IAEA-TECDOC-832

IPERS guidelines for the international peer review service

Second Edition

Procedures for conducting independent peer reviews of probabilistic safety assessments

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

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

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

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

The originating Section of this publication in the IAEA was:

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

IPERS GUIDELINES FOR THE INTERNATIONAL PEER REVIEW SERVICE
IAEA, VIENNA, 1995
IAEA-TECDOC-832
ISSN 1011–4289

Printed by the IAEA in Austria
October 1995

FOREWORD

In order to make international expertise available for reviewing probabilistic safety assessments (PSAs), the IAEA established in 1988 an international peer review service (IPERS) for PSA. Because of the complex character of a PSA and because PSA has reached the point where it affects design, regulatory and licensing decisions, there is an international consensus that an intensive, thorough peer review by independent and experienced PSA practitioners should be an integral part of any PSA programme.

At the beginning of the IPERS review activities a review guideline was written (IAEA-TECDOC-543) which served as the basis for conducting the IPERS PSA reviews for many years. The present document represents a major revision of this first edition of the review guideline published in 1990. The revision is based on the practical experiences made during the past reviews. The scope of the guideline is extended to include Level 2 PSA that deals with phenomena related to core damage and severe accident progression within the nuclear facility, and Level 3 PSA which analyzes the consequences in the environment of the facility. Furthermore, it reflects the developments of PSA methodology and techniques since the first edition was written. The weight for reviewing human reliability analyses has been considerably increased because this area has turned out in past reviews to be especially difficult and critical.

Several IAEA procedures for different PSA areas have been published or are in preparation, which are used and referenced in the IPERS activities. The review guidelines are intended to be consistent with the IAEA PSA procedures.

This publication describes the purpose and the objectives of an IPERS review. The main objective is first to assess whether important technological and methodological issues in the PSA are treated in an adequate manner and, second, whether specific conclusions and applications of the PSA are supported by the underlying technical analysis in an appropriate way. An important aspect for an IPERS review is the communication and exchange of views between the international experts carrying out the review and the members of the PSA team.

This TECDOC is intended to give guidance on how an IPERS review is organized and conducted, it describes the steps needed to prepare the review and it highlights the PSA aspects which should be covered in detail.

EDITORIAL NOTE

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

Throughout the text names of Member States are retained as they were when the text was compiled.

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. BACKGROUND

In order to make international expertise available for reviewing probabilistic safety assessments (PSAs), an international peer review service (IPERS) for PSA was established at the IAEA in 1988. Because of the complex and multidisciplinary character of a PSA and because PSA has reached the point where it affects design, regulatory and licensing decisions, there is an international consensus that an intensive, thorough peer review by independent and experienced PSA practitioners should be an integral part of any PSA programme. Based on past reviews it is noted that the IPERS reviews can have a major influence on the quality of the PSA, thereby strengthening the credibility of the PSA in making safety related plant enhancements.

At the beginning of the IPERS review activities a review guideline was written [1] which served as the basis for conducting the IPERS PSA reviews during the past years. The present document represents a major revision of this first version of the review guideline and it includes the practical experiences made during the previous reviews and the further development of the PSA methodology since the first version was written. The following PSA procedures have been established by the IAEA which have been used and referenced in the IPERS activities:

- Level 1 guideline [2]
- Level 2 guideline [3]
- Level 3 guideline [4]
- External events guideline [5]
- Seismic event guideline [6]
- Common cause failure guideline [7].

Further PSA guidelines are being developed, in areas such as internal fires and floods, human reliability assessment and shutdown and low power operational states. The review guidelines are intended to be consistent with the above IAEA PSA procedures. The review guidelines define a framework for performing the reviews and should be used together with the PSA procedures.

The report deals with the following topics in the review of a PSA:

- The scope of the review
- The objectives of the review
- The review process
- The composition and size of the review team
- Review schedules and manpower
- Developing consensus within the reviewers team
- Review report, review conclusions
- Preparation for the review
- Specific areas to be covered
- Conducting a Level 1 review
- Conducting a Level 2 review
- Conducting a Level 3 review.

The needs of Member States requesting an IPERS PSA review have played a major role in developing the detailed IPERS review process. The different motivations for requesting such review are described in the following section.

1.1. MOTIVATIONS FOR REQUESTING AN IPERS REVIEW

Originators of a request for an IPERS review mission are regulatory bodies and plant operators. As noted in the past, there is a considerable variety in the motivations of Member States for requesting an IPERS review. A selection of important motivations is given in the following list:

(i) International consensus that an intensive, thorough peer review by independent and experienced PSA practitioners should be an integral part of any PSA programme.

(ii) Quality assurance (QA) and review restricted to internal organizations are sometimes biased due to a variety of reasons. Such bias can be minimized by an external, independent peer review.

(iii) The PSA is part of the licensing process, but the safety authority has only limited capacities or experience in the PSA field, and an IPERS mission could augment this capability.

(iv) To support development of regulatory review practices and expertise.

(v) Political and public attention for severe accident risks of NPPs is a motivation for an independent peer review in some Member States.

(vi) Bringing in new, top-level experience into the PSA work and providing communication and exchange of views with experienced specialists. This appears to be especially useful for new PSA teams in countries where the technical capability has recently been developed.

(vii) International independent peer review as a partial replacement of or complementary to internal review and QA if the capacities and experience in a Member State are still limited or under development.

In principle, some of these motivations have a potential to conflict with the basic objective of the review to be independent. Special care is needed in these cases to match the needs of Member States without compromising the basic aims of an independent, high level peer review.

1.2. SCOPE OF IPERS REVIEWS

IPERS reviews can cover partial scope PSAs, complete full scope PSA studies or parts of them for nuclear power plants and research reactors. A full scope PSA includes:

- the whole lifetime of a NPP (project, construction, startup, operation, decommissioning),
- Level 1, Level 2 and Level 3;
- complete operational states (full power, low power and shutdown);
- complete set of initiating events (internal and external).

A number of PSAs are restricted to full power, Level 1. Also it is common practice to begin with a Level 1 PSA for full power and to extend the scope later. To keep the reviews manageable and to follow the development of the PSA, it has become practice to conduct the review in distinct phases for the various PSA parts. Typical parts considered during a review are:

- internal events, full power Level 1 PSA;
- internal events, low power and shutdown Level 1 PSA;
- external events PSA for full power.

Specialized reviews for more restricted areas are also conducted, such as internal fire and floods PSA and Level 2 PSA.

It has to be noted that in the various areas of a full scope PSA differences exist regarding established methodologies and techniques. For example, the full power Level 1 aspect of PSA is relatively well defined today and well covered by PSA procedures. In contrast, Level 2 accident progression analysis still involves a considerable degree of expert judgement. Only a few software tools exist for integrated Level 2 analyses such as MELCOR [8] and MAAP [9]. Review of the Level 2 part of a PSA not only requires an understanding of the results of the Level 1 part of the PSA, but

also intimate knowledge of the analytic models implemented in the analysis code used, of important physical phenomena and of the behavior of the plant under severe accident conditions.

Recent PSAs considering shutdown or low power operational states have shown that these periods can contribute substantially to risks at the plant. The review of these studies also revealed that for these plant states some development effort of PSA techniques and methods, including in particular human reliability assessment (HRA), is still needed. Specific important areas are the adequate modelling of the many possible plant configurations including potential maintenance and repair outages and the assessment of the operator actions and interactions, which may be affected by the limited availability of effective instrumentation and procedures.

The present review guideline is centered on full power PSA methodology and techniques. Furthermore, the procedures were written mainly by experts with US or European light water reactors (LWRs) experience. Therefore, application of the guideline for low power and shutdown states and for reactor types other than the above mentioned LWRs should be carried out by interpreting and applying the guideline as far as possible and useful.

1.3. GENERAL OBJECTIVES

The IPERS provides peer reviews for PSAs performed in Member States by teams of carefully selected independent and international experts. The resulting recommendations consider improvements and extensions of the PSA and provide guidance for a wide spectrum of PSA applications. The basic objectives of the IPERS can be summarized as follows:

- assess the adequacy of the treatment of important technological and methodological issues in the PSA;

- assess whether specific conclusions and applications of the PSA are adequately supported by the underlying technical analysis.

IPERS does not replace internal, independent reviews and it does not perform a validation of the PSA nor does it replace quality assurance.

An important objective of IPERS reviews is that the reviews are conducted in the most profitable way for the PSA team by first assuring that the comments of the reviewers are fully understood and by promoting discussions to allow for a transfer of knowledge from the international experts to the organizations involved in the PSA.

In order to perform an IPERS review and to make related conclusions and recommendations it is necessary that the review team and the review team leader compare the reviewed PSA with the present state-of-the-art in PSA methodology and technology. The current state-of-the-art of PSA is defined by the way PSAs have been practically performed in recent years by Member States according to existing guidelines and using accepted methodologies and techniques. By this definition, advanced and exploratory studies are in principle excluded from being used as a measure to judge a reviewed PSA. However, advanced and exploratory studies might still be used as background information to judge trends regarding future developments.

2. SPECIFIC OBJECTIVES OF THE REVIEW

The determining aspects for the IPERS PSA review are the scope and objectives of the PSA. An IPERS review could include a discussion of the scope and objectives of the PSA if desired, however, basically the definition of scope and objectives has to be determined by the Member State. Therefore the IPERS review is traditionally centered around and following the given scope and objectives of the PSA.

There are three general objectives when performing PSAs to assess the level of safety of a plant:

(1) to identify the important risk contributions and the most effective areas for improvement;

(2) to compare the PSA results with explicit or implicit standards;

(3) to assist plant operations by determining the risk significance of plant configurations and of operational features.

Each study may put different emphasis on specific objectives. The focus may depend on the stage of the plant life cycle (e.g., conceptual or final design stage, operating plant). A review of a PSA can focus on one or more of the following technical areas:

(1) the general validity of the methodology and data used in the PSA;
(2) the validity of the results and conclusions obtained in the PSA;
(3) the validity and applicability of the PSA models as tools to assist operations;
(4) the validity of the PSA models for meeting specific stated applications.

When the focus is the general validity of the PSA methodology and data, the review is carried out to assess the general validity of the assumptions, models, data and analyses used in the PSA.

When the focus is on the results of the PSA, the review is centered on the validity of the qualitative and quantitative conclusions obtained in the PSA. Emphasis is placed on the justification of the results in terms of the contributors which determine the results and omissions, uncertainties, or inaccuracies which may change the results. The assumptions, models, data, use of expert judgment and analyses are specifically reviewed with regard to their influence on the bottom line numbers, results, and conclusions obtained by the PSA.

When the focus is on the PSA as an operational tool, the review is carried out to assess the validity and applicability of the PSA as a tool for use in plant operational applications. These include applications to evaluate technical specifications, modifications to emergency procedures, crew training, control room modifications, use of simulators, applications to evaluate implications of precursors and other events which occur at the plant, and applications to monitor plant performance and plant configurations. The focus of the review is on the validity of the PSA models and analyses, including structure, algorithms, and analyses, for effective and efficient use in operational applications.

Finally, when a specific application of the PSA is the focus, the review is concentrated on the specific purposes for which the PSA was performed and the validity of the PSA for these purposes. For example, if the PSA was carried out to evaluate the impacts of a proposed backfit, then the review is focused on evaluating the validity of the assumptions, models, data and analyses specifically related to the backfit application.

3. THE REVIEW PROCESS

It has to be realized that each IPERS review mission will face an individual PSA study with its own peculiarities, strength and weaknesses. Furthermore, each IPERS mission is usually conducted by a newly composed team of reviewers. Therefore, each review mission has an individual character.

The main elements of a Level 1 PSA are the initiating events with a potential to disturb normal plant operation, the logic sequence and system model which handles the timing and combination of events during the event sequences initiated including human interactions and the models describing the plant response in terms of physical phenomena. Development of these strongly linked elements is since WASH-1400 recognized to be a highly iterative process especially in PSAs developed for the first time for a particular facility. Such iterative procedures apply for almost all other PSA portions. Therefore it can make a drastic difference if a PSA is performed for the first time for a new type of facility or if similar plants have been analyzed in available reference studies. Many of the reviewed PSAs are conducted by teams performing a full size PSA for the first time. This makes a significant difference if compared to a PSA conducted by a PSA team which has previously performed several other PSAs.

For some of the Member States producing an entire PSA report in the language in which the review is performed would represent a disproportional burden. The usual practice in such case is that, at a minimum, a summary report in the language agreed for the review is produced and that the detailed review is based on the original documents, ad hoc translation by the PSA team and interviews of the PSA team members by the reviewers on specific subjects. However, such procedure considerably slows down the review process and diminishes the review efficiency. Furthermore, differences may exist in the capabilities of the PSA team and of the review team members to communicate in the language agreed for the review.

The PSA model even for basically similar facilities can be drastically different due to relatively "minor" design differences, for example due to differences in the reactor protection logic and related setpoints. The level of detail of a PSA model strongly depends on the objectives of the PSA. The range of methods which can be used for a PSA even remaining within the methods described in the current guidelines can vary considerably.

As a consequence, differences in the level of detail and the efficiency of the reviews have to be accepted. The basic requirement for a successful review is that the objectives as described in Sections 1.3 and 2 are fulfilled with a reasonable degree of confidence. This clearly means that if these objectives are not or partially not met this should be stated by the review team and appropriate proposals for extension or continuation activities should be formulated accompanied by detailed reasoning.

An IPERS review can be carried out basically at any stage of a PSA, but ideally it takes place at the beginning of the project, halfway through the project or when the project is nearly complete. This procedure allows to follow and to monitor the progress of the PSA. The advantage of an intermediate review is that corrective measures for the deficiencies identified can be taken in a timely and resource sensitive manner. Team members for the review team do not necessarily have to be the same for each of a phased review, because, if done with the same team, there is a danger that independence of the reviewers might be partially lost during the review process. On the other hand, it might be beneficial to have the same team to avoid duplication of the learning process necessary for each review.

Depending upon the scope and degree of completion of the PSA study, an IPERS would typically take one to two weeks and comprise two to six experts from several Member States with an IAEA technical officer leading the review. An IPERS main review mission can be preceded by a pre-review mission to review the documentation and translation requirements and to prepare a detailed schedule.

Specialized reviews are typically performed for areas such as:

- shutdown and low power PSA;
- internal fires and floods and external events PSA;
- external events PSA;
- Level 2 PSA (accident progression, containment analysis and source terms of radioactive material potentially released from a plant).

The review schedule, manpower and process need to be appropriately adapted for these reviews.

3.1. CONDUCTING THE PRE-REVIEW

If necessary, an IPERS main review mission can be preceded by a mission to review the status of the PSA work, the documentation and translation requirements and to prepare a detailed schedule. Typically such a pre-review lasts about one week and takes place about two months before the main review mission. The pre-review is typically carried out by the IAEA review team leader and up to two external experts for the main PSA areas to be reviewed. Preferably the pre-review group should also participate in the main review. The pre-review can be carried out nearby the facility, at the place where the main PSA work is done or at the IAEA headquarters. The results of the pre-review are documented in a report. The pre-review is typically conducted in a workshop style and a preliminary discussion of technical questions can also be included.

3.2. CONDUCTING THE MAIN REVIEW

Preferably the main review mission is performed nearby the facility studied in the PSA. For main review missions a one day plant visit is organized and one or more additional visits or walkdowns for specific aspects such as human reliability assessment and external events analysis. These visits should take place after the review team has had time to examine the PSA document together in some detail, and has identified areas to examine in greater detail. The visit should be conducted by personnel familiar with the plant design and operation. Experts should be on hand to answer detailed questions concerning the systems, plant operations and personnel training including main control room (MCR) layout and normal and emergency procedures.

The review is organized in a workshop manner with flexible working groups consisting of review team members and members of the responding team including plant staff if needed to discuss detailed questions. At a minimum one large office room providing sufficient space for the review team and the responding team and a smaller room should be available for the review.

In many of the past review missions a dedicated review secretary was available. The main task of the secretary is to compile, type and control the many technical notes or issue lists as they are traditionally called in the IPERS programme. These issue lists which form the "backbone" of an IPERS review consist of a question sheet, an answer sheet and a resolution sheet. Since the issue lists are an important communication means between the reviewers and the responding team the efficient handling of the issue lists is of primary importance for the review especially if language difficulties exist.

The review is performed using two different and complementary approaches, see Fig. 1:

(A) surface checks of the total study regarding completeness, consistency and coherence of the overall model;

(B) detailed spot checks, for example tracing one selected (representative) system fault tree from the event tree heading down to the support systems and basic input data.

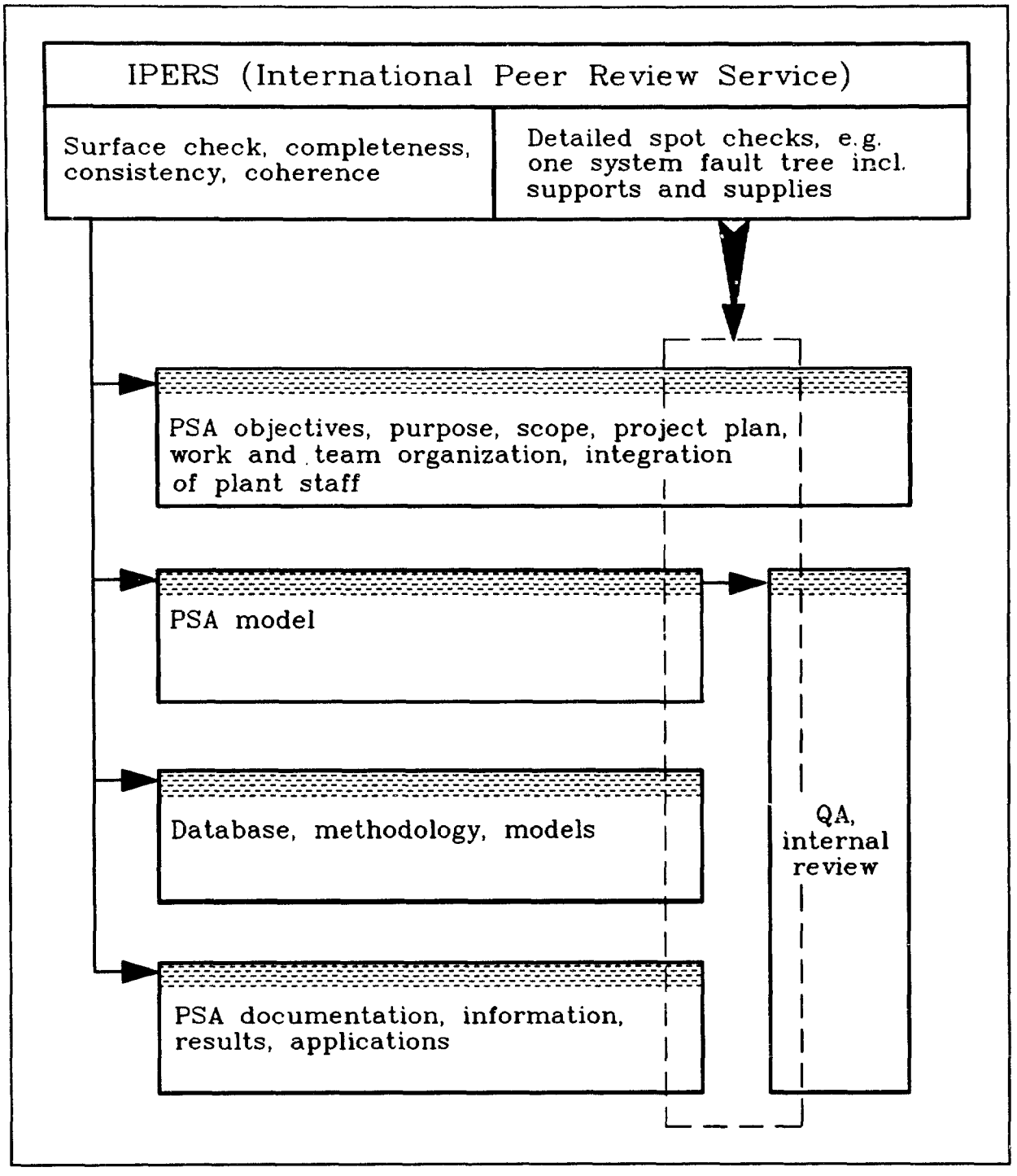

FIG. 1. Technical review approaches.

