IAEA-TECDOC-1106

Living probabilistic safety assessment (LPSA)

IAEA

August 1999

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

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

Telephone: (43) 1 2600-22880 or 22866
Fax: (43) 1 2600-29882
E-mail: CHOUSE@IAEA.ORG
Web site: http://www.iaea.org/programmes/inis/inis.htm

Orders should be accompanied by prepayment of 100 Austrian Schillings in the form of a cheque or credit card (MasterCard, VISA).

IAEA-TECDOC-1106

Living probabilistic safety assessment (LPSA)

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

August 1999

The originating Section of this publication in the IAEA was:

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

LIVING PROBABILISTIC SAFETY ASSESSMENT (LPSA)
IAEA, VIENNA, 1999
IAEA-TECDOC-1106
ISSN 1011–4289

Printed by the IAEA in Austria
August 1999

FOREWORD

Over the past few years many nuclear power plant organizations have performed probabilistic safety assessments (PSAs) to identify and understand key plant vulnerabilities. As a result of the availability of these PSA studies, there is a desire to use them to enhance plant safety and to operate the nuclear stations in the most efficient manner. PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit to plant safety can be obtained. However, any PSA which is to be used in this way must have a credible and defensible basis. Thus, it is very important to have a high quality "living PSA" accepted by the plant and the regulator.

With this background in mind, the IAEA has prepared this report on Living Probabilistic Safety Assessment (LPSA) which addresses the updating, documentation, quality assurance, and management and organizational requirements for LPSA. Deficiencies in the areas addressed in this report would seriously reduce the adequacy of the LPSA as a tool to support decision making at NPPs.

This report was reviewed by a working group during a Technical Committee Meeting on PSA Applications to Improve NPP Safety held in Madrid, Spain, from 23 to 27 February 1998. The responsible IAEA officer was A. Gómez Cobo of the Division of Nuclear Installation Safety.

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 IAEA, the governments of the nominating Member States or 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. INTRODUCTION

Nuclear facilities, because of their complex nature, are subject to change with time. These changes can be physical (resulting from plant modifications, etc.), operational (resulting from enhanced procedures, etc.) and organizational. In addition, there are also changes in our understanding of the plant, due to the analysis of operational experience, implementation of data collection systems, development of improved models, etc. Therefore, if the PSA is to be of continuing use in the enhancement and understanding of plant safety, the PSA must be updated or modified when necessary to reflect the above changes. This has led to the concept of a "living PSA".

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

Some PSA applications require the on-line use of the PSA models, and near-prompt knowledge of the risk caused by the actual situation at the plant. This requirement can be satisfied by using a special tool called a safety monitor.

A safety monitor (also referred to as risk monitor) is a plant specific real-time analysis tool used to determine the instantaneous risk based on the actual status of the systems and components. At any given time, the safety monitor reflects the current plant configuration in terms of the known status of the various systems and/or components, e.g. whether there are any components out of service for maintenance or tests. The safety monitor model is based on, and is consistent with, the LPSA. It is updated[1] *with the same frequency as the LPSA. The safety monitor is used by the plant staff in support of operational decisions.*

Historically, PSAs have been developed for a variety of reasons, such as satisfying a regulatory request to evaluate the general level of safety of a plant or a type of plant. Earlier models were developed when the limited capability of software and/or hardware tools required that significant model simplifications be made. In addition, the methodological approach of some early models is no longer considered adequate (e.g., omission of common cause failures or pre-accident human errors). Also, in many cases, the documentation was not prepared in a way which allowed modelling assumptions to be easily related to the plant design and operation. Thus, there are still PSAs which do not meet all the requirements applicable to a PSA which is to be used in the decision making process at the NPPs. While these studies can provide certain insights regarding NPP safety, they are not suitable for supporting design modifications, maintenance planning, optimization of technical specifications, etc., nor as the basis for safety/risk monitors.

---

[1] To update the safety/risk monitor means, in this context, to revise the models and database as changes are made to plant design and operational features, as the level of understanding of the thermal-hydraulic performance or accident progression increases, or as improvements are made in modelling techniques. This updating needs to be done with the same frequency and in a manner consistent with the updating of the LPSA.

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

This means that in order to change a PSA of the type described above into a "living PSA" suitable for applications at the plant, modifications to the models and data would need to be implemented and a full documentation of the model and the process would need to be prepared.

It is not the intention in this report to define the methodology for doing a PSA, which is already extensively covered by other documents (e.g. Refs [1–3]), but instead, to discuss the planning and documentation requirements necessary to ensure that the completed PSA is an LPSA.

For the purposes of the present document, the LPSA is considered to be both the computer model and the supporting documentation. The management, organizational, and quality assurance requirements for the LPSA development phase are discussed in Section 3. Section 4 discusses the LPSA updating process, and the concluding remarks are presented in Section 5. Appendix I provides information on the key elements of the LPSA technical documentation. Finally, a discussion of computer codes for LPSA is presented in Appendix II.

2. GENERAL REQUIREMENTS FOR LPSA

The core of an LPSA is a risk model of the plant which adequately reflects the current design and operational features. As with any model, there are approximations and assumptions associated with it that limit to a greater or lesser extent its domain of applicability. Therefore, the specification of these analytical boundary conditions and an identification of the limitations of the PSA model is an integral part of the definition of the living PSA. Ultimately it is this information which determines the applications for which the LPSA can be used. Therefore, at the initiation of the project, the documentation associated with the work performed in each task and the project as a whole must be designed to meet two basic requirements:

- The basis for the LPSA model should be comprehensively documented so that each aspect of the model can be directly related to existing plant information[2] or to the analysts' assumptions of how the plant and the operating staff behave.

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

These two general requirements are the key features of an LPSA, which are independent of technical aspects such as scope and modelling approach.

