qualitative discussions of 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, and
— 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 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 need 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 are recommended to assess the relative importance of model uncertainties by reviewing the results of 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 one among the three types of uncertainties.

The reviewers may consider 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 whether dependencies have been properly treated in the uncertainty quantification (for example, 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. [4].

3.11.3. Importance analysis

Importance analysis determines the importance of contributors 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 are recommended also to check that the importance analysis results are in general agreement with the sensitivity analysis qualitatively, and make logical sense.

More details about importance analysis can be found in Section 6.5.1 of Ref. [4].

3.12. RESULTS OF THE PSA

The value of a PSA lies largely in the successful communication of its results to the users, who are liable to include non-specialist senior managers as well as PSA specialists, in both the regulatory authority and the utility. The reviewers should therefore 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 are also to be aware that different groups of PSA analysts, users and reviewers may use somewhat different terminology and concepts and have their own mindset as to what is, or should be, in a PSA, and should take this 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 recommended not to accept a bald presentation of, say, the core damage frequency which leaves it to the reader 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 authorities, 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 should be put forward as best estimates. Some regulatory authorities 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 the results of the PSA

The results of the PSA are expected to give the numerical estimate of the CDF and include sufficient information to give insights into what are the main contributors. This would typically include:

— core damage frequency,
— contribution to the CDF from each of the initiating event groups,
— dominant accident sequences which contribute to the CDF,
— results of the sensitivity studies (see Section 3.11.1),
— results of the uncertainty analysis (see Section 3.11.2) giving confidence limits (typically the 5% and 95% bounds) for each of the main results of the PSA, and
— importance measures for basic events, safety systems, etc. (see Section 3.11.3).

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

It is necessary for the reviewers to ensure themselves 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 PSAs 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 that they are consistent. 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 the 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 the results of the PSA

The core damage frequency may 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 may be given to identifying improvements which could be made to reduce the core damage frequency.

The reviewers are supposed to check whether the overall design and operation of the plant is well balanced. This should confirm 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.

Good practice is 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 THE PSA QA

As discussed in Sections 2.2 to 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 authority at an early stage of a PSA (ideally, before actual analysis starts). Whether or not this is done, the regulatory authority 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 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 recommended to conduct the first one at an early stage in the PSA development, so that any deficiencies identified in the audit can be corrected then.

REFERENCES

[1] NUCLEAR ENERGY AGENCY OF THE OECD, Regulatory Approaches to PSA, Report of a Survey of National Practice, Rep. NEA/CNRA/R(95)2, OECD/NEA, Paris (1995).

[2] NUCLEAR ENERGY AGENCY OF THE OECD, Review Procedures and Criteria for Different Regulatory Applications of PSA, Rep. NEA/CNRAR(97)5, OECD/NEA, Paris (1997).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, IPERS Guidelines for the International Peer Review Service, Second Edition, Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, IAEA-TECDOC-832, Vienna (1995).

[4] 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).

[5] UNITED STATES NUCLEAR REGULATORY COMMISSION, The Use of PRA in Risk-Informed Applications, Rep. NUREG–1602, USNRC (Draft for comments).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA, Vienna (1995).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA, Vienna (1996).

[8] 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).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, Vienna (1993).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA-TECDOC-648, Vienna (1992).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Defining Initiating Events for Purposes of Probabilistic Safety Assessment, IAEA-TECDOC-719, Vienna (1993).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Initiating Events for PSA for WWER Reactors, IAEA-TECDOC-749, Vienna (1994).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).

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

[15] NUCLEAR ENERGY AGENCY OF THE OECD, State of the Art of Level–1 PSA Methodology, Rep. NEA/CSNI/R(92)18, OECD/NEA, Paris (1993).

[16] UNITED STATES NUCLEAR REGULATORY COMMISSION, Probabilistic Safety Analysis: Procedures Guide, Rep. NUREG/CR-2815 BNL-NUREG-51559, Rev.1 (2 Volumes), Brookhaven National Laboratory, USNRC, Washington, DC (1985).

[17] RANSON, V.H., RELAP5/MOD3 Code Manual (Vol. 1–5), Rep. NUREG/CR–5535, EGG–2596, EG&G Idaho Inc., June Idaho Falls, ID (1990).

[18] LIN, J.C., TRAC–PF1/MOD2 Code Manual (Vol. 1–4) Rep. NUREG/CR–5673, LA–12031–M, Los Alamos National Laboratory, NM (1994).