Using this procedure, it is examined that the correct approach is taken and that the methodology is appropriate. Secondarily, the procedure also ensures to some degree that the methodology is correctly applied in detail. Because only selected areas can be considered in the detailed spot checks the usual practice of the review is to generalize related findings unless the PSA team can demonstrate that these findings represent only isolated problems.

The review consists of the following steps:

(1) Discussion of the fundamental objectives of the IPERS.

(2) Discussion of objectives and scope of the PSA to be reviewed, discussion of the areas to be covered, establishment of the distribution of areas within the review team, definition of the framework and team function. Normally primary responsibilities for specific PSA areas are distributed among the reviewers which also includes the task of reporting on these areas in the review report. However, this primary responsibility is considered more as a coordinating task because the other reviewers should not been prevented to look across the borders of their own areas.

(3) Compilation of information, preliminary review of the PSA study documentation. If possible, the documentation is distributed to the IPERS team members before the review meeting takes place.

(4) Issue raising, issue answering, issue resolution process. Formulation of questions (issues) and discussion of the questions with the PSA team. A formalized technique for issue raising, issue answering and issue resolution is used as described below.

(5) Collecting responses to questions, to review more detailed documentation, to compile and resolve any further questions and to write the draft IPERS report. Communication and interactions with the analysts responsible for the PSA are extremely important for the review.

(6) Periodical discussion of findings in the review group, extending the common experience basis of group members and making use of synergetic effects. Notes are taken on collective ideas and findings and appropriate follow-up is organized.

(7) Formulation of specific and general conclusions, i.e. writing the draft report, discussion of conclusions within the review group. The review team leader coordinates the general conclusions and writing of the draft review report.

(8) Discussion of the findings of the draft IPERS report with the host organizations. The draft report is then finalized at the IAEA and sent for comments to the participants. After receiving these comments the final mission report is produced and distributed.

The formalized technique of issue raising, issue answering and issue resolution is a basic part of the review process. Appendix II gives an example for the issue forms used. The issue forms consist of three single forms:

(1) a first form for the primary issue statement or question from the reviewer;
(2) a second form for the written answer of the PSA team;
(3) a third form for the resolution of the issue by the reviewer and a statement characterizing the importance of the issue.

The purpose of these issue forms is first to document the questions, answers and resolutions in a standardized way and second to decouple the questioning and answering process during the review to avoid time consuming and sometimes emotional discussions. In order to avoid a high number of mostly explanatory issues and to assure that the questions and answers are understood by all participants, side discussions are strongly recommended. Typically about 100 significant issues are produced during a review. The issue lists represent the basis for the review report and are included in the report as an appendix. However, the issue sheets are not compulsory for all reviews. Specialized reviews, such as the review of an internal fire PSA, have been conducted without formalized issue sheets.

3.3. THE REVIEW TEAM

The peer review should be carried out by persons who are independent and have capabilities and knowledge essentially equivalent or superior to those performing the study. The peer group

should span the range of disciplines required for the study. The type of persons to be selected as peer reviewers comprises:

- Scientific PSA seniors
- Experts in special PSA areas and PSAs of specific nuclear power plants (NPPs)
- Practitioners with deep plant knowledge and broad PSA experience.

The primary requirement is the peer reviewer's ability and experience in the PSA area for a similar plant. The reviewers should be independent from the organizations performing, sponsoring and requesting the PSA. In addition, traditionally no reviewers from organizations who were competitors for the PSA contract have been admitted to the IPERS review team. Typically a review team is composed of experienced IPERS reviewers and one newcomer to the IPERS process to expand the number of experienced IPERS reviewers.

An IPERS review can cause psychological stress on the reviewers and on the reviewed PSA team. On the side of the PSA team, intensive work during many months is challenged. Usually each PSA has stronger and weaker portions and the PSA team is well aware of this. On the side of the reviewers, the challenge consists of first understanding the complex PSA study within a very short time and second to find major weak points of the PSA and to point them out to the PSA team. This situation can be accentuated by conflicting views of different organizations within the Member State, for example, between the safety authority and the sponsor of the PSA, regarding the scope and objectives of the PSA under review.

Basically the reviews are conducted using the IAEA guidelines, see for example Refs [2], [3] and [4]. However, the quality of a review depends to a larger degree on the experience and knowledge of the reviewers. Furthermore, critical issues are discussed within the review team making maximum use of the combined knowledge of the team. Therefore the ability of reviewers to work in the review team, to communicate with the other team members, and with the PSA team, is of primary importance.

Apart from the PSA team and the review group the following persons can participate in an IPERS review as observers:

- Representatives of the safety authority are recommended to take part in the review as special observers. The safety authority can also delegate contracted experts to the review.

- Member States other than the Member State requesting the IPERS may send observers to the review. The purpose of this participation usually is to gain experience either in the PSA or in the review process. The IAEA has to ask whether the Member State requesting the IPERS is willing to accept the observers. The review team leader decides what role an observer could take in the review. They can be integrated to a various degree into the review team, provided the basic principles of the review are not compromised.

The team members should preferably have previously carried out PSA analyses of the types and NPPs they are to review. For the Level 1 review, at least one team member should have a good knowledge of the specific plant design. For a review of the Level 2 part preferably at least one team member should have some experience in each basic discipline to be covered. Plant specific knowledge should be available through contacts with the analysis team members and (or) direct contact with plant personnel. There should be a strong liaison with individuals who have intimate knowledge of the plant design and operation preferably from the plant personnel.

The team should have a leader (an IAEA staff member) responsible for coordinating the individual members' reviews. Normally the team leader also takes part in the detailed review for specific aspects. The size and background of the review team should be large enough to cover the

basic disciplines involved in the PSA. For a Level 1 PSA these basic disciplines are (see also Section 5 on specific areas to be covered):

- Initiating event analyses
- Accident sequence and event tree analyses
- Systems and fault tree analyses
- Human interaction analyses
- Analyses of dependent events
- Component and systems reliability data analyses
- Quantification and uncertainty propagation
- External event analyses (if included in the PSA).

To cover these disciplines there should ideally be a team of five to six members including the team leader. This constitutes a manageable group that can interact effectively and that can review the PSA in one or two review sessions. Team sizes may vary depending on how many disciplines are represented by each team member. However, having a team of fewer than three persons can place a considerable burden on members in having to review several areas of the PSA. Review teams of more than six persons can be used, however, the responsibilities and interactions of the team members need to be especially well defined.

For a Level 2 PSA the basic disciplines are (see also Section 5 on specific areas to be covered):

- Level 1, Level 2 interface
- Probabilistic analysis
- Human interaction analyses for recovery and accident management
- Accident progression analysis
- Structural response
- Fission product release, transport and behavior.

To cover these disciplines a team of three members including the team leader should be sufficient. If Level 1 and Level 2 reviews are to be combined, the team should consist of six members (including the review team leader) with at least one Level 2 specialist involved.

For a Level 3 PSA the basic elements are as follows (see also Section 5 on specific areas to be covered):

- Level 2, Level 3 interface
- Modelling of radionuclide transport in the environment
- Food chain modelling
- Modelling of countermeasures
- Health effects of radiation
- Radiation dose models and assessment of dose.

The review team for a Level 3 PSA review should consist of three members including the review team leader.

3.4. CONSENSUS WITHIN THE REVIEW GROUP

It is important to realize that the experts do not have to agree on everything. On the other side, the users of the review, which could be the PSA team, the utility or the safety authority, will have difficulties continuing their work with a review result with major disagreements between reviewers about major items of the PSA. As an example a part of the reviewers could believe that the PSA is able to support an application, such as the identification of weak points in the plant design and subsequent decisions on upgrading. Another part of the reviewers however could believe that such an application should not be performed because major and important parts of the PSA are identified

as being deficient and have to be improved. Thus, using the present PSA could lead to wrong decisions regarding upgrading measures.

The following procedure regarding disagreement between reviewers has become the practice in the IPERS reviews:

(1) First, the review group discusses the item and tries to resolve it.

(2) If no consensus can be reached, then the review team leader (if he has the necessary knowledge and background) decides on a statement which resolves the problem in a unique way for the users. In the example above he might decide on the conservative side by recommending the opinion of the second group of reviewers.

(3) In any case, the background information and the reasoning behind the diverting opinions have to be documented and ways out have to be elaborated and documented leaving the final decision to the user of the review.

In case there is only one reviewer in a specialized area, disagreement may exist between the review team leader and the reviewer. A similar procedure is followed as described above, but in addition the review team leader could eventually recommend an extended specialized review on that specific subject.

3.5. REVIEW CONCLUSIONS AND REPORT

The review process, findings and conclusions are documented in a review report. Typically the review report consists of the following parts:

(i) an introduction containing the background information of the PSA such as a description of the NPP considered, organizations involved in the PSA, purpose, objectives and scope of the PSA and objectives of the review;

(ii) major positive and negative findings, general conclusions and recommendations;

(iii) description of detailed issues and conclusions, structured according to the main areas of the reviewed PSA;

(iv) a table with a concise list of issues and steps or recommendations to resolve the issue including also the significance of the item;

(v) a review meeting agenda;

(vi) a participants list;

(vii) a list of abbreviations used in the review report;

(viii) an appendix with the issue lists (questions, answers and resolutions);

(ix) an appendix summarizing the main and important results of the PSA.

The last two days of a review are allocated to drafting the review report including formulation of the conclusions and recommendations. A first draft of the review report should be available at the time of the final presentation of the review results. The review report is then finalized in the form of a final draft report within about one month after the review and sent to all participants for comment. Based on these comments the final review report is prepared.

4. PREPARATION FOR THE REVIEW

The individual review team members should acquire a knowledge of the design and operation of the plant in order to prepare for the review. The team members should also obtain a preliminary knowledge of the modelling and analyses that have been carried out. If possible, in order for the members to obtain this understanding, the following material should be made available to the team four weeks before the review:

(1) *Functional descriptions of safety and support systems.* These should describe: the function of the system; which components must operate; which components receive signals to change state; whether the operations of the components are manual or automatic; and what conditions must pertain for the automatic signals to be received.

(2) *System schematics for selected systems.* A system schematic should show,at least, the system as modelled in the fault tree including the connections to instrumentation and support and supply systems.

(3) *Selected functional event trees describing the safety functions required for given initiating event groups.* Performance of each safety function should be defined in terms of specific system success requirements. Functional dependencies among the systems should be identified.

(4) *Selected system specific event trees and fault trees.* Detailed event trees and fault trees should be supplied, where available, to identify the type of detailed modelling being performed. Explanation for the inclusion of human actions in the event or fault trees should be provided.

(5) *Rationale and approaches for analyses to be carried out in the different areas of the PSA (human reliability analyses, dependency analyses, data analyses etc.).* The rationale and approaches should be made available to the appropriate team members reviewing these areas. Regarding human reliability assessment a description of procedures and training should be included.

(6) *Selected component and human error data.* Samples of data should be supplied to indicate the generic and plant specific data which are being used. If a human reliability model is used to define data then the model should be specified and corresponding parameters supplied.

(7) *Information concerning plant layout.* This should cover primary systems, support systems, containment and adjacent buildings. The information should include control room and relevant local panel location and layout. For a Level 2 review information on related plant characteristics and on plant layout important for Level 2 phenomena and transport of radionuclides in the plant should be provided.

(8) *Extracts from previous PSAs for similar plants.* Deterministic and probabilistic accident progression calculations are of main interest.

(9) *Reference literature for computer codes used for deterministic calculations including plant transient analysis, particularly regarding a Level 2 review.*

(10) *Reference literature for computer codes used for consequence analysis (Level 3 review).*

Selected system descriptions, event tree descriptions and analyses selected for detailed review should be chosen on the basis of experience in past PSAs of dominant contributors and problem areas.

5. SPECIFIC AREAS TO BE COVERED

The specific areas to be covered in the review should include:

(a) Level 1

- An initiating event review
- An event tree review
- A system analysis (fault tree review)
- A dependent failure analysis review
- A human reliability analysis review
- A component data analysis review
- A sequence quantification review
- An external event analysis review (if an external events PSA is part of the study)
- A review of uncertainty and sensitivity analyses (if performed).

(b) Level 2

- A Level 1, Level 2 interface review, including binning of plant damage states (PDS)
- A review of the interface between probabilistic and deterministic accident progression analyses
- A deterministic in-vessel accident progression calculations review
- A deterministic ex-vessel accident progression calculations review
- A quantification of the containment event tree (CET) branching review
- A review of the human interaction analyses for recovery and accident management
- A structural analysis review
- A source term evaluation review
- A review of uncertainty and sensitivity analyses (if performed).

(c) Level 3

- A Level 2, Level 3 interface review
- A review of the definition of release categories
- A review of the modelling of the transport of radionuclides in the environment
- A review of transport parameters
- A review of the modelling of countermeasures and the related data assessment
- A review of the assessment of health effects and dose calculations
- A review of the analysis of economic consequences (if performed)
- A review of uncertainty and sensitivity analyses (if performed).

In addition to these areas, the following related areas should also be covered by the review:

- Presentation and interpretations of the PSA results
- The internal quality assurance process instituted as part of the PSA to validate the analyses and results
- Liaisons set up in the PSA with plant personnel and regulatory personnel and the contributions of those personnel to the performance of the PSA.

6. CONDUCTING THE LEVEL 1 REVIEW

This section presents specific guidelines for conducting the review of the Level 1 portion of the PSA. The IAEA has published guidance for performing a Level 1 PSA [2] and the review guidelines presented here are intended to be consistent with that guidance.

6.1. IDENTIFICATION AND GROUPING OF INITIATING EVENTS

The PSA should identify and include the major types of initiating events using a systematic procedure for identification. For light water reactors (LWRs) the major types of initiating events are:

- loss of coolant accidents (LOCAs);
- transients including reactivity control disturbances.

More generally, and applicable to other reactor types is the following classification of initiating events:

- Breach of primary boundary events
- Imbalance of heat generation and removal transients
- Disturbances of reactivity control.

The PSA should identify the different sizes and locations of LOCAs or breach of primary boundary events considered, which should be based on the different sizes and locations that can possibly occur at the plant (including failures of valves, in particular of relief valves). LOCAs are usually divided into large LOCAs (e.g., break size above 6 inch diameter), medium LOCAs (break size between 4 inch and 6 inch diameter) and small LOCAs (break size below 4 inch diameter). In addition, the plant response may require a different set of equipment to mitigate very small LOCAs such as pump seal failure. LOCA categories are related to the flow capabilities of the plant in terms of the available coolant makeup systems. In addition, interfacing LOCAs and steam generator tube ruptures are usually treated as special events since they can bypass the primary containment.

The reviewer should pay particular attention to the locations of the initiating events, especially interfacing LOCAs. The sizes and locations of LOCA initiating events should be categorized and grouped according to the different systems required for prevention or limitation of core damage. The rationale for system requirements during LOCA conditions should be documented including the effects of harsh environment on systems operation and should be based on plant response analyses or safety analyses.

For transient initiating events, the PSA should identify the basis for choosing an initial set of transients which is as complete as possible. Attention should be paid to the rationale for screening and grouping the transient initiating events which are finally considered. The reviewer should check that the transient reference source is compatible with standard sources of transient definitions. References [10-13] are examples of transient event sources that have been considered in PSAs for LWRs and CANDU plants. The selected transients for the plant should be grouped according to the systems required to respond to the transient. The basis for the grouping should be clearly defined. The reviewer should check for completeness in representation of initiating events in the groups, including checking that distinguishing features (e.g., a spurious trip event compared to an event demanding a trip) are represented correctly in the grouping of events.

The reviewer should select specific transient events to check the basis for the selection and the grouping. The grouping should be based on similar plant response and thus similar success requirements for frontline systems and operator response. The reviewer should assure that the success criteria used for the group are the most stringent criteria of all the individual events in the group. The success criteria, however, should not significantly vary amongst events in the group, since, if

they do, separate groups should be used. Reference [2] contains on pages 36 and 37 examples of initiating event groups for LWRs and CANDU plants.

The reviewer should pay specific attention to the plant specific features that need to be reflected in the assessment of initiating events. Typical examples of initiating events for PWRs which depend on specific plant features are given below:

- Loss of an AC (alternating current) or DC (direct current) bus
- Loss of instrument air
- Loss of service water
- Loss of room cooling
- Interfacing systems loss of coolant initiating events
- Steam generator tube ruptures
- Loss of secondary cooling through loss of feedwater, loss of condenser vacuum.

Loss of support and supply systems requires special concern because it may affect many systems and because sometimes support and supply systems have not had the same safety awareness as frontline systems. Procedures and instrumentation to enable diagnosis of problems might be less comprehensive and complete.

Since station blackout has been a dominant scenario in a number of PSAs, the reviewer should check that particular attention is paid to this event. The basis for the frequencies of the initiating events and the durations of outage times should be clearly documented. There should be clear interfaces between the event tree tasks and the database analyses. There should be clear connections between the duration of the loss of power, and the associated event trees defining the loss of power sequences and resulting effects such as pump seal failures.

Plant specific operating experience should also be analyzed to identify any plant specific transients which need to be considered in the PSA.

A systematic analysis, e.g., using failure mode and effects analysis (FMEA) of all the support and standby systems should be carried out 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.

Further points that should be considered in relation to plant specific initiating events are as follows:

- The PSA should consider the effects of losing normally operating systems, or their subsystems, that also have safety functions after a reactor trip. Examples of such systems include service water systems, power supply buses, DC systems and air systems. The fault tree approach for identifying potential initiating events, or its equivalent, can be used to enumerate and classify candidate events.

- Loss of component cooling and loss of ventilation, as support functions, should be assessed. Loss of cooling to solid state components associated with instrumentation should also be considered.

- 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.

- The reviewer should select particular plant specific initiating event analyses for more detailed review. The process for identifying interfacing systems LOCA initiators should be reviewed to ensure that the investigation is complete and the frequency calculations are correct.