[2] Part of the information on NPP design and operational features will be compiled in plant documentation. However, in some cases, information used to develop the PSA models and database is not supported by plant documents but rather, is based on observations by the PSA analysts. For example, information obtained during plant walk-downs is fundamental for the Hazard Analysis, information obtained from interviews and questionnaires to plant staff and from observation of simulator training sessions and maintenance activities are key inputs to the Human Reliability Analysis. All this information needs to be adequately and comprehensively documented in the framework of the LPSA in order to link these plant design and operational features to the appropriate aspects of the LPSA models and database.

Decisions regarding these technical aspects of LPSA are mainly driven by the intended applications of the LPSA and, sometimes, by regulatory requirements.

The *scope* of LPSA is defined according to the following characteristics:

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

It is important that if a utility aims at having a full scope LPSA covering all levels, initiating events, and operational modes, this be developed gradually through a logical step by step procedure.

Whilst the initial focus of the LPSA may be to provide better understanding of the safety of the plant, it is prudent to bear in mind that an LPSA has many potential applications and that their range increases as the scope widens. For example, a Level 1 PSA may be adequate to support decision making in certain areas, but, in many cases, a Level 2 PSA would provide a more sound basis for the decision making process. Another example is the development or not of non-full-power modes PSA. The availability of a Shutdown PSA (SPSA) will allow the LPSA team to perform applications based on comparing risk at power vs. risk during shutdown. All this will need to be considered when planning the LPSA development.

The applications for which the LPSA is intended may significantly affect decisions regarding the *modelling approach* to be used. One example might be the selection of a single configuration for modelling purposes, versus a more detailed representation of operational status. Such a situation can arise when modelling a three loop PWR plant for which it is common practice to model one out of the three steam generators as the faulted loop. Due to this assumption, the frequency of steam generator tube rupture in the assumed faulted generator is a factor of three higher than it should be, while in the remaining two generators there is no corresponding frequency. This distorts the component importance ranking. It is necessary to be aware of this potential difficulty when performing applications of the LPSA; even the initial choice of modelling approach for the LPSA may be affected.

Finally, practical considerations related to the computer codes used to support the LPSA may also have some bearing on model development, since the software capability may limit both the modelling detail and the type of output. Appendix II presents state of the art and desired features for computer codes for LPSA.

3. DEVELOPMENT PHASE OF THE LPSA

An LPSA can be developed either from a pre-existing PSA or, on the other hand, it may be that a completely new study has to be performed. The conversion from a pre-existing PSA is likely to be aimed mainly at including modifications to the models in order to make it suitable for the intended applications, facilitating the updating process, ensuring appropriate run times and improving its auditability.

Whatever the starting point, three aspects are to be considered in planning the development of the LPSA, each of which contributes to its successful completion. These are the documentation, the quality assurance (QA), and the organization and resources required to perform the analysis. Each of these topics is addressed in the following sections.

3.1. DOCUMENTATION

A fundamental requirement for using the LPSA in decision making is that all results, conclusions and recommendations should be traceable to the plant design, construction and operational information. In all aspects of the analysis where assumptions have been made they and their justification should be clearly described.

The documentation for LPSA needs to be organized in such a way that it can be easily updated as changes occur. It may happen that the documentation for the original PSA had been organized in a different way. In this case, some modifications may need to be considered when developing the LPSA in order to make it more flexible and amenable to updating.

In addition, it is possible that additional documents complementary to the documentation of the original PSA may have to be prepared during the development of the LPSA to ensure that the study is performed in a consistent manner and with the right level of quality assurance.

The various documents recommended for the management of the project and for achieving the required technical quality are discussed in the next two sections. The content of the individual technical documents for each of the LPSA tasks is described in Appendix I.

3.1.1. Management of the LPSA

The documentation for the management and control of the development phase of the LPSA normally includes a project plan, a quality assurance plan and quality assurance procedures.

The primary function of the project plan is to ensure that the LPSA's purpose and objectives and hence its scope are clearly understood at the outset of the project. As many of the future applications as possible should be identified, as these will affect the approach to be used in the individual tasks (for example the development of a full scope Level 2 LPSA as opposed to the development of a Level 1+ LPSA[3]). It also identifies the requisite level of QA, and the various reports and procedures which will be produced during the course of the initial development of the LPSA. It is essential to identify the required documentation at the

[3] Level 1+ PSA is a PSA in which accident sequences are developed to Plant Damage States (instead of core damage states, which are the end states for the Level 1 PSA sequences) taking into consideration the status of containment safeguard systems and other features that affect the progression of the severe accident.

beginning of the project, and develop it throughout the course of the work, as much more effort would be required to generate the technical documents discussed in Appendix I after the models have been developed.

QA is discussed in Section 3.2 and Ref. [5].

3.1.2. Technical documentation

The technical documentation covers the development of each of the tasks and the recording and reporting of the work performed. The following sets of documents are recommended:

- Work plan (task procedure) for each of the LPSA tasks.
- Analysis Files for each of the tasks or sub-tasks within tasks, (for example it is recommended to develop analysis files for each individual system in the systems analysis task).
- Document database, identifying all the externally (with respect to the project) and internally generated documents used in the study and their relationship to each other.
- Summary report.

The LPSA should be accompanied by a set of detailed *individual task procedures*. Procedures are understood in this context as a detailed set of steps that give guidance on how to perform the tasks, the techniques to be used and general assumptions to be made. Each task procedure should clearly identify the interfaces with other tasks and the information/data to be exchanged between tasks. The real purpose of these documents is to ensure that all analysts working in a task develop a consistent set of models which interface without overlap or omission. Future revisions to the LPSA will use the same procedures in order to ensure consistency with the original model. Comprehensive information for the development of these procedures is given in Ref. [1]. Appendix I presents the key elements of the work plan for all the PSA tasks.