[19] BOULET, M., User manual of CATHARE 1 v.1.3 code, Rep. Dossier d'Exploitation D 4–1 CENG Technical Note Seth–LEML EM 87–86, Grenoble (1987).
[20] WOLFERT, K., LERCHL, G., MIRO, J.E., SONNENBURG, H.G., "The GRS thermalhydraulic system code ATHLET for PWR and BWR analyses" (Proc. 3rd International Topical Meeting on Nuclear Power Plant Thermalhydraulics and Operation, Seoul, 1998), KAERI, Seoul (1998).
[21] GRUNDMANN, U., ROHDE, U., "DYN3D/M2 — a Code for Calculation of Reactivity Transients in Cores with Hexagonal Geometry" (Proc. IAEA Technical Committee Meeting on Reactivity Initiated Accidents), IAEA, Vienna (1989).
[22] NYMAN, R., HEGEDUS, D., TOMIC, B., LYDELL, B., "Reliability of Piping System Components", Framework for Estimating Failure Parameters from Service Data, SKI Report 97:26, Swedish Nuclear Power Inspect., Stockholm (1997).
[23] UNITED STATES NUCLEAR REGULATORY COMMISSION, USNRC Draft Rep. DG-1063, Washington, DC (1997).
[24] NUCLEAR ENERGY AGENCY OF THE OECD, Critical Operator Actions: Human Reliability Modeling and Data Issues, Rep. NEA–CSNI–R(98)1, Paris (1998).
[25] HANNAMAN, G.W., SPURGIN, A.J., Systematic Human Action Reliability Procedure (SHARP), Rep. EPRI–NP–3583, Electric Power Research Institute, Palo Alto, CA (1984).
[26] 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).
[27] HANNAMAN, G.W., SPURGIN, A.J., LUKIC, Y.D., JOKSIMOVICH, V., WREATHALL, J., Human Cognitive Reliability Model for PRA Analysis, NUS Report (Draft) NUS–4531, Electric Power Research Institute, Palo Alto, CA (1984).
[28] EMBREY, D.E., SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement, Rep. NUREG/CR-3518, USNRC, Washington DC (1984).
[29] 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).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-508, Vienna (1989).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Implications of Computerized Process Control in Nuclear Power Plants, IAEA-TECDOC-581, Vienna (1991).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Computerized Control and Protection Systems, IAEA-TECDOC-780, Vienna (1994).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Reliability of Computerized Safety Systems at Nuclear Power Plants, IAEA-TECDOC-790, Vienna (1995).
[34] 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).
[35] 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, UK, HSE Books, London (1998).
[36] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, IEC 880, IEC, Geneva (1986).

[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Reports Series No. 10, IAEA, Vienna (1998).
[38] UNITED STATES NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Analysis: Procedures Guide, Rep. NUREG/CR-2300, USNRC, Washington, DC (1983).

ABBREVIATIONS

ABWR	advanced boiling water reactor
APWR	advanced pressurized water reactor
CDF	core damage frequency
ECCS	emergency core cooling system
FMEA	failure modes and effects analysis
HAZOP	hazards and operability studies
HEP	human error probability
HRA	human reliability assessment
I&C	instrumentation and control
LOCA	loss of coolant accident
LPIS	low pressure injection system
MCR	main control room
PDS	plant damage state
pga	peak ground acceleration
PORV	power operated relief valve
PWR	pressurized water reactor
QA	quality assurance
RCP	reactor coolant pump
SGTR	steam generator tube rupture
SHARP	systematic human actions reliability procedure

CONTRIBUTORS TO DRAFTING AND REVIEW

Areia Capitão, J.J.	European Commission, Belgium
Campbell, J.F.	Nuclear Installations Inspectorate, United Kingdom
Clapisson, G.A.	Council for Nuclear Safety, South Africa
De Gelder, P.	AIB-Vinçotte Nuclear, Belgium
Gibelli, S.M.O.	Comissão Nacional de Energia Nuclear, Brazil
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.	Jozef Stefan Institute, Slovenia
Kafka, P.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Kaufer, B.	OECD Nuclear Energy Agency
Kovács, Z.	RELKO Ltd, Slovakia
Labatut, M.	Commissariat à l'énergie atomique, France
Landelius, M.	OKG AG Oskarshamn, Sweden
Lederman, L.	International Atomic Energy Agency
López-Morones, R.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Mexico
Niehaus, F.	International Atomic Energy Agency
Pschowski, J.	ESI Energie-Sicherheit-Inspection GmbH, Germany
Ranguelova, V.	International Atomic Energy Agency
Schueller, G.I.	Institute of Engineering Mechanics, Austria
Serbanescu, D.	National Commission for Nuclear Activities Control, Romania
Shapiro, H.	Atomic Energy of Canada Limited, Canada
Shepherd, C.H.	Nuclear Installations Inspectorate, United Kingdom
Spitzer, C.	TÜV Energy and Systems Technology, Germany

Vallerga, H.R.	Autoridad Regulatoria Nuclear, Argentina
Vojnovic, D.	Slovenian Nuclear Safety Administration, Slovenia
Villadoniga, J.	Consejo de Seguridad Nuclear, Spain
Willers, A.	Australian Nuclear Science and Technology Organisation, Australia
Yllera, J.	Consejo de Seguridad Nuclear, Spain
Zeng, Y.	Atomic Energy Control Board, Canada

Consultants Meeting
Vienna, Austria: 15–19 December 1997

Technical Committee Meeting
Paris, France: 16–20 Novembe