- Although analysis of plant specific initiating events is sufficient to evaluate whether a loss of a system or component can cause a reactor trip, the logic is generally insufficient to determine whether a failure or actuation increases the unavailability of a safety system and to what degree. The reviewer should check that adequate interfaces have been set up between the systems analysis tasks, the event tree analysis tasks and the initiating event identification tasks to deal with this question.

The review should make a comparison of the finalized initiator groups and frequencies with other, similar PSAs to ensure completeness and accuracy.

6.2. ACCIDENT SEQUENCE (EVENT TREE) ANALYSIS

Event trees are developed in order to depict the sequence of events or accident sequences originating from the groups of initiating events. Prior to the construction of detailed event trees, functional event trees are usually developed in the PSA for each of the different groups of initiating events. Based on the functional event trees the detailed event trees can then be derived and the headings can be organized in a functional way. The human actions required to operate the systems can be identified and attributed to these functional event trees. Event sequence diagrams (ESDs) can be used to define, identify and document in detail the human actions. If the plant has well developed emergency procedures then these are examined to determine the key human actions necessary to avoid core damage. The reviewer has to check whether the system analyst and the HRA analyst have jointly determined all the key human interactions. Determination of the key human interactions and related background information is of primary importance, no matter which HRA modelling process is used afterwards, since this will define the HRA parameters. The organization of the event trees should reflect the accident progression in the way that dependencies with respect to equipment and human actions are correctly covered and depicted. Sometimes the sequencing of events in the trees is reorganized without considering whether it affects proper consideration of dependencies. The success criteria for the system to satisfy each function in the event trees should be defined. The system success criteria and their relation to the functional event trees should be clearly documented.

Specific points to review in the detailed event trees are the following:

- Detailed descriptions of the event trees and their associated assumptions should be given, including descriptions of conditions created by the initiator and the chronological requirements to systems operation for the different event tree branches.

- Success criteria for the systems required in each event tree should be explicitly defined and justified. The success criteria for front line systems should be expressed in terms of performance criteria (flow, response time, etc.) related to functional requirements. These should in turn be expressed in terms of hardware requirements (number of trains required, etc.). Mission time requirements should be justified from functional and operational standpoints. Support system requirements should be based on success criteria for front line systems.

- The success criteria should be based on realistic assumptions which are justified by appropriate analyses. The reviewer should check that success criteria are consistent with those in PSAs on similar plants and, if differences exist, that they are explained. Sensitivity analyses should be performed if the effects of different success criteria are in question.

- The success criteria of a system should be checked to determine whether it depends on the prior success or failure of other safety systems. An example for this is the requirement of one-of-two trains of the low pressure injection system (LPIS) after success of two-of-three accumulators in case of a large LOCA event tree in PWRs.

- Criteria for what constitutes core damage and to identify sequences as causing core damage should be clearly stated. For each sequence so identified, there should be a clear explanation

as to why it is identified as causing core damage. The sequence end states can include core damage (reflecting prolonged core uncovery), 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 LWRs 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 considered to obtain a realistic definition of core damage.

- If simplifications or assumptions are made in the event trees, their effects should be clearly identified and justified.

- In the sequence descriptions, an important aspect is the timing for system actuations and operator actions. The timing is an important input for human reliability analysis and should therefore be explicitly identified for each sequence and rationale should be given.

- If expert judgement is used to estimate available time frames, the basis for the judgement should be checked. Personnel from the operations organization of the plant should have taken part in the estimation process. If the time frames are derived from thermohydraulic analyses, then the details should be available for review.

- After reviewing the event tree preparation process and documentation, the reviewer should select an event tree and go through its preparation process in detail to assess the adequacy of the modelling, assumptions, simplifications and timing estimations. The reviewer should check for any neglect of accident scenarios resulting from omission of relevant systems. Event trees that have been found to be important contributors to the core damage frequency in past PSAs for similar plants should be the primary focus of the review.

- The reviewer should check that the personnel who prepared the event trees communicated with the personnel who participated in the systems analyses, human reliability analyses and sequence quantifications in the development of the event trees. The event tree specialist should have coordinated event tree development to ensure correct dependencies are taken into account.

- If the different system success requirements in the event trees are modelled by means of house events in the system fault trees, then the house event descriptions should be reviewed and the interfaces with the respective event trees should be checked.

- The event trees for PWRs should be reviewed regarding the impact of reactor coolant pump (RCP) seal LOCAs during loss of RCP seal cooling conditions. RCP seal LOCAs have been shown to be important contributors to risk at some PWR plants.

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

- The binning of core damage sequences into plant damage states should be reviewed if performed as part of the study. It is necessary to group accident sequences into plant damage states in order to extend the assessment to the Level 2 portion of the PSA. To do this, the core damage accident sequences are characterized according to the general physical plant state to which each accident sequence leads and to the availability of plant systems. Information from other sources (e.g., from previous PSAs for similar plants) should be useful in defining the plant damage states.

  The definition of the plant damage states should be determined by considering the characteristics of each core damage sequence:

- the initiating events (e.g., LOCA, transient);
- failure of safety systems designed to cope with the initiating event (e.g., reactor protection system, emergency core cooling system (ECCS), containment systems);
- RPV pressure (high, low) at the time of core damage;
- early core damage versus late core damage (relative to time of scram);
- containment failed prior to or after core damage (both structural failure and isolation failure should be considered);
- containment bypass (those sequences of interfacing system LOCA type);
- LOCA with or without pressure suppression (boiling water reactors (BWRs));
- pool subcooled or saturated when core damage occurs (BWRs);
- availability of containment sprays;
- availability of containment heat removal;
- availability of AC power and recovery times;
- condition of reactor at vessel failure (water flooded or dry).

The plant damage states must be defined through a cooperative effort between Level 1 and Level 2 analysts. The reviewer should verify that the process for defining plant damage states is sound and that the interfaces between the Level 1 and Level 2 analysis is technically correct. For further guidance in this area, see Section 7.2.1.

6.3. SYSTEM (FAULT TREE) ANALYSIS

Fault trees should be developed for each system failure mode identified in the event trees. To provide a valid and auditable basis for the fault trees, the reviewer should determine that functional descriptions are clearly documented for each system for which a fault tree is devised. The functional descriptions should describe the function of the system; the components that must operate and their normal configuration; the components that must 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 to the functional descriptions, a simplified schematic system diagram should preferably also be drawn for each system for which a fault tree is developed. This system schematic should be a simplification of the plant system diagram and should show the system as modelled in the fault tree. The schematic should show the components and their normal configurations identified in the fault tree and the pipe segments or wiring segments connecting the components. The support interfaces (power, cooling, etc.) should be clearly identified in the system schematic. The detailed fault trees should clearly describe the fault states and fault conditions. Assumptions made regarding normal component states and operability conditions should be clearly documented as part of the tree. The reasons for terminating development of the tree should also be clearly documented. Finally, interfaces with the event trees and other fault trees should be identified.

It is also useful to have simplified schematics for the control wiring of remotely operable components. Instrumentation is generally not included in the 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. The reviewer should also check that interfaces with plant personnel were established to check the accuracy of the schematic. If possible the reviewers should also check schematics of special interest at the plant.

Additional, specific points requiring attention in the systems analysis review are as follows:

- Hardware dependencies should be explicitly modelled in the fault trees. These hardware dependencies include all functional dependencies within the same system. The hardware dependencies should not be included in the "residual" common cause failures that are reserved for more ambiguous dependencies and are quantified by means of beta factors and similar approaches.

- If separate systems perform the same function and have intersystem dependencies, these should be examined as well. Shared component dependencies should be explicitly identified in the fault trees for different systems (or different system failure modes) containing the same component.

- If the limit of resolution for the fault trees is based on consistency with available component reliability data, the reviewer should check that the component boundaries and component failure modes are consistent with those defined in the component failure database.

- The reviewer should also check that the degree of resolution of components is not so gross so as to hide hardware dependencies. One important example involves the cooling of a pump. The pump failure mode caused by cooling equipment failure is generally included in the overall pump failure rate. However, cooling sources and cooling interfaces still generally need to be explicitly modelled in the fault tree to identify possible dependencies caused by multiple pumps having the same cooling water system or water sources.

- This hiding of hardware dependencies should also be checked if components are grouped together into "super components", or modules. Super components or modules should all be functionally independent and should not contain the same components.

- Hardware dependencies can also enter through the secondary support systems for components and subcomponents and hence all support system interfaces should be shown on the fault tree. Examples of secondary support systems are 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 reviewer should verify that the system logic model includes common cause failure events for component groups and that the component groups selected are complete and modelled correctly for each important failure mode.

- The reviewer should examine the treatment of maintenance in the fault tree analysis to ensure that proper allowance for maintenance unavailability is made. The modelling of maintenance unavailability should be consistent with the way the system is actually taken out of service for maintenance and consideration of 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. Maintenance configurations that are prohibited by the technical specifications or operating procedures should not be modelled in the fault trees.

- The success criteria of a system can vary from sequence to sequence depending upon the event tree initiator and sequence of events prior to the demand for the system. The dependency of system success criteria on the initiator and event tree sequence conditions should be checked carefully by the reviewer, and the PSA should provide clear documentation showing these interrelationships. It is desirable that the PSA includes a table summarizing system success criteria for important accident sequence conditions.

- The reviewer should choose selected fault trees and review in detail their development. The system functional description and the system schematic should be sufficiently clear to allow the fault tree to be reviewed in detail. Systems that have been shown to be important contributors to the core damage frequency for PWRs and BWRs should be reviewed first. One selected important frontline system should be reviewed including its supports and supplies.

6.4. ANALYSIS OF DEPENDENT FAILURES

Dependent failures are often dominant contributors to core damage frequency and to other PSA results. The reviewer should therefore pay special attention to the treatment of dependencies in the PSA. The different types of dependencies include:

- initiators that cause safety related system failures ("common cause initiators");
- functional dependencies;
- human interaction dependencies;
- component failure dependencies (common cause);
- external events (including fires and internal flooding).

Initiators that cause safety related system failures ("common cause initiators")

Some initiating events have a potential to simultaneously degrade or fail safety systems required to respond to the initiating event. The common cause transient initiators to which particular attention should be paid include:

- Loss of an AC or DC bus which causes a transient and also degrades one or more safety systems or causes it to fail.
- Loss of instrument air that causes a transient and causes failure or degradation of instrumentation or air operated components.
- Loss of service water that causes a transient and a loss of cooling water supply or flooding.
- Interfacing loss of coolant initiating events (interfacing LOCAs) that occur when high pressure coolant flows back through low pressure piping owing to a valve failure. These events cause LOCAs which, because of their location, also can fail the emergency core cooling system (ECCS) due to harsh environmental conditions or flooding.

Functional dependencies

Functional dependencies occur between systems or components because the function of one system or component depends on the function of the other system or component. 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. Typically this type of dependence is explicitly modelled in the fault trees or in event trees.

Functional dependencies include:

- shared component dependencies;
- actuation requirement dependencies;
- isolation requirement dependencies;
- power requirement dependencies;
- cooling requirement dependencies;
- indication requirement dependencies;
- ventilation requirement dependencies;
- phenomenological effect dependencies.

The reviewer should select some of these dependencies to review in detail.

Human interaction dependencies

Interactions between operator actions or multiple component failures due to common maintenance errors have been particularly critical in past PSAs. The reviewer should check that the following human interaction dependencies have been addressed by the PSA:

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

The reviewer should check that all these activities have been identified, evaluated and documented. The reviewer should determine in particular how the activities were screened and assessed for human interaction dependencies. Specific assessments should be investigated for the data used and the quantifications that were carried out.

Component failure dependencies

These dependencies cover those failures of usually identical components which are otherwise not analyzed. Such common cause failures may be caused by design, manufacturing, installation, calibration or operational deficiencies and are treated quantitatively by common cause failure probabilities or other dependence quantification approaches. Common cause failure probabilities are usually quantified by using the alpha factor approach, the beta factor approach or the MGL (multiple Greek letter) approach to assess the probabilities of failure of other components given that one component has failed. Reference [7] contains additional guidance in this area.

The reviewer should check that these potential dependencies have all been covered in the PSA, have been modelled correctly in the fault tree, and have been quantified correctly and documented. It is particularly critical that the selection of common component groups was performed correctly to ensure that important common cause failure groups were not omitted. The reviewer should determine how the above potential dependencies were screened for and how their probabilities were assessed. Consistency of common cause failure probabilities with past experience should be checked.

6.5. 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 in the event sequences, incorporation of these actions in the plant logic model (event and fault trees) and quantification of the related events.

Guidance in the organizational aspects of HRA is contained for example in the SHARP (systematic human actions reliability procedure) framework, Ref. [14]. The review should examine the HRA process used by the PSA team to ensure that the HRA approach has been systematic and covers the following important steps:

- Identification of HIs (human interactions)
- Establishment of the importance of the actions (qualitative and quantitative screening)
- Incorporation of the actions into the appropriate parts of the logic model
- Selection of suitable HRA models
- Quantification of the human interaction events.

It is very important that the human reliability analysis (HRA) is performed in a structured and logical manner and that all steps of the analysis are documented in a traceable way. This is due to the fact that there is a wide variation in available methods for performing HRA and the state-of-the-art in this area is still evolving. Consistent application of the HRA methods selected is the critical factor in a successful HRA. The SHARP framework provides a general framework for guiding an HRA to ensure that all of the key HRA elements are included in the process. If the plant specific HRA has not followed the SHARP framework, it is useful to compare the HRA process utilized to the SHARP steps to verify that the HRA process is complete. It is important to realize that SHARP is only a framework for guiding the overall HRA, and does not prescribe specific methods for performing the actual quantification of human error probabilities (HEPs). The human error probabilities are derived

by using the THERP [15] (technique for human error rate prediction) method, the HCR [16] (human cognitive reliability) method, SLIM [17] (success likelihood index method), or some other available method as discussed below.

SHARP identifies a number of steps which cover the above process in more detail. One important step of the SHARP framework describes screening. The objective of screening is to minimize the necessity for detailed modelling and quantification of all human actions in the logic model. This is done by assuming first conservative screening values for the human error probabilities. Detailed modelling and quantification is then only done for the HIs contributing in a significant way to the total core damage frequency (CDF). The reviewer should examine the screening guidance carefully to ensure that the screening process does not eliminate any human actions from detailed consideration which are significant for core damage.

The objective of another SHARP step ("breakdown") is to amplify the qualitative description of each key HI identified and to identify the major elements of the key HIs. The purpose of this step is to ensure that the analyst has determined all the significant aspects associated with the action of the plant personnel including timing of the action, envelope of information available and influence of prior actions. The reviewer should look for information in the PSA documentation which addresses these issues, to ensure that the PSA team understands the situational influences on the plant personnel during the accident scenario.

Human interactions (HIs) are usually classified as one of the three types:

Type A: Pre-initiator human interactions that may affect system unavailability
Type B: Human interactions that cause an initiating event
Type C: Post-initiator human interactions which are performed during the sequences caused by an initiating event.

The human reliability analysis should be focused on the requirements which are associated with each of these different types of actions.

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 analyzed using the THERP method. However, this is not the only method and other methods may have been used. The reviewer should verify that important Type A actions have been identified and included in the assessment in a thorough and consistent manner, so that none are overlooked. 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 reviewer should check that the maintenance and test departments practices to minimize human induced dependencies, such as the use of different crews for redundant trains, are reflected in the HRA. The reviewer should also verify that the quantification process was done correctly. It is also helpful to review plant experience for Type A human errors. The reviewer 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. Single faults, however, usually do not represent a problem.

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. However, if a human error has actually caused an initiating event as documented in the plant history, this would be accounted for in the initiating event analysis.

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. Unfortunately, they are also the most difficult ones

to analyze since there might be cognitive aspects in the operators response. There are a number of available methods to analyze these actions, such as the HCR model, THERP, SLIM, and others. However, the state-of-the-art in this area is still evolving. Regardless of the method chosen for analyzing Type C human actions, the same review criteria as for Type A actions should be evaluated: that the process for identifying Type C actions to analyze is thorough and complete (none are overlooked), that the quantification process was performed accurately and consistently, and that input and review from the plant operators has been included in the evaluation if possible. In some cases, the results of simulator observations may have been incorporated into the process.

To assess pre-accident (Type A) human actions validly, 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 times required to restore the components that are in a reconfigured state;
- 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).

The reviewer should check that all this information is given in the PSA. Specific evaluations of the probabilities of human error should be reviewed to assess the data and quantification techniques used.

To assess post-accident (Type C) operator actions validly, the PSA should have clearly identified and documented two sets of actions:

(a) post-accident operator actions required for systems to operate successfully;
(b) 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. The reviewer should check that all this information is available in the PSA and has been properly documented. If expert judgment methods, such as the direct estimation approach, are used, the reviewer should examine the process carefully as to how the process was carried out. The review should cover the detailed description of HIs, the situational influences with regard to the event sequences or scenario, the selection and number of experts and the elucidation process. The involvement of plant personnel in the assessment and modelling process should be looked for. For cases when there are no developed procedures, the model building process should be examined very closely. The reviewer should check whether the methods selected are adequate for the assessment of human interactions for which no (or no written) procedures are available.

The reviewer should review specific evaluations of human error probabilities to assess the data and quantification and to determine their consistency with the approach used. Checks should be made to see whether the estimated probabilities are sensible with regard to influences and assumptions made. It is also very important to identify any cases where more than one operator actions are combined together in the same sequence and to ensure that any dependencies between the actions have been accounted for.

The second set of operator actions, those required to recover specific minimal cut sets of accident sequences, include those recovery actions that are intimately linked to combinations of events (the minimal cut set events). The PSA should identify and justify the specific rules used for excluding and including recovery actions. The rules should cover the feasibility of the recovery actions. Modelling of the HIs should 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 should be verified that if their probabilities are independent there are no dependencies between the actions or if they are dependent then the dependency is accounted for.

In the recovery actions that have been included, the time to diagnose and correct the failures (this may mean that coordination is required between the 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 should all be identified, justified and documented.

If screening values were used initially to help focus the analysis effort, it is very important to verify that the screening values represent an upper bound for the human error probability. For all human actions that appear in important cut sets using the initial screening values, a detailed HRA should be performed. It is important to also 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 dependent HI probability is set to 1.0 to ensure that the related human action dependency is not eliminated in the process.

The reviewer should be aware of how the various HIs are incorporated into the plant logic model. 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 type C actions included in the top logic should be those actions which are considered to be key or critical actions and failure to perform these actions could lead to core damage. Examination of the procedures may reveal other operator actions which are linked to these critical actions, but are directly associated with plant equipment operation. These latter HIs should be incorporated into the fault trees. An example is RHR (residual heat removal) operation actuated by the operator. The cognitive part of that action is incorporated at the event tree level and the associated action to start an oil pump to support RHR pump operation is included at the fault tree level.

6.6. INITIATOR AND COMPONENT DATA ANALYSIS

For initiating event frequencies, the reviewer should verify that an analysis of plant specific initiating events was performed if the plant has been in operation for more than a few years. The frequencies of normally occurring transients should be based on the plant specific data, if available. 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. For those initiators that cannot be quantified using plant experience, generic initiator frequency data can be used instead. The reviewer should check the completeness and technical accuracy of the initiator frequency estimates.