The *analysis files* are a crucial part of the LPSA. Such files include reports, input data, relevant calculations, and model or database files containing task results. The PSA task reports describe clearly the analyses performed, particularly modelling assumptions, identify interfaces and information or data exchanged between PSA tasks, and provide all the references used. The model or database files that contain the task results include, for example, accident sequences, fault trees, basic event probabilities, etc. The analysis files will be controlled documents which are maintained for the life of the plant. They enable any PSA analyst familiar with the particular task to either recreate or modify the particular part of the model covered in the analysis file. Only if there is a complete set of such files is it possible to define and understand each element of the computer model and the results of its quantification. Appendix I presents the key elements of the analysis files for all the PSA tasks.

The development of the LPSA requires the use of documents held in the plant (P&ID, etc.), and documents generated by outside bodies such as the plant designer, architect engineer, or research organizations. A significant amount of new material is generated during the development of the LPSA, for example, records of information exchange between tasks,

minutes of meetings, procedures, calculation notes, reports, etc. In the future there may be changes to the input documents which will bear on the assumptions and models in the LPSA. In order to facilitate the updating process, it is highly advantageous to have a *document database* which cross references the input, output, and internal usage of the various documents.

The purpose of the *summary report* is to communicate the project motivations, objectives and scope, as well as the essential results, methods and conclusions of the study, to interested users. In addition, the summary report should provide an overview of the contents and organization of the documentation of the study. Section VIII.1 of Ref. [1] suggests the format for the summary report.

3.2. QUALITY ASSURANCE

The importance of QA to LPSA cannot be stressed enough, hence the importance of the Quality Assurance Plan and Procedures. If the LPSA is to be of continuing use in the enhancement and understanding of the plant, it must be based on a secure and traceable process in which all details of the LPSA, including explicit and implicit assumptions, modelling techniques. etc., are fully checked, documented and recorded. The purpose of the plan and procedures is to ensure that the necessary documentation is developed and the review process for all work products clearly specified. The framework for setting up the QA programme for a PSA is presented in Ref. [5]; it is based on and consistent with the IAEA QA guideline [19].

The QA practices and procedures in use at the plant should be considered when QA is planned for the LPSA.

3.3. ORGANIZATION AND RESOURCES

Plant support activities which are not directly associated with the power production processes and the profitable generation of power can sometimes be considered additional constraints or unjustified limitation on the power production. The PSA activities may be perceived as too complex, unrelated to the production process, not representative of the real plant, subject to manipulation by specialists, or an unnecessary requirement imposed by the regulators. If the PSA has not been developed with significant involvement of plant staff at all stages of the development, review and approval processes, it may be seen by the utility as simply a tool for use by research organizations or the regulator.

Therefore, an LPSA can only be developed successfully with the full commitment and support of the plant management and personnel, so that on completion of the initial model it is perceived as an integral part of the plant operational and safety documentation which provides a valuable resource for the safe and efficient operation of the plant.

3.3.1. Organization

The establishment of an LPSA for each plant and its effective use in the management of risk depends on the safety culture at the plant. The development of the model, its scope and the end uses, has to be an integrated plant activity, with the co-operation and assistance of several departments.

However, the LPSA itself can only be performed by a team of analysts who are trained in the methods and techniques needed to develop the model. The wide diversity of expertise on which the team will have to call is reflected in all the areas which have to be considered, such as, thermal-hydraulic response under off-normal conditions, construction of the risk model (fault trees, event trees and quantification of the results), analysis of human performance, structural analysis of the containment response under severe accident conditions, hazard analysis (seismic, fires, floods), source term and radiological analysis, etc. Some organizations may not possess experienced staff in all the areas that need to be covered and may therefore need to use external technical support. In these cases, the selection of qualified support teams and the interfaces with them are very important (e.g. clear definition of expected output, review/validation of the work externally performed, etc.) and it is necessary to allow for close monitoring of external work and to ensure good technology transfer. The NPP organization must hold responsibility for ensuring that their LPSA model accurately represents the plant.

Therefore, the composition of the team and its interaction with different departments in the plant is a fundamental part of the success of the project and the provision of results which will be fully recognized by these departments.

Once the decision is made to go ahead, the first step is for plant management to designate which department takes responsibility for the development and maintenance of the LPSA. Because it covers virtually all aspects of plant performance, it should be placed into a department with strong analytical or safety responsibility. For example, typical departments which have responsibility for a number of existing LPSA are nuclear analysis and fuel, independent safety and analysis group or engineering group.

3.3.2. Resources

The allocation of resources required to develop the LPSA depends on a number of factors which determine the distribution of the work between the plant and other support organizations. Examples of these factors are:

- starting point (i.e. whether an earlier model already exists)
- required level of technology transfer
- number of people who will maintain the LPSA following its completion
- areas in which the utility will take responsibility in the future
- review to be performed by plant personnel.

The key to establishing the credibility of the LPSA for long term applications is to involve the plant staff in the development of the model. Thus, in setting up the project schedule, review activities by plant staff from each area (operations, training, maintenance, system engineers, etc.) need to be included. This will ensure that all hypotheses and assumptions made in the development of the model conform to the known experience from plant operation.

Table I of Ref. [1] presents an estimation of the manpower required to develop a Level 1 PSA at full power. It indicates that a manpower level between 96 and 200 man-months is required depending on the team experience.

4. LPSA UPDATING

The LPSA should be updated as changes occur in any aspect of plant operation or design or if there is improved understanding of thermal-hydraulic or accident phenomenology, new information leading to revised data, or advances in analytical techniques. In the following sections, all of these factors are referred to as "modifications".

Some modifications are originated at the plant. Therefore, appropriate procedures should be put in place to ensure that all of them are reported to the LPSA group. These modifications include plant changes such as permanent configuration changes, hardware changes, changes to the plant operating procedures, maintenance procedures etc. It may be that, as part of the LPSA applications programme, some of these modifications have been analysed with the PSA prior to their implementation at the plant.

Other modifications, such as changes to the component unavailability data due to a review of the plant specific data, are originated by the LPSA group. In addition, the LPSA group will have to identify modifications related to generic issues such as advances in techniques, availability of new information, or experience feedback (e.g. real events not properly represented by the PSA).

4.1. DOCUMENTATION

In order to maintain the LPSA, the following documentation is required: LPSA updating procedure, LPSA update database (log book of changes) and LPSA application guidelines.

The *LPSA updating procedure* describes the steps of the LPSA updating process (see Section 4.3).

All assessed changes to the plant design or operation, including those judged not to impact significantly on the LPSA need to be logged in the *update database*. The former are recorded so that they can be included at a later date when a number of such items cumulatively call for a model update.

In addition, in the framework of the LPSA project it is expected that *LPSA application guidelines* be developed to perform the applications in a systematic and consistent manner.

The introduction of the LPSA into the mainstream of plant operation will also necessitate the modification of plant management procedures so as to define the way in which the LPSA group and the plant staff exchange information and their terms of reference.

4.2. FREQUENCY FOR UPDATING THE LPSA

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

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

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

If the PSA is part of the licensing basis, the frequency for updating the LPSA may be driven by a regulatory requirement.

4.3. LPSA UPDATING PROCESS

The LPSA updating procedure describes the process which is needed to control model revisions. Figure 1 summarizes the LPSA updating process.

The steps in the updating process are the following:

- Preliminary assessment of the impact of modifications on the LPSA model. This implies a qualitative analysis of the identified modifications with respect to the LPSA assumptions, evaluations, models and data. This process allows the LPSA team to decide whether:

  (a) The identified modification does not impact on any aspect of the LPSA, and therefore no update is needed. The modification and the preliminary assessment are logged and no further action is needed.

  (b) The impact of the identified modification is judged not to require an immediate LPSA update. The modification and the preliminary assessment are logged and held for the next scheduled or necessary update.

  (c) The impact of the identified modification is judged to require an immediate LPSA update. The modification and the preliminary assessment are logged and an update is scheduled, taking account of the resources and support required.

- Assessment of how the modification relates to one or more elements of the model. At this point it is necessary to evaluate the need to perform further analyses, e.g. thermal-hydraulic calculations or statistical data processing, and take the necessary actions to compile all the required information to update the LPSA.

- LPSA updating, i.e. implementation of the required modifications, re-quantification of the updated model using the updated database and analysis of results. This process needs to take due account of the QA procedures (e.g. review of the modifications implemented, proper record keeping, etc.).

The documentation of the changes and conclusions is performed iteratively throughout the updating process. All modifications need to be recorded in the LPSA update database (logbook of changes). Modifications that lead to minor LPSA changes, e.g. changes to the documentation, could be included in the form of Addenda (or similar) to the relevant Analysis Files. However, if the LPSA change is substantial, it may be better to reissue part or all of the document. In any case, it will be necessary to revise the document database to reflect the current status of plant information used in the LPSA and the summary report when all affected analysis files have been updated. This completes the LPSA updating process.