In some cases, such as the initiators due to loss of plant support systems, fault trees may be used to estimate an initiator frequency. For this kind of analyses the reviewer should check whether the following aspects are correctly handled:

- Most of these systems are operated with parts, trains or components of the system in on-line mode and redundant parts, trains or components in standby. For example, a three train compressed air system is usually operated with one train in operation, a second train as a first backup and the third train as a second backup. After one month of operation in this mode, the order of the trains is rotated. The first train is stopped and replaced by the second train. Thus

the former second train becomes now the train in operation and the former third train first backup. Usually some preventive maintenance is made at the formerly operating train, now in second backup. The reviewer should check whether a reasonable reliability model is used to depict such system including consideration of specific operation modes, scheduled and unscheduled maintenance. If system fault trees from the sequence analysis are used to estimate initiating event frequencies, it should be checked whether the necessary modifications and extensions have been made in a correct and consistent way.

- Many of these systems have passive or active elements which are common to redundant trains or components. For the compressed air system there are usually common headers. If the failure of these common elements potentially fails system operation, they need to be considered when evaluating the frequency of an initiating event.

- Some of the fault tree evaluation programmes, in principle, cannot handle correctly the combination of the expected number of primary failures (or frequency) and conditional secondary failure probabilities existing in initiator fault trees. The reviewer has to check whether a method is used to correctly evaluate the initiator fault trees.

- After an initiating event caused by the failure of a support system it has to be assured, that the failures assumed for the initiating event are correctly propagated to and handled in the sequence analysis.

The component data cover information on failure modes, component failure rates and unavailabilities, surveillance test intervals, maintenance intervals, maintenance and repair durations. The following specific points should be assessed in reviewing the component data analysis of the PSA:

- Selection of generic data for each type of component 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 should be given.

- Standby component failure rates should generally be in rates per hour. If rates are given per demand (per cycle) there should be appropriate explanation of how the numbers were derived.

- If standby component failure rates are given per demand in the generic data sources, they generally should be translated to per hour failure rates by dividing them by one half of the appropriate surveillance test interval.

- The PSA should consider the use of plant specific experience and generic data in obtaining the final estimates and associated uncertainties for the PSA quantification. Bayesian approaches have been used for the combination process. Care should be taken, however, that the generic data and Bayesian priors are consistent with plant specific data.

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

- Poisson distribution approaches for time related events should be used for the data analysis. Binomial distributions should be used for demand related events, when this is justified.

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

- The results of the generic and plant specific data analyses should be shown in a table that gives for example the median and mean estimates and associated 95% and 5% probability limits.

- Mission times that are used for operating failure rates need to be justified. The mission time definitions should include considerations of minimal times to access or replace the components.

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 analyzed. If a plant specific analysis has been performed, the reviewer should do a spot check to determine if the calculations were performed correctly. If generic data is used, the reviewer should verify that the source is fairly recent and is recognized as an acceptable source. The frequency of unscheduled maintenance should be assessed in a conservative way. If no experience data is available, an established, conservative approach is to increase the failure rate for catastrophic failure by a factor of 10 to assess the frequency.

Further guidance in this field may be found in Section 5.3 of Reference [2]. Appendix I 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. [18].

6.7. QUANTIFICATION OF ACCIDENT SEQUENCES

The quantification process for PSA sequences uses initiating event definitions, event trees, fault trees, dependent failure analyses, human reliability analyses and data analyses to produce the quantified PSA results. The reviewer should verify that the PSA quantification process is technically correct and thorough, and that key dependencies are correctly accounted for in the quantification process. For cases where screening values are used, e.g., for HRA or common cause failure (CCF) assessment, the choice of cutoff probabilities for selection of events for which a more detailed assessment is required should be reviewed to ensure that key contributions are correctly quantified in the final iterations.

The PSA reviewer should next check that sufficient PSA results are calculated in the accident sequence quantifications to quantify the PSA comprehensively. The PSA results that are calculated should include:

- the mean core damage frequency (with 95% and 5% confidence bounds if an uncertainty analysis is performed);
- the mean core damage frequency for each plant damage state (with 95% and 5% confidence bounds if an uncertainty analysis is performed);
- the mean accident sequence frequency for each dominant accident sequence (with 95% and 5% bounds if an uncertainty analysis is performed);
- The mean accident sequence frequency for each initiating event type (with 95% and 5% bounds if an uncertainty analysis is performed);
- the mean system unavailability for each system failure mode in the event trees (with 95% and 5% bounds if an uncertainty analysis is performed);
- the percentage contribution of each plant damage state to the mean core damage frequency;
- the probability and the percentage contribution of each dominant accident sequence to the mean core damage frequency, and a description of each sequence;
- the contributions of the dominant minimal cut sets to the mean core damage frequency, each mean plant damage state frequency, each mean accident sequence frequency and each mean system unavailability;

- the Birnbaum importances and Fussell-Vesely importances of the dominant component contributors to the mean core damage frequency, each mean plant damage state frequency, each mean accident sequence frequency and each mean system unavailability;
- Risk Reduction and Risk Achievement Worths for basic events represented in the plant model;
- Results of sensitivity studies on high importance contributors and on all important assumptions, models or data values;
- A ranked list of the dominant human actions should be provided for each plant damage state and for the mean core damage frequency.

Specific points include the following:

- The failure probability of a system can vary from event tree to event tree depending upon the event tree initiator and the sequence of events prior to the demand for the system. The dependency of system failure probability on the initiator and event tree sequence conditions should be checked carefully by the reviewer, and the PSA should provide clear documentation showing these interrelationships. It is desirable that the PSA includes a table summarizing failure probabilities for various accident sequence conditions.

- The reviewer should check that the computer codes used are subject to a quality assurance (QA) programme to ensure that they are capable of correctly determining the minimal cut sets and correctly quantifying the PSA.

- The reviewer should check that there is a systematic, quality controlled process for determining the minimal cut sets to be used to quantify the system unavailabilities, accident sequence frequencies, plant damage state frequencies, and core damage frequency. The reviewer should specifically check that the support systems are validly included in the minimal cut set determinations, and that the different fault trees are validly combined to obtain the minimal cut sets for the accident sequence.

- The reviewer should check that the proper quantification formulae are used to calculate system unavailabilities and accident sequence frequencies from the component unavailabilities, initiating event frequencies and human error probabilities.

- The Boolean reduction of sequences with system success states and system failure states should eliminate the minimal cut sets in which the failed states of components are not compatible with the success states of the same or other components (for example, a pump's failure to start and then succeeding in operation are incompatible).

- If cut sets have been truncated in the analysis, either through the use of a cutoff probability or maximum cut set order, the reviewer should check that this truncation has not introduced errors into the results or the logic of the PSA. This is particularly important if it is intended to use the PSA for making operational decisions where setting a component failure probability to unity will increase the probability of a cut set containing that component and reduce its order.

- If common cause failures and human dependencies are quantified at the sequence level after a truncated set of minimal cut sets has been obtained, the reviewer should check that the truncation criteria used in the PSA do not lead to cut sets being truncated that could be important if common cause failures, dependencies and uncertainties are considered.

- The reviewer should check the process of quantifying dependencies at the sequence level to ensure that all dependencies identified are systematically quantified. He should also check the process of including recovery factors after the initial sequence quantification to make sure that they are properly included.

- Where applicable, with regard to uncertainty analyses, the reviewer should assure that uncertainties are properly quantified and propagated. Uncertainties should be correlated when the same data value is used for a group of components or different events.

6.8. EXTERNAL EVENT ANALYSES

The guidelines for the review of the external event analyses performed are divided into review guidelines for the external events selected, review guidelines for seismic analyses, review guidelines for internal fire analysis and review guidelines for internal flood analysis. The review guidelines for the external events selected in the PSA cover the screening of external events to determine which are potentially important contributors to core damage frequency. The subsections on seismic analysis, internal fire analysis and internal flood analysis cover additional points to review in these specific external event analyses.

External event selection

The PSA should clearly identify the basis for selecting the external events that are analyzed in the PSA. If external events are selected (screened) according to their potential contribution to core damage frequency, the screening criteria for selecting the external events should be clearly identified.

In the screening process, the estimated frequency of an external event beyond the design basis is usually compared with the core melt frequency from internal event contributors to determine whether the external event frequency is negligible under the conservative assumption that if the design base limit is exceeded, core damage occurs. If the external event frequency is negligible compared with other contributors to core damage frequency, the external event can be neglected. Otherwise, more detailed analysis of the external event should be performed, including estimation of the actual likelihood that core damage occurs if the design limit is exceeded. The reviewer should check that such a valid screening approach, or other equivalent approach, has been taken.

After the screening analyses, the reviewer should assess the validity of the more detailed external event analyses. This involves assessing whether the data of external event frequency versus severity is consistent with appropriate historical data. It also involves an assessment of whether the probabilities of failure of components for external events of given severities have been validly estimated. Finally it involves assessing whether the probabilities of failure have been properly combined using the accident sequence minimal cut sets of the PSA, accounting for dependencies between the failures in the same minimal cut set.

Seismic analysis

Seismic analyses in a PSA generally include the following steps:

(1) Estimation of the frequency of seismic events as a function of their severity, which is often characterized by the peak ground acceleration. This is often referred as the seismic hazard curve.
(2) Calculation of the transmission of the seismic event from the source to determine the severity at the plant.
(3) Estimation of component and structural failure probabilities (fragilities) as a function of seismic severity.
(4) Evaluation of physical dependencies between components due to the seismic event.
(5) Estimation of the effects of the seismic event on the possibilities for and probabilities of human error. This should cover loss of instruments as well as psychological factors, like increased stress.
(6) 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.

The reviewer should 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 should be reviewed to determine that they are consistent with accepted data and models used in these areas.

Additional specific points that should be reviewed are the following:

- The estimation of the curve of the seismic frequency as a function of severity (seismic hazard curve) should be 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 cutoff for the curve should be identified and justified.

- The model used for the transmission of the seismic events to the plant should account for the structure of the soil around the plant. The possibility of soil liquefaction should be considered.

- The assessment of component and structural fragilities should utilize accepted log-normal approaches or stepwise approaches. Uncertainties for the fragility curves should be quantified and be documented. Sources for the fragility curves should also be documented.

- Evaluation of physical dependencies between components should 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. The evaluations should 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.

- Estimation of the effects of the probability of human error due to the seismic event should identify 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 should 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 melt 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 maxima of the component fragility and the component unavailability due to internal plant causes should be used as the component unavailability in these calculations.

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

Additional guidance to support the seismic analysis review may be found in Reference [6].

Fire analysis

Fire analyses in a PSA generally comprise the following steps:

(1) Initial screening to eliminate fire scenarios in rooms that are small contributors to plant risk.
(2) Estimation of the frequency of fires of different size starting in different rooms of the plant.
(3) Assessment of the type of plant disturbance potentially caused by a fire.
(4) Calculation of the propagation of the initiated fire and propagation of fire effects to affected components and operators.

(5) Estimation of non-detection and non-suppression probabilities for the initiated, propagating fire.
(6) Evaluation of component dependencies and component failure probabilities due to fire effects.
(7) Estimation of the effects of the fire on human actions and possibilities for increasing the probabilities of identified human errors.
(8) 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 reviewer should 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 are the following:

- The documentation should clearly state 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, should 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 should be referenced so that the reviewer can check for consistency between the databases and the data for the plant analyzed.

- 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 should 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 should be reviewed to determine whether they represent the actual plant. These parameters to be reviewed should include the amount of permanent or transient fuel available in each zone. The transmission of smoke through ventilation ducts and the heating of instrument and component compartments should be included in the propagation analyses.

- The probabilities of non-detection and non-suppression should be 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 and human error effects related to the fire should take account of the effects of smoke (through ventilation ducts) and hazardous effects due to materials in fire suppression systems.

- Effects on the operator also should include effects of fire on the availability of instrumentation and related equipment.

- The quantification of fire barrier efficiency should be documented by the PSA. The reviewer should 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 lead to high human error probabilities (HEPs). This should be revealed in the PSA.

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

- The results of the fire analysis should be as clearly presented and structured as the rest of the PSA analysis. Sensitivity analyses should be performed on the areas of the analysis where especially questionable assumptions have been made.

Internal flood analysis

The internal flood analysis usually comprise the following steps:

(1) Initial screening to eliminate flooding scenarios in rooms that are small contributors to plant risk.
(2) Identification of the possible water and steam sources.
(3) Assessment of the type of plant disturbance potentially caused by the flooding.
(4) Evaluation of the frequency of occurrence of an initiating event caused by these sources.
(5) Estimation of the likelihood that the operator does not detect the effects.
(6) Identification of the components that are affected by the flooding.
(7) Calculation of the frequency of core damage due to internal flooding by combining the initiating event frequencies with the probability of occurrence of the accident sequence.

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

Specific points to focus on are the following:

- 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 floodings on plant operation should include component or system actuation due to flooding effects which could initiate special sequences.

- The frequencies of initiating events should first be screened for their potential contribution to the core damage frequency. Initiating event frequencies that are lower than the frequencies of internal event core damage sequence probabilities 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. The possibility of flooding from one room to another through equipment drains should be assessed.

- All potentially contributing initiating event frequencies should be evaluated with regard to the means of detecting the event. The means of detecting the event should 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. These include, for example, inadvertent isolation and subsequent restoration of the power conversion system. Considerations of operator confusion should be covered in the HRA because of loss of equipment and spurious indications.

6.9. SENSITIVITY AND UNCERTAINTY ANALYSIS

The purpose of sensitivity analysis is to address those modelling assumptions suspected of having a potentially significant impact on the results. These assumptions are generally in 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 and evaluating their individual impacts on the results. The reviewer should verify that sensitivity analyses have been performed on all PSA inputs that significantly impact the results. Section 6.5.2 of Reference [2] provides additional guidance in this area.

The objective of uncertainty analysis is to provide qualitative discussions and quantitative measures of the uncertainties in the results of the PSA, namely the frequency of core damage, the frequency of plant damage states and the dominant accident sequences. Uncertainty analysis is an important task of a PSA. This activity is discussed in detail in Section 6.4 of Reference [2]. This reference should be used to assist the PSA reviewer in this area. The primary focus of the review should be to ensure that the uncertainty analysis process is technically accurate, and that the uncertainties have been propagated through the models correctly.

6.10. ORGANIZATION AND PRESENTATION OF THE PSA

The reviewer should check whether the results of the PSA are presented in a clear and balanced manner. The bottom line numbers should not be the principal focus of the PSA. Instead the important contributions found and the findings regarding plant strengths and plant vulnerabilities should be emphasized. The critical human errors and the dependencies that have been found should also be emphasized.

Specific points that can be focused on include:

- The comprehensive list of the assumptions and constraints of the PSA including the HRA should be clearly stated.
- A description of the plant should be included in the PSA report to provide sufficient detail to enable understanding of initiating events, the mitigating systems and their interdependencies.
- The methodology should be described in a logical and complete manner.
- The scope assumptions and constraints of the PSA should be clearly stated.
- The results should be traceable to the associated analyses, models, assumptions and data used.
- The important contributors and findings should not only be tabulated but associated explanations and discussions on their relevance should also be given.
- The dominant event sequences and dominant contributors should be described in a manner understandable to the non-specialists.
- Conclusions and recommendations, including applications to operation and design implementation should be highlighted in the result presentations.
- The PSA model should be organized so that the minimal cut sets, fault trees and event trees will be traceable for individuals who have not been intimately involved in the analyses.

7. CONDUCTING THE LEVEL 2 REVIEW

7.1. INTRODUCTION

The intention of this chapter is to provide the reviewer with guidelines for the review of a Level 2 analysis, either in parallel to a Level 1 review or independent of a Level 1 review. These guidelines should provide information for the review of an all inclusive Level 2 analysis. The all inclusive Level 2 analysis referred to here is defined as an analysis that calculates the magnitude, timing, frequency, energy and the composition of the source terms from severe accidents in a nuclear power plant.

It is also the intention of these guidelines to be useful while reviewing a Level 2 analysis that is not all inclusive as defined above. Two examples of analyses that are not all inclusive are first an analysis that calculates containment failure probabilities, but does not provide source term information and second an analysis that considers a few sequences or plant damage states deterministically, but does not provide information on the frequency of source terms or containment failure modes. It is important for the review team to ask the PSA team to identify the objectives of the Level 2 PSA. The review of a Level 2 PSA that is intended only to show that a nuclear power plant fulfills quantitative safety goals will be different than the review of a Level 2 PSA in which the objective is to produce information about the relative importance of systems and phenomena for accident management decisions or other purposes. Conservative assumptions that may be appropriate for the comparison to quantitative goals may be inadequate for making realistic accident management decisions. The review team should develop criteria for acceptability on the basis of the PSA objectives.

7.2. REVIEW OF THE LEVEL 1, LEVEL 2 INTERFACE

7.2.1. Review of accident sequence grouping

To perform a Level 2 analysis, it is necessary that all of the accident sequence information that is critical to the analysis of containment failure and radionuclide transport is transferred from the Level 1 analysis to the Level 2 analysis. In the past, this has usually been treated by regrouping the accident sequences into plant damage states that hold all of the information necessary to perform the Level 2 analysis. The regrouping can involve combining sequences into plant damage states and/or separating sequences into two or more plant damage states. The plant damage states are defined through a cooperative effort between the Level 1 and Level 2 analysts. They have typically been specified by a list of descriptors that identify all of the characteristics important to the Level 2 analysis. An example list of characteristics important to containment failure and radionuclide transport that have been used to define plant damage state groups is presented below:

Accident progression prior to core damage:

- Initiating events (e.g., LOCA, transient)
- Failure of safety systems designed to cope with the initiating event (e.g., reactor protection system, emergency core cooling system (ECCS), containment systems)
- LOCA with or without pressure suppression (BWRs)
- Suppression pool subcooled or saturated when core damage occurs (BWRs)
- Availability of containment sprays
- Availability of containment heat removal
- Availability of AC power.

System status for accident phases after core damage:

- AC and DC power (e.g., available, not available, recoverable)
- ECCS (e.g., available, not available, recoverable).

Containment status:

- Isolated and effective
- Non isolated and ineffective
- Failed and ineffective.

Reactor pressure vessel (RPV) conditions at the time of core meltdown and vessel lower head failure:

- High, intermediate or low pressure.

Containment ESF status:

- Containment sprays (e.g., available, not available, recoverable)
- Fan coolers (e.g., operate at all times, early or late operation)
- Venting systems (e.g., containment vented or not vented)
- Pressure suppression devices such as suppression pool or ice condenser (e.g., effective or ineffective at all times, bypassed early or late, pool subcooled or saturated, ice remaining or all melted).

Reactor building, secondary containment status:

- Isolated and effective
- Non isolated and ineffective
- Failed and ineffective.

Regarding the transfer of information the reviewer should assure that the Level 2 analyst has received all of the information from the Level 1 analysis that is necessary to evaluate containment failure and radionuclide transport. If the Level 1 and Level 2 analyses were performed in parallel and the Level 2 analysts presented their list of needs to the Level 1 analyst during the study, the information transfer may be performed automatically by computer. In this case, the reviewer needs to verify that the appropriate information was requested, and that the mechanism of the transfer was sound.