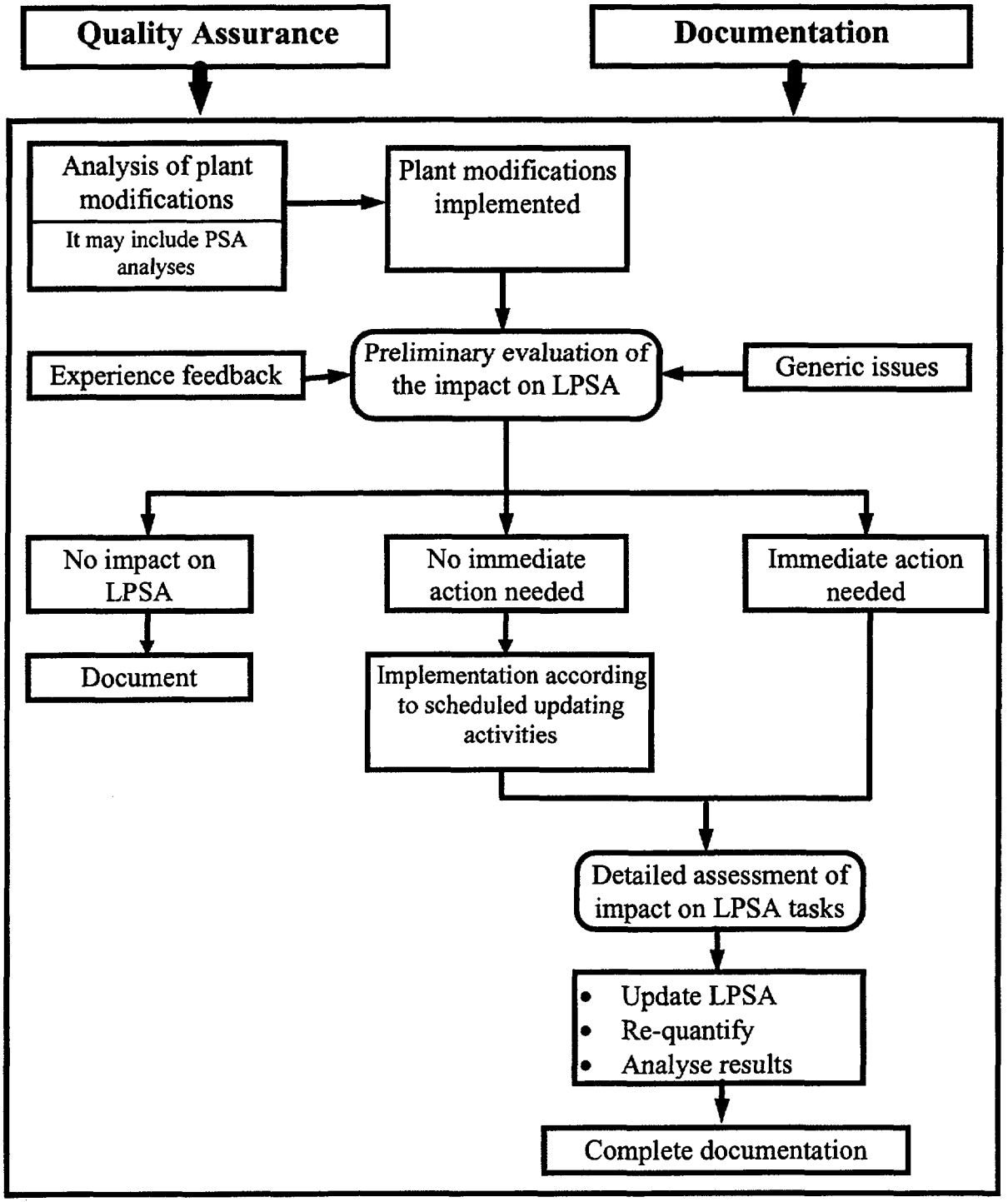

FIG. 1. LPSA Updating process.

4.4. QUALITY ASSURANCE

The same QA procedures used in the development of the model will continue in force for the updating process.

Ref. [5], which is based on and consistent with the IAEA QA guideline (Ref. [19]), indicates that changes in LPSA models, data, information and results, including changes to requirements, scope and objectives and input data, should be made in a controlled manner. The reason for a change should be documented and consideration should be given to the impact and implications of the change. When carrying out a change, in principle, the modifications should be handled in the same way as during the development of the LPSA. If appropriate, this effort can be limited to those parts and aspects of the LPSA which are affected. Activities which should be performed include: information control; configuration control; documentation control; verification and validation; review.

Depending on the type of changes, a new version or an update of the previous LPSA version may be created. If necessary, appropriate and controlled steps need to be taken to store and document the previous version. Information concerning the changes should be transmitted to persons, groups or organizations potentially affected by the changes.

4.5. ORGANIZATION AND RESOURCES

The organization and resources required for the maintenance and update of the LPSA are very much dependent on the number of units owned by the utility, the number of LPSAs, and the intensity of intended applications. Even if a utility itself is maintaining the LPSA, certain areas of the analysis may still be performed by external organizations.

The minimum number of personnel required at the plant would be one dedicated engineer with support from personnel from several plant departments (operations, training, maintenance, etc.). This would imply that the LPSA is being fully maintained by another team. The responsibilities of the plant engineer would be to ensure that all changes at the plant are recorded and the information is made available to the LPSA team. The engineer would co-ordinate visits to the plant, any internal plant review which may be necessary and would also help advise plant management of potential applications of the LPSA.

Alternatively, the utility may have a larger team performing the majority of the activities, and consequently resort to outside organizations only for one or more special areas. In this case, the team would consist of several persons (for example four to seven experts) in different areas of expertise. This team would be responsible for maintaining and updating the LPSA as well as for performing many of the applications.

A utility may well establish the LPSA team at the headquarters, particularly if the safety analysis and design control is done at headquarters.

In each case the LPSA team should be made up from personnel who have a good background in plant operations, maintenance, training, engineering and safety analysis.

It is preferable to develop an organizational structure that allows for potential controversial issues between the LPSA team and other technical disciplines within and outside the organization to be resolved effectively.

5. FINAL REMARKS

The purpose for performing a "living PSA" is to have a risk model of the plant which will be used when making decisions on changes in design or operation, or to meet the needs arising from risk informed or risk based regulation. The availability and use of the LPSA will also help to increase the awareness of the NPP and utility staff of safety aspects and will improve their understanding of where the risk lies.

The LPSA is the basis for applications. The main considerations at the beginning of the process for upgrading an existing PSA to an LPSA must therefore be the planning of the intended applications and the choice of hardware and software support for maintaining and using the LPSA. Use of a state-of-the-art platform will also provide flexibility for future extensions of the model and applications.

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

A high quality LPSA is the starting point in the implementation of an LPSA applications programme. The LPSA needs to be updated as modifications occur in NPP design and operation, new experience feedback is obtained or technological advances occur. This will ensure that the LPSA continues to provide a sound basis for the risk-based or risk-informed decision making process.

Appendix I

KEY ELEMENTS OF THE LPSA TECHNICAL DOCUMENTATION

I.1. INTRODUCTION

As stated in the main text, the two elements of the LPSA are the computer model and all the supporting documentation. In this appendix, for each LPSA task, the information to be included in the work plan (task procedures) and in the task documentation (analysis files) is described. The following sections do not intend to provide guidance on how to perform the various LPSA tasks, but rather, to identify the information that it is necessary to record in order to properly document the principal steps of each of them. There is much guidance available on methods for performing the various PSA tasks, but for each individual LPSA it is necessary to record in detail the exact technique to be used and the assumptions to be made. This is the main purpose of developing the documents referred to in this report as task procedures. Each task procedure should also provide guidance for the information exchange among the different LPSA tasks and for the preparation of the task analysis files.

The task analysis files are a crucial part of the LPSA. These document have been described in Section 3.1.2 of the main report. They contain all the descriptions, models and data associated with the different LPSA tasks. Each analysis file should also include explicit and detailed documentation of the information exchanged with other LPSA tasks and a list of all the references used, including their version number and date.

This appendix is divided into five sections to cover Level 1, 2 and 3 LPSA, hazard analyses and non-full power modes. Its structure is based on practical considerations, that is, the structure of this appendix by no means implies a suggested order for the development of a full scope LPSA. The five sections are divided further according to the related tasks. For each LPSA task two aspects are treated, which are the *key elements for the work plan (task procedure)* and the *key elements for the task documentation (task analysis file)*.

I.2. LEVEL 1 LPSA

I.2.1. IDENTIFICATION AND GROUPING OF INITIATING EVENTS

Key elements of the work plan (task procedure)

Information for the performance of this task is given in Refs [1, 6, 7]. The information contained in these documents can be used to derive the task procedure.

The work plan for the identification and grouping of initiating events may be combined into a single procedure with the work plans on the determination of success criteria and the event sequence modelling tasks. Or it may be that independent procedures are developed for the three tasks. In any case, the work plan needs to address the following:

- Processes to be used in the identification and definition of initiating events.
- Source documents to be used.

- Way in which consequential initiating events are to be developed.

- Process for grouping initiating events.

- Definition of the information to be exchanged with the success criteria, event tree, data, system modelling, human reliability analysis, and quantification tasks.

Key elements of the task documentation (task analysis file)

The task documentation for the identification and grouping of initiating events may be combined with the documentation of the success criteria determination and the event sequence modelling tasks into a single analysis file. Or it may be that independent analysis files are developed for the three tasks. In either case, the analysis file needs to provide a clear definition of each initiating event that is included in the study. This should include where applicable:

- A database of abnormal events and incidents which have led (or could lead) to disruption of normal plant operation. This should include those equipment failures that led to an initiating event and any consequential failures to perform one or more of the safety functions required. It should also include information on any test or maintenance activity taking place at the time which could be related to the event.

- Events based on previous experience at similar plants.

- A record of all failure modes and effects analyses to identify initiating events, capturing all significant assumptions.

- Fault tree and human reliability analyses used to derive initiating events (interface with system analysis and human reliability analysis).

- Derivation of consequential initiating events or cross reference to the document(s) in which they are developed.

- Assessment of the applicability of initiating events to each plant operating mode.

- Derivation of the grouping criteria and the mapping to derive the final initiating event groups.

- Provision of clear definitions of the initiating event groups for the quantification of initiating event frequencies (interface with data and system analysis tasks).

I.2.2. DETERMINATION OF SUCCESS CRITERIA

This is an area of the LPSA for which it may be necessary to make many significant assumptions which may strongly affect the results. Therefore, the documentation of this part of the PSA plays an important role in understanding the results of the study.

Key elements of the work plan (task procedure)

The work plan for the determination of success criteria needs to address the following:

- Sources to be used for the derivation of success criteria.
- Thermal-hydraulic codes to be used for derivation of plant specific criteria.
- Definition of the limiting conditions for success/failure (for example, cladding temperature, coolant system pressure, containment temperature and pressure, etc.).
- Specific acceptance criteria for the performance of equipment during the course of an accident sequence, including minimum system requirements and mission times.

Key elements of the task documentation (task analysis file)

The documentation needs to provide a clear understanding of the success criteria for each event in the event tree. In order to do this the following information should be included:

- Definition of the safety functions and the systems which can perform each of the functions.
- Relationship between the defined safety functions and the event tree headings and functions.
- Success criteria for each safety function, i.e. minimum equipment requirements and mission times.
- Rationale for the use of success criteria for the various initiating event groups from sources other than plant specific analysis.
- Thermal-hydraulic analyses performed to demonstrate that a given system response will prevent the safety limit being exceeded, and those performed to develop timing for operator actions.

I.2.3. EVENT SEQUENCE MODELLING

This task is closely related to those previously described (i.e. definition and grouping of initiating events and determination of success criteria) and therefore it is not uncommon to find that the documentation for these three tasks is grouped together. In fact, the definition and grouping of initiating events needs to be performed on the basis of similar plant response, and the success criteria need to be obtained for any expected accident progression sequence.

As for the task on determination of success criteria treated in the previous section, important assumptions may be made when developing the sequence models which can have a strong influence on the PSA results. Thus, it is very important to develop a comprehensive and detailed task documentation.

Key elements of the work plan (task procedure)

The performance of the accident sequence analysis is described in Ref. [1]. The procedure for this task needs to address the following:

- General assumptions relating to all event tree development.
- Sequence end states.
- Definition of the type of models to be produced (e.g. small event trees and large fault trees) and level at which the event tree headings are to be defined (safety function, system, train).
- Requirements for the development of event sequence diagrams.
- Interface between the initiating event, success criteria, human reliability, system modelling and data analysis tasks.

Key elements of the task documentation (task analysis file)

The documentation needs to provide a clear understanding of the development of each accident sequence in the event tree and sufficient information to set up the boundary conditions for the quantification of each sequence. It is necessary to address the following:

- Description of the evolution of the sequence of events following the representative initiator from each group.
- If event sequence diagrams are developed, the trip parameters challenged to cause the scram, the signals/channels challenged to initiate various safety functions, and the operators intervention in the course of the sequence, either as the result of system failures or in response to changes in plant state, need to be documented.
- Description of each heading in the event tree, and its relationship to a system (or systems) fault tree, human failure event, or other event. (This will include a functional fault tree, top logic or other link to the system models, as applicable.)
- Treatment of dependencies explicitly and implicitly included in the accident sequences.
- Reference to all relevant operational and emergency procedures used in the development of the individual sequences in the event trees. This information will also be used in the evaluation of the operator response modelling and quantification.
- Boundary conditions for each function. These include such things as the impact of the function failure on other functions, environmental and other impacts of initiating events, or dependency on the success or failure of preceding functions.
- Mission time for each function and the justification for each time.