If the Level 2 analysis was performed at a later date than the Level 1 analysis or if the Level 2 analyst could not communicate the Level 2 needs to the Level 1 analyst, the review is more difficult, but probably also more important. The Level 2 analyst will probably have been forced to reconstitute the accident sequences by hand to obtain the necessary information. It is necessary for the reviewer to ask the analyst for the documentation to review this operation carefully.

A very important aspect of the Level 1, Level 2 interface is to account for any dependencies among operator actions that are combined together in the same sequence or cut set. Operator action dependencies can result if the same procedures are used, same indicators or annunciators are used, or the same operator must perform both actions in a limited time. This is a critical aspect of the PSA and should be carefully reviewed. There are usually some subtle correlations in the definition and application of the characteristics identified above which need careful examination. For example, there may be a dependency between recovery of electric power and recoverability of failed engineered safety features (ESF). Some plants have special emergency procedures for post-core damage situations. Operator actions under these circumstances depend on operator performance prior to core damage.

7.2.2. Consideration of feedback from containment events to core damage frequency calculation

Consideration of the feedback of containment events to core damage accident sequences is usually done as a part of the Level 1 analysis. It is however appropriate to review these feedback mechanisms from a Level 2 perspective.

The following list gives some typical examples of containment events that may lead to core damage:

(a) During loss of heat removal for BWRs and ATWS (anticipated transients without scram) sequences, overpressurization of the containment may lead to containment failure before the onset of core damage. Cavitation of pumps due to the depressurization of the containment, shearing off of injection pipes, or steam flooding of injection systems in the reactor building may then cause loss of coolant makeup and consequential core damage.

(b) Injection failure due to high containment pressure leading to closing of air operated valves inside containment.

(c) Injection failure due to steam flooding in the reactor building following failure of ductwork during venting.

The reviewer should verify that all interactions of this type have been considered appropriately. The analysts should have performed the following steps in doing this evaluation:

(i) identify all systems used for core damage mitigation;

(ii) identify all systems used for containment heat removal, radionuclide scrubbing, etc.;

(iii) evaluate the impact of phenomena within the containment on the systems;

(iv) determine which interactions warrant inclusion in the final accident sequence evaluation given the overall goal of the analysis.

7.2.3. Review of Level 1 events used in Level 2 models

The Level 2 models will most likely require the use of system unavailabilities, system non-recovery probabilities, and quantification of operator actions during the accident progression. Typical examples of events quantified in the Level 1 analysis that are used in Level 2 analysis are listed below:

(a) Containment spray unavailability
(b) AC power recovery probability
(c) Operator action (probability of the operator to fail to depressurize the primary system)
(d) Vacuum breaker failure probability.

The reviewer should assure that all events of this type have been addressed by the analysts. Some Level 2 events may be similar to Level 1 events, but may occur in different circumstances. It may be necessary to requantify these events. If these events were quantified in the Level 1 portion of the analysis, they will have been reviewed by the Level 1 reviewer. If however, these events were quantified in the Level 2 analysis, they should be reviewed by someone with the appropriate Level 1 expertise.

7.2.4. Selection of plant damage states to analyze deterministically

Some Level 2 analyses have relied entirely on previous deterministic analysis. However, most Level 2 analyses perform plant specific deterministic analyses. The reviewer should check the rationale for selecting scenarios on which to perform deterministic analyses. Some appropriate criteria are listed below:

(a) Select scenarios that best exercise the entire range of phenomenological models required for the analysis of this plant in order to allow extrapolation of these results to other scenarios.

(b) Select the scenarios that are dominant to core damage frequency.

(c) Select scenarios that are expected to have high source terms.

7.2.5. Review of Level 1 issues included in an integrated uncertainty analysis (may not be relevant for many Level 2 PSAs)

If an integrated uncertainty analysis is performed as part of the Level 2 analysis, the selection of Level 1 issues and Level 2 issues for inclusion in the uncertainty analysis should be compared for consistency in level of detail and for consistency in passing the Level 1 data to the Level 2 analysis.

7.2.6. Documentation to be requested

The documentation required to review the Level 1, Level 2 interface is listed below:

(a) Cut sets (or equivalent) from Level 1 analysis
(b) Description of sequences
(c) Description of plant damage states
(d) Description of containment systems
(e) Documentation describing grouping of sequences into plant damage states (or equivalent document)
(f) Any quality assurance documents available for the Level 1, Level 2 interface.

7.3. REVIEW OF THE ACCIDENT PROGRESSION/SOURCE TERM CALCULATION

There are many different types of methods (both probabilistic and deterministic) which can be employed to model the progression of an accident from core melt to the release of a source term to the environment. At first, the reviewer should become familiar with the containment geometry and the containment systems. The following containment characteristics are important to the reviewer:

(a) Containment size (free volumes, water pool volumes)
(b) Containment geometry (compartmentalization, sumps and pools)
(c) Structural design of the containment (free standing steel, reinforced concrete, containment penetrations, masses and areas of structures)
(d) Containment type (large dry, subatmospheric, pressure suppression)
(e) Containment design criteria (pressure, temperature, external impacts)
(f) Containment operating conditions (pressure, temperature, openings)
(g) Design of the compartments below the RPV (cavity, pedestal; geometry, proximity of containment boundaries and penetrations, flooding potential, dedicated flooding measures)
(h) Basemat design (type of concrete, basemat thickness, penetrations)
(i) Hydrogen control (inerting, ignitors, recombiners, locations)
(j) Spray systems (capacity, setpoints, distribution) and other containment systems related to cooling, fission product removal or ventilation (e.g., pool heat removal, control of water chemistry, fan coolers)
(k) Pressure suppression devices (suppression pool, ice condenser)

(l) Filtered and non-filtered venting systems for containment pressure relief (venting location, venting procedure, automatic or manual actuation, passive burst disc, filter efficiency, release to environment)
(m) Most likely flow paths of gases and aerosols, originating from the reactor coolant system (RCS) or reactor cavity or pedestal, to the containment leak location
(n) Features of the reactor, auxiliary or secondary containment buildings surrounding the containment (geometry, volumes, structures, design conditions, sprays, ventilation, aerosol and gas flow paths).

The individual containment features may cause significant deviations from the results of other Level 2 PSA studies, and the reviewer should pay particular attention to features that could necessitate highly specific considerations. Furthermore, the RCS features (e.g., reactor type, actual thermal power, masses of core materials, RCS coolant type and volume, ECCS features, containment bypass potential) related to the containment phenomena have to be examined as well.

7.3.1. Review of probabilistic models

As in the other phases of the review, it is critical to consider the objective of the PSA. The acceptability of the probabilistic models and the assumptions inherent in the models are critically dependent on the objective. The architecture of a study in which uncertainty is considered can differ significantly from the architecture of a point estimate study. The following sections highlight some considerations that should be addressed no matter what probabilistic modelling approach was used.

7.3.1.1. Are the appropriate time regimes considered?

All accident scenarios can be broken up into discrete time regimes within which physical phenomena and events can occur. The method by which phenomenological and system behavior within and between time regimes is addressed depends on the plant design and is specific to each Level 2 analysis. A typical set of time regimes is given below:

(a) Prior to core damage
(b) After core damage but before vessel breach
(c) At or around vessel breach
(d) A few hours after vessel breach
(e) Many hours after vessel breach.

The time regimes listed above should only be used as a coarse guide to help the reviewer assure that the analyst has addressed the importance of the timing of events. The reviewer should be aware that the timing of the recovery of accident mitigation systems can significantly impact the source term signature.

7.3.1.2. Have all of the relevant phenomena been considered?

During the time regimes described above, it is possible for one or more phenomenological events to occur. It is also possible for the same event type to occur in different time regimes. The phenomenological events can be addressed in the discrete stages described above, or can be considered in some other manner. It is important that a comprehensive set of phenomena are considered with an appreciation for the time of their occurrence in relation to core damage and vessel breach. Typically, the following phenomena, events and parameters are evaluated:

Phenomena:

- In-vessel core melt progression (from intact core to meltdown)
- Natural convection of steam and non-condensible gases in the RCS (flows and heat distribution)

- Hydrogen combustion in the containment (mixing, deflagrations, detonations, deflagration-to-detonation transition)
- In-vessel fuel-coolant interactions (energetic and non-energetic FCIs)
- Release of fuel from the vessel (high or low pressure, vessel lift-off)
- Direct containment heating (DCH) due to high-pressure melt ejection (HPME)
- Ex-vessel fuel-coolant interactions (energetic and non-energetic FCIs)
- Melt attacks against containment boundaries and penetrations
- Core debris coolability and molten core-concrete interactions
- Containment pressurization due to steam and non-condensible gas generation and heatup (including heat losses to structures)
- Effects of activated ESFs (e.g., ECCS, sprays, fan coolers, venting)
- Effects of redistributed fission products (and decay heat generation).

Parameters:

- In-vessel hydrogen generation (core degradation, molten fuel-coolant interactions, reflooding of an intact but overheated core)
- Ex-vessel hydrogen generation from fuel-coolant and core-concrete interactions (also other combustible gases such as carbon monoxide)
- In- and ex-vessel steam and non-condensible gas (e.g., hydrogen, carbon dioxide, carbon monoxide) generation.

Events:

- Timing for start of core melting and slumping to the RPV lower head
- Timing, location, size and mode of a structural RCS failure (other than RPV lower head, e.g., the PWR surge line or steam generator tube)
- Timing, size and mode of the RPV lower head failure (melt-through)
- Timing, location, size and mode of containment leakage or failure (over-pressure, thermal or dynamical loadings, basemat penetration)
- Timing and location of containment venting.

The matrix given in the following Table I correlates as an example some typical phenomenological events occurring during the time regimes as defined in the previous section.

The reviewer must use his knowledge of the plant to assure that the analyst has considered an appropriate set of phenomena for each time regime. The reviewer must also assure that the initial conditions for each event in the model are presented clearly and follow a logically correct pathway.

7.3.1.3. Is the logic structure of the model correct?

In the past many Level 2 studies have used containment event trees (or accident progression event trees) to model the accident progression. The level of detail in past containment event trees has varied from extremely simple to extremely complicated. Extremely simple event trees have had branch points representing containment failure modes only. Intermediate sized event trees have had branch points that represent different time regimes and some intermediate events (such as debris cooling). Complicated event trees have had branch points that represent different time regimes, all major phenomena, system events, and operator actions. The accident progression can be represented correctly by the simple event tree method as well as by the complicated event tree. However, insights regarding the relative importance of individual phenomenological events and system events may be impossible to obtain using simplified models in which events are not modelled explicitly. Also, when simple trees are used, particular care must be used to determine the effect of various phenomena on the final result. The level of probabilistic representation and level of deterministic detail will depend on the objective of the study and the depth of deterministic information available.

TABLE I. TIMING AND CORRELATION OF TYPICAL PHENOMENOLOGICAL EVENTS

Accident progression event or phenomenon (examples)	Possible time regimes in the accident progression model				
	Prior to core damage	After core damage but before vessel breach	At or around vessel breach	Few hours after vessel breach	Many hours after vessel breach
In-vessel melt progression	X				
RPV water level below TAF [a]		X	X		
In-vessel fuel-coolant interactions		X	X		
High-press. melt ejection and DCH[b]			X		
Ex-vessel fuel-coolant interactions			X	X	
Core-concrete interactions			X	X	X
Basemat penetration			X	X	X
Radionuclide (fission prod.) transport		X	X	X	X
Natural circulation of RCS gases		X	X	X	X
Hydrog. combustion in containment		X	X	X	X
Containment over-pressure failure	X	X	X	X	X
Initiation of containment venting	X	X	X	X	X
Initiation of cont. sprays or coolers	X	X	X	X	X

[a]TAF: top of active fuel [b]DCH: direct containment heating

The results of the containment event trees may have been expressed in terms of source term bins (or accident progression bins). These bins have been defined by the characteristics important to the source term calculation and represent the initial conditions for the source term analysis. Source terms are calculated either probabilistically or deterministically from these bins.

The reviewer must go through the logic structure of the models and assure the following:

(a) that impossible pathways do not occur;
(b) that each event reasonably follows the previous event;
(c) that the level of detail is commensurate with the objective of the study;
(d) that the relationship between the timing of mitigating system recovery and phenomena is addressed appropriately;
(e) that the characteristics of the source term bins (or accident progression bins) are defined correctly.

7.3.1.4. Have the interfaces between analysis modules been handled correctly?

Analyses in the past have used separate modules in the Level 2 analysis. Many studies have separated the source term analysis from the accident progression analysis. Other analyses have used a different module for each time regime. At every interface, a grouping exercise is usually performed to assure that the appropriate information is passed across the interface as efficiently as possible (such as the regrouping of sequences into plant damage states to facilitate the transfer of information needed for the accident progression calculation).

At each interface between modules, it is critical for the reviewer to assure that the correct information is transferred across the interface during the grouping, binning or whatever process occurs at the interface. A description of the method for each interface should be made available. The reviewer should understand the method.

7.3.1.5. Have correlations between events in the model been handled correctly?

Many of the events throughout the Level 2 analysis are correlated, either probabilistically or physically. Selected examples of correlated events from past studies are presented below:

(a) The amount of Zirconium oxidized in vessel is correlated to the amount of Zirconium available for a direct containment heating event or for oxidation in core concrete interactions. If the Zirconium is oxidized early, a smaller amount is available as a source of chemical energy later on.
(b) Early hydrogen burns are correlated to later hydrogen burns in the same scenario (you cannot burn the hydrogen twice).
(c) The coolability of the debris is correlated to the hydrogen production (high fragmentation means higher probability of debris coolability and higher hydrogen production rates during fuel-coolant interactions).
(d) The probability of recovering AC-power in different time regimes is correlated.
(e) Operator errors in the containment event tree are correlated to the operator performance prior to core damage.

The reviewer should assure that the analyst has a method in place to track and quantify these probabilistic and physical correlations.

7.3.1.6. Documentation to be requested

For the review of the probabilistic models, the reviewer should request the following documentation:

(a) Plant containment information
(b) Description of logic models with associated assumptions
(c) List of references for physical assumptions determining or affecting the logic structure,
(d) Documentation of quality assurance activities.

7.3.2. Review of input to probabilistic models

The input to the probabilistic models usually comes from the following sources:

(a) Available code calculations
(b) Extrapolation from code calculations
(c) Extrapolation from experiments
(d) Hand calculations
(e) Expert judgement (possibly using all of the above sources)
(f) System analysis.

Much of the input will come from plant specific deterministic calculations performed for the PSA. The review of these calculations is described in the next section. The reviewer should assure that the input is consistent with the input from past studies and identify any differences. The reviewer should also identify the individual plant features that may require specific evaluation and input. Radical differences from previous studies should be documented clearly and explored further. Events not quantified in any previous study should be inspected with caution. The document should contain either a reference or a description of any standard codes that were used as a basis for input. The reviewer should explore any non-standard codes or hand calculations that were used further with an

emphasis on consistency of input. The input from the system analysis (system unavailabilities, non-recovery probabilities, operator actions), should be reviewed by a Level 1 reviewer.

7.3.2.1. Documentation to be requested

The review of probabilistic model input requires typically the following documentation:

(a) Input for probabilistic models
(b) Rationale for input
(c) References for standard codes used
(d) Documentation for non-standard codes
(e) Documentation for hand calculations
(f) Documentation of QA activities.

7.3.3. Review of deterministic calculations

The purpose of the deterministic calculation is to mechanistically evaluate core melt progression, containment response and source terms for several selected sequences. This information can be used directly to characterize plant performance or can be used to develop branch point probabilities to quantify the containment event tree. The review of the deterministic calculations needs to consider whether the objective of the study is to assess the magnitude of the source term, or to use insights from the deterministic calculations directly for the development of accident management or mitigative procedures. The reviewer is cautioned that if the intent is to use the deterministic calculations for the development of accident management procedures, that the analyst or regulator consider the impact of the procedures on a diverse set of accident scenarios to assure that the procedures do not exacerbate some scenarios while mitigating the target scenarios.

If the aim of the analysis is to assess the magnitude of the source term for probabilistic studies which include a comprehensive range of accident scenarios, simplified models such as those in the risk oriented codes (e.g., STCP [19], MAAP [9], MELCOR [8]) may be preferable. However, depending particularly on the containment design, there may be a specific set of phenomena which are critical when assessing the probability of containment failure but which are not adequately modelled in the integrated codes. Examples of such phenomena important for assessing the potential merits and concerns of proposed accident management strategies are the melt-structure-coolant interactions (e.g., fuel-coolant interactions, melt attacks against the RPV lower head and containment boundaries, core debris coolability) and containment hydrogen response (e.g., with ignitors, recombiners). If the objective of the study requires deeper understanding of severe accident phenomena, more extensive methods must be used in addition to, or instead of, the integrated risk oriented codes. The assessment methods should typically involve also the use of simplified models, but the completeness of the study (all important mechanisms considered) and implications of the results have to be confirmed by comparing the results to those of more sophisticated models and experimental data available. The reviewer should ensure that the applied methods comply with the objectives of the study.

After understanding the objectives of the PSA the reviewer should evaluate:

(a) input data used;
(b) validity and suitability of the models used;
(c) performance of the calculations;
(d) organization and presentation of the deterministic information.

7.3.3.1. Input data

A large amount of input data from different sources needs to be reviewed when performing a review of a deterministic Level 2 analysis. The input can be grouped as follows:

(a) *Plant specific input data and the nodalization used to represent the plant.* The reviewer should check the basic data (for example, the mass of the water inventory in the primary coolant system and the volumes of containment compartments) and assure that these data are used appropriately in the models representing the plant. The material property data (such as heat conductivity of the walls, concrete composition, etc.) should also be checked. Models (e.g., containment model) should be nodalized so that further subdivision will not change the results drastically. Tests for convergence may be helpful. The reviewer should assure that the containment is modelled such that the overall convective flow pattern is correct in order to get a reasonable distribution of gases and fission products. He should also verify that the heat sinks are modelled correctly.

(b) *Accident scenario specific input.* The reviewer should assure that the input describing a particular accident sequence is reasonable. Some example input to review is presented below:

(i) in-vessel progression (system related input):
- leak areas and location;
- operation of pumps (feed rate, pump characteristic);
- operation of valves (set points, flow rates);
- accumulator injection (this may be calculated or postulated according to the primary coolant system models used).

(ii) in-vessel progression (phenomena related input):
- melt temperature (range);
- Zirconium oxidation (blockage, candling);
- slumping behavior (coherent or gradual relocation);
- RPV break module (leak size, location).

(iii) ex-vessel progression (system related input):
- leak rate of the containment, wetwell;
- operability of systems for heat removal (spray, recirculation pump, wetwell cooling, etc.);
- venting.

(iv) ex-vessel progression (phenomena related input):
- melt quenching behavior (particle size assumption);
- transient heat distribution;
- debris coolability behavior;
- forced ignition of combustible gases and parameters to calculate ignition (flame speed);
- fission product release (if input);
- containment failure (pressure, leak size, pathway).