- Description of the development of any basic events used to replace an integrated time dependent function (such as the failure to recover off-site power before a certain time interval has elapsed, given that the diesel generators have failed to supply power).

- All event tree drawings and core damage events (for example vessel rupture), together with an identification of the end state for each sequence.

- All the functional fault tree models (models developed to link the event tree headings with the system fault trees).

- Development of consequential initiators within event trees and transfer of sequences as initiators in other event trees.

- Thermal-hydraulic analyses performed to support event sequence modelling.

- Interface with the quantification task.

I.2.4. SYSTEM ANALYSIS

Key elements of the work plan (task procedure)

Basic information required for this task is given in Section 4.2 of Ref. [1]. The system analysis task procedure needs to cover the following:

- Guidance for the definition/identification of system boundaries and interfaces with other systems. This includes the identification of front-line/support system and of support/support system dependencies.

- Process for determining when a fault tree model will be developed for a system or whether the system will be modelled by a single basic event or a small number of modules (for groups of components within the system).

- Approach to define system boundaries.

- Identification of components and component failure modes relevant to the given system failure event (fault tree top events).

- Approach used to define component boundaries in the mechanical, I&C and electrical subsystems.

- Approach applied for the inclusion of test and maintenance activities into the system model, and the way it is to be documented.

- Way in which the human failure events and common cause failures are to be treated.

- Generally applicable modelling assumptions, e.g. those related to inclusion or exclusion of passive components, criteria for inclusion or exclusion of diversion paths.

- Event naming scheme.

Key elements of the task documentation (task analysis file)

It is necessary that the documentation for the system analyses contain all the information needed to develop the system models. The following information needs to be included:

- Description of the system and its operation modes. Its normal configuration when the plant is at power, its configuration(s) following plant trip, and its configuration for non-power plant states (if shutdown modes are included in the LPSA).

- Reference to all design information/characteristics, including environmental qualification of all system components.

- System success criteria according to the input from the task on determination of success criteria or additional criteria derived for support system models.

- Clear definition of the system boundaries.

- Simplified system diagram including all the components modelled adequately labelled and clearly indicating the system boundary and the interfaces with other systems.

- Information on dependencies for each component/support system/actuation signal interface (e.g. dependency matrix). This should include room/cabinet cooling when necessary.

- Transfer events (fault tree link) for each of the interfaces (downward transfers).

- Information on system tests (e.g. test matrix) including, for each system test, relevant aspects such as test frequency, components and failure modes tested, system realignments and component unavailabilities due to test.

- Information on system maintenance (e.g. maintenance matrix) including tag out boundary, mechanical and electrical, for all components.

- Fault tree modelling assumptions specific to the system (including specific instances of the global assumptions specified in the task plan).

- All assumptions made to simplify the model, such as identification of one train as running in a multi-train system.

- Description of all house events used to deal with asymmetry in the system alignment or to enable the single fault tree model to be used for the various possible system configurations.

- A table showing the house events included in the system models and their settings in each heading, sequence or event tree.

- All top gates which are transfers to other fault trees (this includes all the support system top gates) and any specific boundary conditions (upward transfers).

- If lumped or module events are used in the fault tree (for example for an instrumentation train) the contents assumed within the boundary of the event should be clearly specified. Also, the way in which the reliability parameters are obtained needs to be defined.

- For any hardware recovery modelled, the recovery factor applicable to the given failure event needs to be justified. An alternative to this is to provide clear references to the document where these analyses are described, e.g. the human reliability analysis file.

- For any functional recovery modelled, the logic structure of the model needs to be justified. Also, the conditions under which the alternative performance of a system function is achieved need to be specified. An alternative to this is to provide clear references to the document where these analyses are described.

- Fault tree drawings.

- A list of all the modelled events and their description.

- Qualitative (cut-sets) and quantitative results of the system quantification.

I.2.5. HUMAN RELIABILITY ANALYSIS

Key elements of the work plan (task procedure)

Information required to perform the human reliability analysis (HRA) task is contained in several reports, including Refs [8–10]. The procedure for the HRA task needs to address the following:

- Identification and definition of the types of human failure events (HFEs — basic events which represent the human induced failures of functions, systems or components) that need to be included in the logic model structure.

- The details of the HRA process are different for pre-initiating event HFEs, post-initiating event HFEs and human errors associated with the initiating events (which can be important for the low power and shutdown modes of operation, in particular). Detailed guidance for the implementation of this process needs to be provided.

- Guidance for the identification of opportunities for human/system interaction.

- Criteria for screening out those opportunities that are most unlikely to result in human failures.

- Methodology for the evaluation of probabilities of human failure events:

  - In many PSAs, HRA is done by using initial screening values for the HFEs, and detailed evaluations for those HFEs which are more significant contributors to risk. The approach and criteria for definition of initial screening values needs to be identified. Also, the qualitative and quantitative criteria have to be defined for the selection of HFEs to be analysed in detail.
  - Description of the methodologies to be used for the detailed analyses of the different types of HFEs. This description needs to include identification of the specific plant conditions or performance shaping factors (PSFs) that are assumed to impact upon the probability of HFE.

- Guidance on how to treat dependencies among human failure events both at the system and event sequence levels.

- Guidance on how to analyse human actions included in the hazard analyses, e.g. manual fire suppression or flood isolation, and how to assess the hazard influence on human actions involved in managing hazard caused plant transients (interface with hazard analysis).

Key elements of the task documentation (task analysis file)

The documentation needs to provide a clear definition of each HFE included in the model and the details of the derivation of its probability. This should include:

- Identification of the human/system interaction with which the event is associated. This may be a surveillance test, a calibration, a maintenance action, or a procedure directed response. In the case of responses to equipment failures or other cues, the cues need to be identified.