The reviewer should review both plant and scenario input and check the justification for the use of the data. Assumptions made in formulating the input should be checked. No matter what type of input is provided, the reviewer is advised to consider the following:

(a) Consistency between the input and the models used. Different models may require input that appears similar in nomenclature, but in actuality is used differently in the models.

(b) Consistency between the physics in models for one phenomenological area and the models in another phenomenological area should be checked (for example, sprays affect both the thermal hydraulic calculations and the fission product transport calculations).

7.3.3.2. Validation and suitability of the models used

Many computer codes are available with differing degrees of complexity and with differing degrees of experimental validation. The suitability of the models and the accuracy required for every step of the calculation depends on the objective of the analysis. The reviewer has to assure that the models are detailed enough for the particular purpose and that the experimental and theoretical verification is appropriate. The documentation of the computer codes including references should be extensive enough to assess the detail and verification. After the reviewer has assessed the general suitability of the codes (or code system) he should revisit areas where the verification of the models is poor, and assess the acceptability of the analyst's justification of the models in these areas (for example, parametric calculation, additional hand calculation, use of experimental data, conservative assumptions, etc.).

The following list gives an overview of the areas where experimental verification is poor and how one may assess this in the frame of a PSA.

PROBLEM	SOLUTION
Melting temperature (melting temperature of eutectic can be substantially lower than that of individual fuel rod constituents)	Use bounding sensitivity calculations.
Hydrogen production after core melt	Use bounding sensitivity calculations.
Core melt slumping behavior	Use bounding sensitivity calculations.
RPV failure mode	Address probabilistically.
Early phase of molten core concrete interactions	Parametric calculations may be performed for: a) layered/homogeneous melt, b) chemical reactions other than Zirconium oxidation to assess the range of fission product release and hydrogen release rate.
Coolability of the melt	Use bounding sensitivity calculations, address probabilistically.

Other uncertainties that are not associated with the models of risk oriented computer codes, like containment failure behavior, are to be reviewed in the framework of the logic accident progression analysis.

7.3.3.3. Performance of the calculations

The deterministic calculations can either be performed by using an integrated code or by using several different codes (with different degrees of accuracy). The reviewer should check the performance of the calculation by examining simple mass, energy (and/or power) balances for several time intervals. He should become acquainted with the important fission product flow paths and check this for plausibility using results from PSAs for comparable plants.

In the case of integrated codes the reviewer should check the intermediate results for nonphysical results (nonphysical range of temperature etc.). Data transfer between the different modules of the code can be assumed to be automatically correct (the verification of this is appropriate for the review of the code, not the Level 2 PSA review).

When the calculations require linking of different codes, data transfer between the codes and the interface of the codes is a major challenge for the reviewer. A major source of confusion that the reviewer should be aware of can be different interpretation of intermediate results by different coworkers of the PSA study. The reviewer should check consistency within the analysis team.

Every value calculated (e.g., relevant times, released masses, source terms) has a related uncertainty (error) which has several causes:

- uncertainty due to nodalization;
- uncertainty of the physical models applied for a given course of the accident (e.g., core melt slumping behavior, H_2 release);
- uncertainty in material properties (e.g., melting, solidification temperatures);
- uncertainty in the actual course of the accident (e.g., accident management measures for reflooding, dependent failures);
- uncertainty from phenomenology not modelled.

The reviewer has to ensure that the PSA reflects adequately these uncertainties. If this is done by parametric calculation, he has to check whether these investigations fit into the complete calculations and influence the result.

7.3.3.4. Organization and representation

A major part of the review is to assess the presentation of the PSA for two reasons: first a comprehensive presentation is the necessary base for the review and, second, the objectives of the PSA can only be achieved if the end user of the PSA has confidence that the results are correct. For the deterministic calculations, this implies the following:

- Input to the codes should be listed completely and compared with the basic (plant specific) data. A distinction between important and less important data should be provided.
- Linkage between the different computer codes or the logic within an integrated code should be presented.
- Major assumptions for the deterministic calculations should be listed preferably together with information of what kind of results these assumptions may affect.
- The course of the accident as calculated should be clearly presented (table, flow chart, etc.).
- A comprehensive graphical presentation of the most important results should be given.
- Mass, energy (or/and power) balance should be presented in a manner that the accident progress can be drawn from this information.
- Quantitative results should be shown together with their error range; the most important contribution to the error should be specified.

7.3.3.5. Structural response

Structural input to deterministic calculations warrants special consideration. Structural response of both the reactor coolant system and the containment to thermal and pressure loads should be reviewed. Reactor coolant system response can often be treated generically(using results from studies made for similar plants and sequences), but containment response must be considered in a plant specific fashion.

The reviewer has to check the following items:

- The reactor coolant system failure mode used should reflect the common best estimate assumption and/or should be justified.
- The containment failure mode used should be based on an adequate investigation of all major discontinuities in the containment as well as the containment shell itself. Typical discontinuities

are: large penetrations (personnel lock and material hatch with associated sealing boxes), intermediate penetrations (pipes), small penetration, change of material (concrete/steel).
- The analytical tools used (if any) should be sufficiently validated by experiments.
- Direct experimental results available (pressurization of test containments) should be sufficiently considered.
- Appropriate material properties should be used, including discussion of uncertainties.
- For each major discontinuity as well as for the containment as a whole, a well founded best estimate value as well as a comprehensive range for the failure pressure should be provided together with an indication whether this failure means small leak (no further pressure increase), medium leak (depressurization of the containment in which fission products are retained in adjacent buildings), large leak (with no fission produce retention in adjacent buildings), or global failure.

It is clear that even a thorough investigation of the containment failure behavior cannot narrow the large range of uncertainty with respect to failure pressure, failure location, and leak size. Containment response will be dealt with probabilistically, but the reviewer should check the deterministic basis for the failure pressure and leak size.

7.3.4. Review of quantification of probabilistic models

The reviewer must be convinced that logic models are quantified correctly and that the methods for transfer of information across interfaces and correlations previously reviewed are handled correctly. The reviewer should sit down with the analyst and follow several scenarios all the way through the quantification from plant damage state to source term quantification. The following points must be verified:

(a) Is the multiplication of the conditional probabilities done correctly?
(b) Is the information passed correctly across all interfaces? (Emphasize Level 1, Level 2 interface and containment event tree/source term interface).
(c) Are correlations between events considered correctly?
(d) Are initial and boundary conditions for each event quantitatively correct? Consider conditions passed from the in-vessel analysis to the containment analysis, from the containment analysis to structural response analysis, and from the in-vessel, containment, and structural response analyses to the source term analysis.
(e) Are physical quantities (mass, energy, etc.) conserved in the model?

7.3.5. Special considerations for the review of source term analysis

Source term is defined here to mean the quantity of fission products released from the plant as a function of time, supplemented by information on the release time, location and energy. The quantification of source terms in different PSAs may have different objectives; the presentation of the source term results should reflect this. Some examples of different objectives are presented below:

- To show that certain release limits are met
- To quantitatively compare different mitigative procedures
- To deliver the input for a (Level 3) consequence analysis.

7.3.5.1. Fission product release

The reviewer must consider release from the following areas:

(a) Release from fuel

The reviewer should check:

- that all release possibilities are considered, such as gap release, release during heat-up and melting of the fuel, vaporization releases, and molten core-concrete interaction (MCCI) releases;
- whether the binning of fission products is comprehensive and reasonable release fractions are applied;
- whether the calculated release is consistent with other calculations and experimental results.

(b) Behavior of fission products within reactor coolant system

The reviewer should verify that the analyst has considered deposition as well as resuspension in the RCS.

(c) Fission product deposition within the containment

The reviewer should check:

- The adequacy of the modelling of active systems (sprays and fans) and the relevant parameters (spray droplet size) as well as the corresponding fission product transport models.
- The adequacy of the modelling of natural decontamination from overlying pools and pressure suppression devices and the relevant parameters (decontamination factors) as well as the corresponding fission product transport models. Furthermore the correlation to the thermohydraulic flow rates has to be checked.
- Whether the correlation between aerosol behavior and fission product behavior is sufficiently conservative. Natural deposition processes within the containment: these processes are normally governed by aerosol-physical processes (gravitational settling, diffusiophoresis, thermophoresis, condensation on the walls and on aerosols, etc.). For high aerosol loading rates, sensitivity studies using the MAEROS code [20] have shown that gravitational settling dominates.

(d) Fission product resuspension within the containment

Although resuspension is not normally considered one of the major fission product pathways in the containment, the reviewer should check whether this issue is considered appropriately. In the late time frames (if the containment is open or bypassed) this could be of importance.

In addition to reviewing the specific items described above, the reviewer should perform simple mass balances for either representative radionuclide groups or for all of the radionuclide groups to assure that mass is conserved during these scenarios. Some fission products are chemically active and can be found in different chemical states within the containment atmosphere and water sumps, e.g., iodine. The chemical reaction that may take place highly influences its airborne part and chemical state and thus the source term. The reviewer should assure that this problem is handled adequately according to the objective of the analysis (conservative assumption or special iodine calculation).

7.3.5.2. Analyzed sequences or bins

Depending on the objective of the study, one may end up with a small number of deterministically calculated source terms for selected sequences or with source terms that might be calculated for every CET (containment event tree) branch. The source terms of each CET branch (end point), or release category (a so-called release bin including several CET branches), can also be estimated using simplified methods, such as the XSOR [21] models of the NUREG-1150 study. The parameters (such as core release fractions, water pool decontamination factors) of simplified models may then be treated as probability distributions to reflect the uncertainties involved. In this case, the

reviewer should confirm that the parametric selections produce results that are consistent with the deterministic calculations and with current understanding of source term uncertainties.

For source term categorization, the review could typically be based on consideration of the following binning attributes:

Release timing relative to reactor shutdown (characterizing decay of short-lived radionuclides) and core damage (first major releases to containment atmosphere):

- Very early (containment failed or bypassed prior to core damage because of structural failure, isolation failure, major leakage, interfacing system LOCA or steam generator leakages)
- Early (e.g., a few hours after shutdown or shortly after core damage)
- Intermediate (e.g., some hours after core damage or vessel breach)
- Late (e.g., many hours after core damage and vessel breach).

Fission product flow paths and active removal mechanisms:

- Containment ESFs (e.g., sprays, fan coolers, filtered venting)
- Flow through containment water pools (suppression pools, water overlying ex-vessel core debris) or ice beds (ice condenser)
- Flow through RCS water pools (e.g., in the steam generator secondary side)
- Flow through tortuous pathways (e.g., long pipes with bends)
- Flow through the secondary containment (or reactor or auxiliary building).

Containment release (leakage or failure) mode:

- Leakage below the design basis accident (DBA) level
- Beyond DBA leakage
- Containment rupture
- Basemat penetration.

Characteristics of release to environment:

- Location of release (ground level, elevated)
- Energy of release (low, high and energetic)
- Duration of release (rapid, protracted).

In reviewing the attributes of the release categories, attention should be paid to the requirements of the Level 3 PSA. The source term information for Level 3 should contain:

- Radionuclides (fission product groups)
- Frequency (distributions) of release categories
- Release amounts (distributions) and durations
- Time of release relative to shutdown
- Warning time for countermeasures (from accident initiation to release)
- Location and energy of release
- Particle size distribution.

Most importantly, the reviewer should assure that the selected binning attributes lead to source term categories, in which the releases cause equivalent off-site consequences.

7.4. REVIEW OF THE INTERPRETATION OF RESULTS

In addition to checking intermediate results, the reviewer should ensure that the global results of the PSA are plausible, that the conclusions drawn from these results are correct and that the overall objectives of the PSA are met.

7.4.1. Plausibility of the results

The most effective means of checking the plausibility of global results are:

- comparison with results of other relevant PSAs;
- assurance that experimental results are not in contradiction to the results of the PSA;
- assessment of why previous major expert opinions deviate from the assumptions made in the PSA;
- performance of simple mass balance or hand calculations whenever appropriate.

While doing this plausibility review, supporting interviews with the members of the PSA group may be helpful. The list below should make intuitive sense to the reviewer.

- timing of events;
- relative importance of phenomena;
- conditional failure probability (reactor coolant system, containment);
- source term results (amount, timing, energy versus frequency).

7.4.2. Adequacy of the results with respect to the objectives

If the objective is to establish the size and frequency of the source term, the reviewer should check:

- That the source terms calculated are representative for the particular plant.
- That they address known uncertainties in a manner that is consistent with the objective of the PSA. For example, conservative source term estimates may be appropriate for demonstrating regulatory compliance, but a realistic ("best-estimate") evaluation may be appropriate for other objectives.

If conclusions are drawn from the source terms calculated, e.g., that a certain goal is met, the reviewer may have to check whether this is derived logically and that assumptions are consistent with this objective. For example, major uncertainties have to be addressed in a way that supports the confidence expressed in conclusions.

If the objective is the detailed understanding of the accident progression the reviewer has to check:

- that all important phenomena are considered;
- that this is done in a comprehensive manner (probabilistic quantification, selection for deterministic calculation);
- that best estimate, state-of-the-art methods are used.

It also has to be examined whether the conclusions drawn from these results have been derived in a logical way.

8. CONDUCTING THE LEVEL 3 REVIEW

8.1. INTRODUCTION

8.1.1. Background

The Level 3 step of a probabilistic safety assessment is commonly understood to refer to the modelling of the consequences of an accident involving release of radioactive material. This section is concerned principally with the off-site consequences evaluated from Level 3 PSA as applied to nuclear power plants and accidents whose primary release pathway is to the atmosphere. However, the general principles involved can be applied to accidents at other types of nuclear facilities where the major release pathway is initially airborne.

The review of a Level 3 analysis involves technical disciplines and expertise quite different from the ones required for the Level 1 and Level 2 analysis. With the exception of the Level 2, Level 3 interface, which should be reviewed from both sides, it follows therefore, that the Level 3 review can be mostly carried out independently.

8.1.2. Scope of the review

A Level 3 analysis takes as an input the results of the Level 1 and Level 2 analysis and produces as an output, estimates of accident consequences and risk. The Level 3 analysis involves characterizing the radiological consequences of the releases to the environment by estimating the dispersion of the releases in the vicinity of the facility under study and calculating the potential effects on the affected environment and population. These effects can be both health-related and/or economic. In order to mitigate these consequences a range of countermeasures, consistent with national policy may be considered in the PSA. The extent of countermeasure considerations would then be within the scope of the review. Presentation, discussion and application of PSA results, together with uncertainty and sensitivity analysis, are also considered to be part of the Level 3 analysis for review purposes.

The results of the Level 2 analysis are usually generated in the form of a set of accident categories, each of which is defined in terms of accident category frequency and a set of release characteristics (timing, magnitude, duration, composition). Some preliminary offsite consequence analysis may have been done in order to optimize the categorization prior to the completion of the Level 2 stage. A review of this aspect of the Level 2 work may be needed in order to ensure that the categories have been properly defined and that the release characteristics assigned to each category are representative of the events contributing to the category, from the viewpoint of the Level 3 analysis.

Level 1 and 2 analysis is undertaken by a variety of techniques, and computer programmes form an important tool in the overall analytical approach. However, when carrying out a Level 3 PSA, a computer programme specifically designed for consequence assessments becomes the primary approach. Provided it can be established that the program contains models and data bases valid for the site under study, the review may be limited to assessing the adequacy of program input data and interpretation of results.

A further consideration in establishing the scope of the review is the extent to which early health effects are anticipated. The consequences of accidental releases, for which the primary concern is stochastic health effects in a widely-distributed population, are far less sensitive to models and assumptions than the threshold behavior associated with non-stochastic effects.

Economic consequences can be included in Level 3 PSA's. Should the economic consequences of accidents be considered then the overall cost of the accident is dependent on whether countermeasures are implemented or not, and the type of countermeasures implemented (i.e. early and/or late). The review team will expect to see in the documentation a description of the

countermeasures proposed, a discussion of the criteria for countermeasure implementation, and a discussion of costs and of expected effects.

8.2. GENERAL OBJECTIVES OF THE REVIEW

The major objective of the review will be to establish the extent to which the models, assumptions and data used in the analysis are appropriate for the plant and site, and that the results and the significance claimed for them can be supported, within the limitations of current models. The focus of the review will depend to some extent on the intended applications of the results such as:

(a) to calculate public health consequences and risks arising from the potential for accidental releases of radioactivity for comparison against risk-based safety goals or targets;

(b) to calculate economic consequences and risks as a contributor the external influences of nuclear power generation;

(c) to evaluate the potential benefits of various countermeasures for emergency response planning;

(d) to evaluate importance measures for accident sequence ranking;

(e) to confirm that a balanced design of the plant has been achieved, so that no particular class of accident or feature of the plant makes a disproportionate contribution to the overall risk;

(f) to permit value-impact analysis to be used as an aid to safety-related decision making.

In the final analysis, the objective of the review is to increase the user's confidence in decisions that can be made using the results of the Level 3 PSA.

8.3. THE REVIEW PROCESS

8.3.1. Main steps in the review process

It is anticipated that the review would be completed in a number of discrete steps as follows:

(a) Preliminary review or pre-review. During this phase the review team should become familiar with:

- the terms of reference and objectives of the Level 3 PSA analysis;
- the Level 3 PSA documentation;
- the uses to which the results will be put;
- the computer program used in the analysis;
- the general characteristics of the site and surrounding area;
- the national policies on risk and emergency planning;
- the way uncertainty and sensitivity is dealt within the analysis.

(b) Identification and resolution of any issues raised in the pre-review.

(c) Performance of the detailed review.

(d) Documentation and issue resolution.

8.3.2. Qualifications of review team members

Members of the review team should be individuals with direct experience in the Level 3 aspects of PSA. At least one member should have participated in a Level 3 analysis in a lead role and one

should have experience in managing and reviewing such an analysis, with emphasis on the presentation and interpretation of the results. The background of the review team should be adequate to cover the basic disciplines involved in a Level 3 PSA. These areas of knowledge are:

- Radiation dose models
- Health effects of radiation
- Atmospheric dispersion modelling
- Food chain modelling
- Countermeasures following releases of radioactivity.

Preferably the review team should be experienced with the same probabilistic consequence code that was used in the analysis.

8.4. COMPUTER PROGRAM REQUIREMENTS

In order to perform the type of analysis usually associated with Level 3 PSA, the computer program used must possess the capability to perform the following series of computations:

(a) modelling of radionuclide release and initial plume behavior;
(b) modelling of the dispersion of the plume as it travels downwind, including deposition;
(c) systematic sampling of local meteorological conditions for near range effects and, if applicable, of regional synoptic conditions for long range effects;
(d) representation of major exposure pathways and associated dosimetric models;
(e) representation of the effects of countermeasures;
(f) calculation of health effects;
(g) calculation of economic effects (optional).

A number of databases are needed to support these models:

(a) meteorological data representative of the site or region where the plant under study is located;
(b) population distribution and characteristics;
(c) topographical features in the region of interest;
(d) a library of radionuclide data;
(e) environmental transfer and dosimetric data;
(f) economic data based on land use.

The computer program used should have been subjected to a formal quality assurance program and preferably have been tested in some form of international benchmark exercise. Examples of computer programs which are generally considered to meet the above requirements are:

ARANO, Finland [22]
CONDOR, UK [23]
COSYMA, CEC [24]
LENA, Sweden [25]
MACCS, USA [26]
OSCAAR, Japan [27].

The above list of computer programs is not intended to be exhaustive since these programs may not deal with some specific pathway or consequence which is desired for the Level 3 PSA. The user should demonstrate that the databases used by the program e.g., radionuclide data, health effects etc. are those currently recommended. Other codes may be used but the user should demonstrate consistency with other programs e.g., via benchmarking with one of the codes from the OECD/NEA code comparison exercise [28]. Any customization performed on a code previously subjected to a formal quality assurance and benchmarking exercise should in itself again be subjected to an adequate quality assurance process.

8.5. CONDUCTING THE LEVEL 3 REVIEW

8.5.1. Preliminary review

Prior to conducting the detailed review, the reviewer should become generally familiar with:

- the results of the Level 2 analysis;
- the results from the Level 2 peer review;
- the computer program used in the Level 3 analysis;
- the site characteristics and any specific features which are likely to influence the results;
- any available documentation of the Level 3 analysis.

8.5.2. Modelling review

Given that the computer program meets the general requirements set out in Section 8.4 above, it would not normally be the practice to review the models within the program. Instead the review is focussed on the assumptions used to generate the input data, the applicability of the models and data to the situation being represented, and the interpretation and application of results.

The following subsections discuss each of the major steps in the analysis. The approach taken is to briefly outline the issues involved, discuss the important assumptions associated with the step and important considerations that may enter into the review.

8.5.2.1. Characterization of the initial radionuclide releases

A set of data specifying the release characteristics of every representative accident to be included in the Level 3 analysis should be generated as part of the Level 2 process. Each set should comprise: the magnitude of the release for each major radionuclide group and its time-dependence relative to reactor shutdown, the release height, release energy, release pathway and the predicted probability of occurrence of the release. In addition, the time available for the initiation of countermeasures should be specified because there may be some delay between the occurrence of the accident and the recognition that countermeasures may become necessary. In practice, the categorization of in-plant sequences and selection of representative accidents may have been guided by some preliminary consequence analysis. This work should be reviewed to assess consistency with the important assumptions in the Level 3 analysis.

All computer codes have limitations in the detail with which a prolonged release can be represented. The approach taken is to replace the continuous release by a series of plumes. The way in which this is done has been found to contribute to variation in dose predictions. The review should ensure that the periods where release rates are highest are specifically modelled in the plume representation, that the early phase plume release is modelled in more detail than the later phases and that the modelling of the phases is correlated with the countermeasures taken.

Another characteristic of the release important to consequence assessment, but rarely specified as part of the Level 2 information set, is the chemical form and size distribution of aerosol particles. Even if such information was provided, the Level 3 computer programs have limited capability to model the effects on environmental transport. The assumption of an average particle diameter of 1 micrometer is a common practice. However, release pathways may exist which can alter the average particle size, such as through post-accident filters. Overestimation of particle size tends to increase near-field dose at the expense of far-field dose, which may or may not be conservative depending on the population distribution.

In summary, the important issues to be resolved in assessing the characterization of the releases are:

- from a consequence assessment point of view, whether the representative accidents adequately reflect the overall characteristics of the accident categories they are intended to represent;
- whether the approximation of prolonged releases as a series of plumes adequately reflects the maximum release rates expected during the release;
- whether the assumed aerosol particle size differs from the code default value and, if so, whether there is a legitimate basis for the new assumption(s) and, if not, whether there is a basis for doing so for some accidents.

8.5.2.2. Atmospheric dispersion

Gaussian-based modelling is recognized to possess some limitations. In practice, this limitation is more important for real-time emergency response than for PSA and more sophisticated models have been developed for this application. It turns out that the repetitive process used in PSA Level 3 programs to develop statistical results also tends to average out local variations, particularly where stochastic health effects are of more interest. Only if key results of the PSA relate to some specific phenomenon not well treated by the Gaussian model there is cause for concern.

The atmospheric dispersion simulation first determines the initial characteristics of the release puff or plume by allowing for the effects of release energy and momentum on plume rise, taking account of any wind-field perturbation due to building structures. For a given set of meteorological conditions selected from a suitable data set, the plume is allowed to move downwind, dispersing in the crosswind and vertical directions, subject to certain limitations from the ground and atmospheric layering. The output of the dispersion calculation is time-integrated airborne concentrations and surface concentrations as a result of deposition in the region of interest.

Most programs use dispersion models based on a Gaussian distribution assumption. Some allow for changes in wind direction during the passage of the plume (so-called "trajectory" models) and some do not ("straight-line" models). Straight-line and trajectory models are generally felt to be equally valid out to a few tens of kilometers, possibly as far as 100 km on a level terrain, but beyond this trajectory models using a wind-field are more appropriate. Dispersion models used in areas of complex terrain should be applicable to that specific terrain.

The most important example arises in assessing the potential for early health effects. The existence of a threshold in the dose response curve and the relatively high doses required to cause early effects, makes the prediction of numbers of such effects highly sensitive to assumptions that can influence calculated airborne concentrations close to the site. Careful review of the modelling assumptions which govern initial plume characteristics is important if early effects are anticipated.

The normal approach is to ensure that input parameters are on the conservative side where limited information on the distribution exists. For example, a direction-invariant value for building cross-section should generally correspond to that of the smallest cross-section of the structure. If the nearest population center is at an elevated location with respect to the plant it may be necessary to artificially lower the initial height of release to accommodate the difference. In most cases, sensitivity of results to these assumptions disappears after a few kilometers.

A key determinant of accident consequence is the calculation of dry and wet surface deposition. These processes are automatically addressed in the referenced computer programs but the degree to which the user can influence the outcome by changing default data varies. High elevation areas closer to the plume centerline would be expected to experience higher deposition rates but this may not be reflected in the computer model. Complex terrain may exhibit air flow patterns which bypass elevated regions. An assessment of the implications of such modelling limitations on the results may be needed.

In summary, the principal questions to be resolved on the subject of dispersion modelling are:

- whether the dispersion model (or models) used are valid over the range covered by the analysis;
- whether there are specific topographical features or other considerations that may influence the results of the analysis and how they have been accounted for;
- for those releases with the potential for early health effects, whether the characterization of initial plume behavior is sufficiently conservative with respect to the uncertainties involved;
- whether the deposition data used in the analysis are appropriate for the type of terrain.

8.5.2.3. Meteorological sampling

Normally, the dependence of consequence analysis results on meteorological conditions is treated in a statistical manner by systematic sampling from a suitable meteorological data base (see Subsection 8.5.3.1). The purpose of choosing a sampling strategy is to obtain a set of representative weather conditions, computationally efficient but ensuring extreme conditions are properly taken into account. Most programs offer default stratified sampling routines.

A review of the sampling strategy should be carried out sufficient to establish whether it contains any bias, for example, due to insufficient sample runs. The basis for any customizing of the sampling scheme should be addressed, together with an assessment of likely implications to results.

8.5.2.4. Calculation of dose

The process of dose calculation for each sampled case is usually automatic, using well-established models and data bases. Separate dose contributions may be calculated from external sources (cloud and deposited material), inhalation (cloud and resuspension) and ingestion, with and without relevant countermeasures. There are, however, a number of user-supplied parameters which are direct multipliers in the dose calculation and which can have a very significant influence on predicted health effects.

In most cases, doses are calculated for average individuals of the population, i.e. adults. Depending on the objectives of the PSA, however, it might be necessary to calculate individual doses for certain subgroups of the population, for instance one year old children. In such cases the reviewer should confirm that the right set of parameter values have been used for these calculations, like age-dependent data for groundshine and cloudshine doses, metabolic data consumption rates and dose conversion factors. In PSAs where on the one hand individual doses are assessed for such subgroups and on the other hand collective doses are calculated for the whole population, it is necessary to certify that the appropriate set of parameter values have been used in these calculations.

External dose

The user can influence these results mainly through the specification of shielding factors to account for protection from building structures. An estimate of the relative fraction of indoor/outdoor activity can be specified representative of average behavior of the population or may be specified on an area basis in some programs.

In high population areas (i.e. urban), people spend a much higher fraction of their time indoors than in rural areas. Calculated building shielding factors can vary by an order of magnitude or more. Other shielding factors are applied to groundshine, because of the different shielding geometry, and allowance for removal of surface radioactivity by weathering can be made.

Specification of shielding factors should be reviewed for the following issues:

- whether the shielding factors used are appropriate for the type of structures that exist in the potentially most exposed areas;
- whether the possibility of activity being deposited indoors has been adequately considered;

- whether the relative fraction of indoor/outdoor activity is typical of that expected from the population, particularly in the potentially most exposed areas;
- whether the groundshine shielding factor(s) has been derived on a basis consistent with that of the cloud shielding factors;
- whether the effect of weathering is a default value or based on local terrain conditions.

Inhalation

Many models allow the specification of a filtering factor to reduce the relative concentration of airborne activity between the inside and outside of buildings. This parameter should be reviewed to ensure it is adequately representative of local structures.

Ingestion

Ingestion of contaminated foodstuffs represents the major potential dose pathway for long-term dose accumulation in the general population, especially after countermeasures have been taken. Many of the parameters involved in calculating this dose component are contained in standard databases invisible to the user but the computer programs usually require the user to specify agricultural production and consumption behavior.

The ingestion models have typically been developed assuming food production and consumption patterns typical of the region from which the program originates. Application of these models to a different environment may require adjustment to the databases such as land use etc. The review should also consider if and how seasonal variation has been addressed.

The issue of contamination of water bodies may be of significance, especially where drinking water supplies could be affected. The degree of sophistication with which the various computer programs deal with aquatic pathways varies. This may be a factor in selecting an appropriate program to use for a PSA study. Fresh water pathways should be taken into account especially where fish from these sources is a major part of the diet of the population.

In summary, the review needs to consider the extent to which the data related to dose assessment is reflective of the characteristics of the site and the surrounding region, taking into account the limitations of the models and the importance of each pathway to the total dose estimates. Any model of such complex and variable phenomena is bound to contain major simplifications but this need not invalidate the overall results and conclusions of the PSA.

8.5.2.5. Countermeasures

Depending on the objectives of the PSA, the reduction of the potential risks by the implementation of countermeasures may be an important endpoint of the calculations.

Most programs allow a number of countermeasures to be credited. These can be effective either in the short-term (sheltering, stable iodine prophylaxis, evacuation) and intended primarily to reduce the likelihood of early effects, or in the long-term (relocation, food bans and decontamination) to reduce total population dose. In all cases, the reviewer should check that the modelling of the countermeasure implementation in the Level 3 analysis is in compliance with the specifications of the PSA and according to the national and local policy on countermeasure strategies.

Short-term countermeasures

The focus of the review should be on the role of short-term countermeasures in minimizing early health effects. Most computer programs require an estimate of the time at which the various countermeasures are implemented. These values may be compared against local emergency plans to confirm their feasibility.

The effectiveness of sheltering and, to a lesser extent iodine prophylaxis, may be limited if a large fraction of the population is already credited as being indoors. Assumptions regarding population location and shielding effectiveness, reasonable when applied for the entire population, may not be so for the subset of population at risk from early effects.

Some computer programs establish the extent of countermeasures by calculating a "potential" dose without countermeasures, taking into account shielding effects and then applying countermeasure dose criteria. The review should consider the degree to which this approach reflects local emergency response procedures. Evacuation and/or decontamination assumptions should be closely related to local emergency response capabilities. Reviewers should bear in mind that there is a tendency for optimism in emergency plans, particularly in areas which cannot be tested, such as large-scale evacuation.

Long-term countermeasures

Long-term countermeasures are of importance to the extent that they are able to produce significant dose reductions to large numbers of people. The prediction of latent health effects is usually dominated by the integration of small dose increments over a large number of people, most of whom would be unaffected by the implementation of countermeasures involving decontamination and/or relocation.

As a general rule, implementation of countermeasures is not something that can be mandated by the PSA analyst. The review needs to ensure that the assumptions credited in the analysis are consistent with local emergency planning procedures as they are likely to be applied in the event of an emergency, i.e., that they are reasonable and practical.

An effort should be made by the reviewer to gauge the importance of the various countermeasures to the overall results, if the PSA analysts have not already done so. This will enable the review to focus on the key issues. However, care must be taken to ensure that the apparent lack of significance of a particular countermeasure is not due to an unreasonable assumption in the first place.

8.5.2.6. Calculation of health effects

Most of the available Level 3 computer codes include models for deterministic and stochastic health effects, based on dose-effect relationships. It is common practice to evaluate deterministic effects by means of a hazard function. The dose rate dependency of the effects has been implemented in these models either by specifying certain periods of time and corresponding LD_{50} (the dose at which 50% of a representative group is expected to suffer lethal effects) values and threshold doses, or by expressing LD_{50} as a function of dose rate. The reviewer should check that the appropriate parameter values for the different deterministic effects have been used.

Generally, the risk of stochastic effects is calculated by a linear-quadratic dose response function, without a threshold. In current consequence analysis codes this linear-quadratic function has been reduced to a linear function. The application of such a linear dose-effect relationship is in accordance to recent ICRP recommendations [29], but may lead to overestimation of the stochastic effects at low doses and dose rates. To correct this overestimation some codes modify the linear dose response function by a dose and dose rate effectiveness factor (DDREF). The reviewer should check if an adequate use of the capability of the models has been made.

Risk factors are age dependent. In cases that have been pointed out in Section 8.5.2.4, the reviewer should also check the use of the right risk factors for consistency with the age group for which the risks of stochastic effects are to be evaluated.

8.5.2.7. Calculation of economic consequences

Economic consequences include the cost of health effects and the countermeasures imposed. In many cases the countermeasures make the main contribution. In general, the health effect cost will vary inversely to the cost of countermeasures related to health consequences. A more complete estimate of the total cost might include some of the indirect and social costs that could reasonably be associated with reactor accidents.

Data for the economic calculations are provided partly by the user, who must specify the economic activity and land values on an area basis, and partly by data previously supplied for health effects calculations. Inevitably, considerable averaging must occur to represent a diverse region on a polar grid. It is more important that the absolute economic values are estimated realistically and based on data from the region being studied.

Data on the costs of implementation of countermeasures (evacuation, relocation, decontamination, food bans, etc.) related to the various land use areas are also required. These data can be difficult to obtain and often involve judgements on the part of the analyst collecting the data. The review should focus on the possibility of over-optimism in generating this information through an approach which is too simplistic.

Typical issues that need to be reviewed are:

- whether the costs of countermeasures have been estimated realistically and consistent with local costs of goods and services;
- whether the value of land near urban areas is related to agricultural use or housing/industrial use;
- whether the impact of contamination of the water supply has been considered;
- whether the cost of decontamination reflects the full implications of this activity (i.e., dose accumulation and control, incentives, waste disposal, etc.).

8.5.3. Review of databases

8.5.3.1. Meteorological data

The overall objective in reviewing the meteorological data is to establish that the data used are representative of the vicinity of the plant location and, where applicable, include extreme meteorological conditions. The data need to reflect local conditions for near-field calculations and regional conditions for far-field results.

Typically, one year's data recorded on an hourly basis is required as a minimum, to ensure that seasonal variations are included. A true picture of the overall patterns probably requires several years of data to be summarized in order to properly characterize the potential for extreme conditions, but this is unlikely to be available for most PSAs.

If the location of the plant under study is close to a major topographical interface that can influence local meteorological conditions, such as a coastline, it is desirable that the data be obtained from a source within the zone of influence. Some methods of stability class determination may not be reliable in such zones. Similarly, wind direction can vary significantly from general synoptic conditions and local layering can occur at interfaces.

Very high concentrations can be predicted under low wind speed conditions if the accompanying wind meander is not included in the dispersion calculation. This and other related concerns can be addressed by deriving horizontal dispersion behavior and stability class from direct measurement of the standard deviation of wind direction about the mean value.

The occurrence of rain during the passage of a release has important implications on the results. Treatment of this phenomenon tends to follow standard procedures within the programs. In regions where rain is infrequent or exhibits large seasonal variations, a review of the procedure used by the program might be warranted to assess the suitability of the database.

In summary, some of the important issues to be included in the review of the meteorological data base are:

- whether there are sufficient data to represent the range of conditions experienced in the region;
- whether the source of data is adequately representative of local or regional conditions, depending on the application;
- whether the method of inferring atmospheric stability is reliable under local conditions;
- whether wind meander at low windspeed is incorporated into the data;
- whether an adequate description of precipitation behavior exists in the data.

8.5.3.2. Spatial data

The requirement to specify population, agricultural and economic data on a spatial grid system in polar coordinates is common to most computer programs for Level 3 analysis. High resolution is desirable close to the plant and in areas of dense population if early effects are to be estimated properly. A coarse grid close to the site may artificially include a large number of people in a high dose category, but may also move the points at which airborne concentrations are calculated to a radius beyond which early effects are anticipated.

Choice of the size of the region to be included in the Level 3 calculation should be guided by the location of sensitive areas such as productive farmland and population distribution. The process of generating the spatial data from sources that may be old, compiled in a non-compatible format or simply sparse requires a process of averaging using the judgement of the analyst. In most cases this is unlikely to be a major source of uncertainty.

Experience suggests that the location of the far boundary of the analysis region can have some bearing on dose calculations if wind direction reversal occurs and a trajectory model is being used. The presence of such anomalies can be hard to detect in a review of a study containing a large number of repeated calculations. A review of the spatial variation of intermediate results such as airborne or deposited concentrations should be carried out to search for any apparent anomalies.

8.5.3.3. Radiological data

The computer programs all contain libraries of data governing radionuclide properties, environmental transfer coefficients, dose conversion factors and health effect models. It is generally not necessary to review such data unless the analyst has made some changes to address an issue specific to the study.

8.6. RESULTS FOR ACCIDENT CONSEQUENCE AND RISK

8.6.1. Presentation of results

The Level 3 analysis should present the results that will be used in the final application. However, the review team will expect to see intermediate results which may vary with the type of analysis. This is an issue that can be discussed with the review team in the pre-review phase.

The results should be presented in a graphical form as a conditional and unconditional CCDF (complementary cumulative distribution function) or tabular form as expectation values and suitable percentiles.

Finally the contribution of the exposure pathways and the contribution of individual radionuclides to the effective dose should be provided together with the extent of application of the various countermeasures employed.

8.6.2. Application of results

The proposed application or use of the PSA results may have some bearing on the review process and its findings. The results of PSAs are used in two general ways.

The first way is to compare the PSA results to safety targets which have been derived from real data and experience. These targets are generally regarded as absolute values. Thus, this type of comparison is an absolute application.

The second way of using the PSA results is to compare the results of one PSA to another PSA. In this case it is the relative difference between the two sets of results that is important (i.e. is one practice or countermeasure more effective than another).

If the results are to be used primarily in comparison to absolute values and uncertainty exists in the input parameters, the values chosen should be as realistic as possible. In the case where realistic values are not available the values should tend towards conservatism.

Comparison of PSA results with absolute targets is usually performed using the expected value from the CCDF. Even if not explicitly required, some accounting for the role of uncertainty and its significance to the conclusions with regard to acceptability should be made.

If the results are to be used in relative sense, the PSA should tend towards best expert judgement in those areas of uncertainty not accounted for in the uncertainty analysis.

8.6.3. Sensitivity and uncertainty

A full treatment of uncertainties and sensitivities, that is one where the consequence analysis is repeated many times, sampling from a specified range for each input variable is desirable. However, this treatment is rarely carried out because of the high cost in both effort and resources. Yet it is important and necessary in any Level 3 PSA to have some sense for the way the results depend on variations in selected parameters.

For some currently available Level 3 PSA computer codes international sensitivity and uncertainty studies are underway [30]. However, the results of these studies are not yet available to analysts. Even when the results of these studies are available they may not be applicable to all PSA situations. It is therefore strongly suggested that some limited form of sensitivity and uncertainty analysis should be undertaken as a part of the Level 3 PSA. In this case the limitations of such an abbreviated study should be clearly identified.

Because of the importance of this issue the review team will expect to see this issue addressed. The details of how it is addressed and the limitations of the method used can be discussed in the pre-review phase.

8.7. DOCUMENTATION AND QUALITY ASSURANCE

8.7.1. Analysis documentation

A general structure for the documentation of a Level 3 PSA is provided in Reference [4]. The review of the documentation should be aimed at ensuring that sufficient information is included to

permit a knowledgeable but non-expert reader to identify the key issues affecting the results and to understand the significance of the results.

The Level 3 documentation should be reviewed against the following general characteristics:

- a clear definition of the objectives of the analysis and the expected application of the results;
- an outline of the methods and data used, with references to the sources of more detailed information;
- identification and justification of the major assumptions and simplifications that are thought to have influenced the results;
- a detailed description and justification of any changes to standard models and data;
- a clear presentation and explanation of the important intermediate and final results;
- a discussion of sensitivities and uncertainties (see Subsection 8.6.3);
- a discussion of any application of the results, conclusions drawn and the significance of those conclusions.

8.7.2. Quality assurance

An analysis of the complexity of PSA Level 3 should be supported by a documented quality assurance procedure aimed at providing reasonable assurance that there are no inadvertent errors in the analysis.

Typical features of a QA procedure should include:

- a documented project plan;
- an outline of the methods to be followed, computer programs to be used and sources of data;
- definition of roles and responsibilities of users;
- a process for independent review of major assumptions and non-standard modelling;
- a process for independent review and sign-off of data bases and computer program input;
- requirements and standards for project documentation;
- systems for periodic functional checks of the project outputs.

The function of the review team should be to confirm that the procedures are adequate for their purpose and have been followed.

8.8. THE REVIEW REPORT

The findings of the review should be documented as a formal report to the host organization. The report should be structured along the following lines:

- A summary of general findings and conclusions.
- An introduction containing general information such as a brief description of the plant type and location, and the organizations involved in the Level 3 analysis.
- A definition of the main objectives of the Level 3 PSA and the purpose it serves. Main uses of the Level 3 results should be stated, including comments on the suitability of the methods for the intended application.
- A review of the methodology followed in the Level 3 analysis, including computer codes used and principal sources of data.
- A description of the major issues raised, their resolution and any follow-up recommendations.
- A detailed discussion of findings and recommendations.
- Conclusions regarding the Level 3 component of the PSA, the review and the review process.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 1), Safety Series No. 50-P-4, Vienna (1992).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series, Vienna (in preparation).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Off-site Consequences and Estimation of Risks to the Public, Safety Practice, Vienna (in preparation).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessments for Nuclear Power Plants, Safety Series No. 50-P-7, Vienna (1995).

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA-TECDOC-648, Vienna (1993).

[8] SUMMERS, R.M., COLE, R.K., BOUCHERON, E.A., CARMEL, M.K., DINGMAN, S.E., KELLY, J.E., MELCOR 1.8.0: A Computer Code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analyses, Rep. NUREG/CR-5531, SAND90-0364, Sandia National Laboratories, Albuquerque, NM (1991).

[9] FAUSKE AND ASSOCIATES INC., MAAP Modular Accident Analysis Program User's Manual, Vols. I and II, IDCOR Technical Report 16.2-3 (1987).

[10] ELECTRIC POWER RESEARCH INSTITUTE, Anticipated Transients Without Scram: A Reappraisal: Frequency of Anticipated Transients, Rep. EPRI-NP-2230, Palo Alto, CA (1982).

[11] ONTARIO HYDRO, Darlington Probabilistic Safety Evaluations (Summary Report), 2 Vols. (plus 18 Vols. Appendices), Toronto (1987).

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

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

[14] HANNAMAN, G.W., SPURGIN, A.J., Systematic Human Action Reliability Procedure (SHARP), Rep. EPRI-NP-3583, Electric Power Research Institute, Palo Alto, CA (1984).

[15] SWAIN, A.D., GUTTMAN, H.E., Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Rep. NUREG/CR-1278, Sandia National Laboratories, Albuquerque, NM (1983).

[16] 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).

[17] EMBREY, D.E., SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement, Rep. NUREG/CR-3518, USNRC (1984).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-508, Vienna (1989).

[19] GIESEKE, J.A., Source term Code Package, A User's Guide (Mod 1), Rep. NUREG/CR-4587, BMI-2138, Battelle's Columbus Div., Columbus, OH (1985).

[20] GELBARD, F., MAEROS User Manual, Rep. NUREG/CR-1391, SAND80-0822, Sandia National Laboratories, Albuquerque, NM (1982).

[21] JOW, H.-N., MURFIN, W.B., JOHNSON, J.D., XSOR Codes Users Manual, Rep. NUREG/CR-5360, USNRC (1993).

[22] SAVOLAINEN, I., VUORI, S., ARANO - A Computer Program for the Assessment of Atmospheric Radioactive Releases, Rep. VTT-YDI-53, Technical Research Center of Finland, Nuclear Engineering Laboratory, Otaniemi (1980).
[23] AEA CONSULTANCY SERVICES (SRD), CONDOR 1: A Probabilistic Consequence Assessment Code Applicable to Releases of Radionuclides to the Atmosphere, Rep. SRD-R-598, NE-TD/ETB/REP-7021, NRPB-R-258, Risley (1993).
[24] COMMISSION OF THE EUROPEAN COMMUNITIES, COSYMA: A New Program Package for Accident Consequence Assessment, Rep. EUR-13028, CEC, Luxembourg (1991).
[25] BÄVERSTAM, U., KARLBERG, O., LENA P. A Probabilistic Version of the LENA Code Version 1.0", Rep. SSI-93-05, Swedish Radiation Protection Institute, Stockholm (1993).
[26] JOW, H.N., SPRUNG, J.L., ROLLSTIN, J.A., CHANIN, D.I., MELCOR Accident Consequence Code System (MACCS). Model Description, Rep. NUREG/CR-4691, Vol. 2, USNRC, Washington DC (1990).
[27] HOMMA, T., TOGAWA, O., IIJIMA, T., Development of Accident Consequence Assessment Code at JAERI, Methods and Codes for Assessing the Off-site Consequences of Nuclear Accidents (Proc. Seminar, Athens, 7-11 May 1990), Rep. EUR-13013/2-EN, CEC, Luxembourg (1991).
[28] OECD NUCLEAR ENERGY AGENCY and COMMISSION OF THE EUROPEAN COMMUNITIES, Probabilistic Accident Consequence Assessment Codes, Second International Comparison - Overview Report, Paris (1994).
[29] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Recommendations of the International Commission on Radiological Protection, Publication 60, Annals of the ICRP 21 (1-3), Pergamon Press, Oxford and New York (1991).
[30] NUCLEAR REGULATORY COMMISSION and COMMISSION OF THE EUROPEAN COMMUNITIES, Probabilistic Accident Consequence Uncertainty Analysis: Dispersion and Deposition Uncertainty Assessment, Rep. NUREG/CR-6244, EUR 15855EN, SAND94-1453 (1994).

Appendix I
RANGES FOR COMPONENT FAILURE DATA FROM PAST PSAs

The following table gives ranges of central values (values used for point estimates) for failure data of components that have been used in past PSAs. The failure rates are for normal environments and the values are rounded to the nearest half order of magnitude. The ranges are taken from the data given in Ref. [18]. The associated 90 % error factors about a given central value are generally of the order of 3.

TABLE I.1. RANGES OF COMPONENT FAILURE RATES TAKEN FROM PAST PSAs

Component/Failure mode	Range
Diesel driven pump, fails to start	3×10^{-4} - 3×10^{-2}/d
Diesel driven pump, fails to run	1×10^{-3} - 3×10^{-2}/h
Motor driven pump, fails to start	3×10^{-4} - 3×10^{-2}/d
Motor driven pump, fails to run	1×10^{-4} - 3×10^{-4}/h
Turbine driven pump, fails to start	3×10^{-3} - 3×10^{-2}/d
Turbine driven pump, fails to run	1×10^{-5} - 1×10^{-3}/h
Air operated valve, fails to change position	1×10^{-4} - 1×10^{-2}/d
Air operated valve, fails to open	3×10^{-4} - 1×10^{-2}/d
Air operated valve, fails to close	1×10^{-4} - 3×10^{-3}/d
Air operated valve, fails to remain in position	1×10^{-7} - 3×10^{-6}/h
Manual valve, fails to change position	1×10^{-5} - 3×10^{-4}/d
Manual valve, fails to remain in position	1×10^{-7} - 3×10^{-6}/h
Motor operated valve, fails to change position	3×10^{-4} - 3×10^{-2}/d
Motor operated valve, fails to remain in position	1×10^{-7} - 1×10^{-6}/h
Check valve, fails to open	3×10^{-6} - 3×10^{-4}/d
Check valve, fails to close	1×10^{-5} - 1×10^{-3}/d
Solenoid valve, fails to change position	1×10^{-4} - 1×10^{-2}/d
Relief valve, fails to open	1×10^{-4} - 1×10^{-2}/d
Relief valve, fails to close	3×10^{-3} - 3×10^{-2}/d
Safety valve, fails to open	1×10^{-4} - 1×10^{-2}/d
Safety valve, fails to close	1×10^{-3} - 3×10^{-2}/d
Diesel generator, fails to start	3×10^{-3} - 3×10^{-2}/d
Diesel generator, fails to run	1×10^{-3} - 1×10^{-2}/h
Battery, fails to function	1×10^{-7} - 3×10^{-6}/h
Battery charger, fails to function	1×10^{-6} - 1×10^{-5}/h

TABLE I.1. (cont.)

Component/Failure mode	Range
Bus, fails to function	3×10^{-8} - 1×10^{-6}/h
Inverter, fails to function	1×10^{-6} - 1×10^{-4}/h
Motor, fails to start	1×10^{-4} - 1×10^{-3}/d
Motor, fails to run	1×10^{-6} - 1×10^{-5}/h
Rectifier, fails to function	3×10^{-7} - 3×10^{-6}/h
Relay, fails to remain in position	3×10^{-8} - 1×10^{-6}/h
Transformer, fails to function	1×10^{-7} - 3×10^{-6}/h
Switch (flow, level, pressure, temperature, torque), fails to function	3×10^{-7} - 1×10^{-5}/h
Transmitter, fails to function	3×10^{-7} - 3×10^{-6}/h

Appendix II
EXAMPLE OF AN ISSUE LIST

The example has been taken from a past review. Names and details have been altered to prevent identification of the PSA study and the facility.

ISSUE LIST — ***Issue No.: JS-012*** [a]

Problème(s), questions — ***PSA Area No.: A21,A25b*** [b]

Statement of Issue or Background Info
Description du problème, explication du contexte

Assignment and screening of CCF groups

A spot check for CCF groups on the secondary side showed that very few CCFs for isolation valves in the steam lines (air and motor operated valves) appear in the model. Large isolation valves, especially on the steam side should at least be considered as CCF candidates.

List Questions arising out of this Issue
Notez les questions résultant du problème

Please give the reasoning or background information why practically no CCFs for these isolation valves appear in the final model.

---

[a] The unique issue identifier JS-012 is composed of the initials JS (John Smith) and a running number for the issues of each reviewer, 12 in this example.

[b] The PSA areas are identified with the PSA task numbers from Ref. [2].

The large isolation valves on the steam side have been considered to be susceptible to common cause failures. These valves include the air operated steam generator isolation valves, the motor operated steam generator isolation valves and the three air operated steam collector isolation valves.

The common cause group for the air operated isolation valves on the steam side is given under group identifier ..... on Page ... of Table ..... in Appendix ... (Evaluation of Common Cause Failures). The reliability data for this group can be found on Pages ..... of Table .....

There is also a common cause group for the motor operated steam generator isolation valves ..... which is described on Page ... of Table ..... and the associated reliability data are provided on Page ... of Table .....

All the above mentioned common cause groups have been identified for the "failure to open" failure mode. If the steam generator isolation valves are required to operate, then either a single steam generator needs to be isolated (delta p ... bar protection signal) or the delta p/delta t > .... bar/s protection signal should isolate all the steam generators. In the latter case the success criterion is not fulfilled if one out of N isolation valves fails to close. Therefore common cause failures of these valves for the "failure to close" failure mode would not reveal additional risk contributors, and there is no reason to create such common cause groups. However, if the main steam collector needs to be isolated, the success criterion is the closure of one valve out of three. Thus, it appears that the model ought to be extended with the common cause failures of these valves.

[a] The unique issue identifier JS-012 is composed of the initials JS (John Smith) and a running number for the issues of each reviewer, 12 in this example.

[c] Name of the member of the responding team giving the answer.

Summary of Conclusions from Questions and Answers
Résumé des conclusions déduites des questions et des réponses

A check was done regarding completeness of CCF groups on the secondary side. It appears that CCF identification for isolation valves to open has been done, but not for closing.

Resolution of Issue
Le problème est-il résolu par les réponses? Les réponses sont-elles satisfaisantes?
(Conclusions and Recommendations)

Missing CCF (closing) for the isolation valves of the main steam collector should be introduced.

Short Description of Importance, Priority or Implications of the Issue
Brève description de l'importance, de la priorité, des effets potentiels ou des conséquences du problème

Important for completeness of the model and results.

[a] The unique issue identifier JS-012 is composed of the initials JS (John Smith) and a running number for the issues of each reviewer, 12 in this example.

ABBREVIATIONS

AC	alternating current
ATWS	anticipated transient without scram
CCDF	complementary cumulative distribution function
CCF	common cause failure
CDF	core damage frequency
CEC	Commission of the European Communities (now European Commission)
CET	containment event tree
DBA	design basis accident
DC	direct current
DCH	direct containment heating
ECCS	emergency core cooling system
ESF	engineered safety feature
ESD	event sequence diagram
FCI	fuel-coolant interaction
FMEA	failure mode and effects analysis
HCR	human cognitive reliability
HEP	human error probability
HI	human interaction
HPME	high pressure melt ejection
HRA	human reliability assessment
ICRP	International Commission on Radiological Protection
LD_{50}	the dose at which 50% of a representative group is expected to suffer lethal effects
LOCA	loss of coolant accident
LPIS	low pressure injection system
LWR	light water reactor
MAAP	modular accident analysis programme
MAEROS	aerosol behavior and transport computer code
MCCI	molten core-concrete interaction
MCR	main control room
MELCOR	integrated severe accident progression computer code
MGL	multiple Greek letter (a CCF model)
NEA	Nuclear Energy Agency (of the OECD)
NPP	nuclear power plant
OECD	Organization of Economic Co-operation and Development
PDS	plant damage state
PRA	probabilistic risk analysis
PSA	probabilistic safety assessment
QA	quality assurance
RCP	reactor coolant pump
RCS	reactor coolant system
RHR	residual heat removal
RPV	reactor pressure vessel
SHARP	systematic human actions reliability procedure
SLIM	success likelihood index method
STCP	source term code package
TAF	top of active fuel
THERP	technique for human error rate prediction
WASH-1400	reactor safety study
XSOR	source term codes used in the NUREG-1150 study

CONTRIBUTORS TO DRAFTING AND REVIEW

J.I. Calvo	Consejo de Seguridad Nuclear, Madrid, Spain
L. Carlsson	International Atomic Energy Agency
M. Cullingford	International Atomic Energy Agency
A. Debenham	AEA Technology (SRD), Culcheth, Cheshire, United Kingdom
K. Dinnie	Ontario Hydro, Toronto, Canada
J. Eyink	Siemens AG, KWU, Erlangen, Germany
R. Gubler	International Atomic Energy Agency
S. Hall	AEA Technology (SRD), Culcheth, Cheshire, United Kingdom
F.T. Harper	Sandia National Laboratories, Albuquerque, New Mexico, USA
S. Hirschberg	International Atomic Energy Agency
M. Khatib-Rahbar	Energy Research Inc., Rockville, Maryland, USA
M.T. Leonard	Science Applications International Corp., Albuquerque, New Mexico, USA
J. Munoz	Empresarios Agrupados, A.I.E., Madrid, Spain
T. Okkonen	Royal Institute of Technology (KTH), Stockholm, Sweden
J. Quilliam	Cycla Corporation, Menlo Park, California, USA
P.J. Ross	Nuclear Electric, Knutsford, Cheshire, United Kingdom
T. Spurgin	San Diego, California, USA
A. Torri	Risk and Safety Engineering, Leucadia, California, USA
A. Valeri	ENEA, Rome, Italy
W.E. Vesely	Science Applications International Corp., Dublin, Ohio, USA

Consultants Meetings,
Vienna, Austria:

14 - 18 May 1990; 8-12 April 1991;
17 - 21 October 1994; 14 - 18 November 1994; 12 - 16 December 1994; 19 - 23 December 1994.

QUESTIONNAIRE ON IAEA-TECDOCs

It would greatly assist the International Atomic Energy Agency in its analysis of the effectiveness of its Technical Document programme if you could kindly answer the following questions and return the form to the address shown below. Your co-operation is greatly appreciated.

Title: **IPERS Guidelines for the international peer review service**
Second edition
Number: **IAEA-TECDOC-832**

1. How did you obtain this TECDOC?

[ ] From the IAEA:
  [ ] At own request
  [ ] Without request
  [ ] As participant at an IAEA meeting
[ ] From a professional colleague
[ ] From library

2. How do you rate the content of the TECDOC?

[ ] Useful, includes information not found elsewhere
[ ] Useful as a survey of the subject area
[ ] Useful for reference
[ ] Useful because of its international character
[ ] Useful for training or study purposes
[ ] Not very useful. If not, why not?

3. How do you become aware of the TECDOCs available from the IAEA?

[ ] From references in:
  [ ] IAEA publications
  [ ] Other publications
[ ] From IAEA meetings
[ ] From IAEA newsletters
[ ] By other means (please specify)
[ ] If you find it difficult to obtain information on TECDOCs please tick this box

4. Do you make use of IAEA-TECDOCs?

[ ] Frequently
[ ] Occasionally
[ ] Rarely

5. Please state the institute (or country) in which you are working:

Please return to:
R.F. Kelleher
Head, Publishing Section
International Atomic Energy Agency
P.O. Box 100
Wagramerstrasse 5
A-1400 Vienna, Austria