- Specific human error contributors to the HFEs:

  - Identification of the sub-tasks included as possible contributors to the HFE and the ones which are not included. Rationale for the exclusion of sub-tasks.
  - Identification of the possible human failure modes included (i.e. commission, omission, etc.).

- Determination of the plant specific and HFE specific influence of the factors required by the quantification model. Although no universally accepted objective standards exist for measuring many of these factors, any assumptions adopted by the analysts need to be documented.

- Identification and documentation of the sources of data and information for HRA. Typical sources of data for the human reliability analysis include observations made at the plant or during simulator exercises, review of procedures for maintenance, tests and calibration activities, discussions with and interviews and questionnaires to operational or maintenance personnel, and also plant walkdowns. Since all these elements will constitute a very significant input to the human reliability analysis, they need to be adequately documented.

- Dependencies between HFEs appearing in the same accident sequence cut-sets need to be documented. This documentation should record the process by which the candidates for dependency were identified, the determination of the degree of dependency and the method by which the conditional probabilities were calculated.

- What is equally important from an applications point of view however, is understanding why events are not included in the model. Therefore, the following points need to be documented:

  - Any potential HFEs, or more properly the human/system interactions associated with them, that have been screened out, and the reasons why.
  - Cases where the hardware contribution to the human/system interaction has not been included in the model on the assumption that the HFE dominates. Thus the HFE implicitly includes the hardware failures. Justification needs to be provided.
  - HFEs that are assumed to dominate or lead to a complete dependence of subsequent HFEs. For example, it might have been assumed conservatively that, because of the increased time stress, failure of the first of a set of required actions may lead directly to failure of an associated function, or perhaps even to core damage, whereas, in fact, success is still possible.

- Documentation of the sensitivity analyses performed.

- A list of all the HFEs included in the PSA, and their associated probabilities and uncertainty ranges.

- This task interfaces significantly with the event sequence, system analysis, analysis of hazards and quantification tasks. The information exchanged with these tasks needs to be included.

I.2.6. DATA ANALYSIS

This section deals with the derivation of the independent component unavailability model parameters, certain function or system unavailabilities (when detailed models are not used) and initiating event frequencies. Parameters of HFE models and CCF probabilities are discussed in Sections I.2.5 and I.2.7.

Key elements of the work plan (task procedure)

Information required to perform this task is given in Section 5 of Ref. [1]. The task procedure needs to address the following:

- It is essential that the parameters be estimated using data and other information that is compatible with the definitions of the associated basic events. Therefore, the task procedure must either explicitly contain the appropriate definitions of the events, or must do so by reference to the appropriate task procedures for systems analysis and initiating events. The component boundaries and the interfaces among connected components must be explicitly identified. Since a component may be required for different operating conditions, basic events representing different failure modes may be included in the system model.

- Guidance on how to choose an appropriate data source when generic data sources are used. Also, if several sources of generic data are to be combined, the choice of method needs to be stated and described.

When plant specific data are to be used, the task procedure needs to give guidance on:

- Specific items of data needed to estimate initiating event frequencies, component failure rates, or probabilities and unavailabilities, etc.

- Specific plant information sources to be used in order to obtain information on initiating event occurrences, component failures, equipment outages, numbers of demands or operating times, etc.

- Definition of component families and population of these families.

- Interpretation of the plant records to, for example, allocate a particular historical event to the appropriate data set for the evaluation of basic event probabilities. This includes guidance on identification on how to determine which failure mode the event represents, or in the case of an initiating event, which event group it belongs to.

- Method to update generic (or pre-existing plant specific) data using new plant specific data, for example using a Bayesian approach.

- Method for parameter estimation from the raw data.

Key elements of the task documentation (task analysis file)

The documentation needs to provide clear details of the derivation the probabilities assigned to each event included in the model. This should include:

- Definition of appropriate component populations and their characteristics by reference to the plant design documentation. This is particularly important when using generic data sources, e.g. Ref. [13]. Specific need for updating engineering data occurs when a given component is replaced.

- Description of the rationale for choosing a particular source for those parameters which rely on generic data. The rationale should explain why the source is considered appropriate given the definition of the event in the LPSA. If several sources are combined, the method of combination needs to be explained.

- Where plant specific data is used, a comprehensive and exhaustive collection of all the plant event records, engineering data, and operating history data which have been used needs to be included, or, as a minimal requirement, a reference list for all the records.

- Explanation of the method used for each event record, i.e. whether it represents a specific component failure mode, or whether it represents an initiating event of a specific group. If the content of the event record is not complete or clear, the assumptions made or interpretation derived by the analyst need to be clearly stated.

- Records of the operating history of each component, so that all the information necessary for evaluating component failure parameters is available and traceable. This includes records of operating/stand-by hours, of test/maintenance/repair time history, etc. The interpretation of this plant history to reconstruct demand counts, operational times, etc. must be clearly documented. Any assumptions made to compensate for missing information must be clearly stated.

- Description of the plant operating history, so that the determination of the denominators for the evaluation of initiating event frequencies can be seen.

- Record of the fault trees and human reliability analyses used to calculate initiating event frequencies.

- Estimation of the parameters from the data. This is often done using the Bayesian approach, in which case if generic data is used for the prior distribution. It is necessary that the document explain why it is appropriate. Whatever method is used, the document needs to address the uncertainty in the parameter value.

- List of both the raw data and the processed data.

- This task interfaces with the initiating event, accident sequence, system analysis, and HRA tasks. The information exchanged with these tasks needs to be recorded.

I.2.7. COMMON CAUSE FAILURE ANALYSIS

Key elements of the work plan (task procedure)

The task procedure for the common cause failure (CCF) analysis needs to address the following:

- Guidance for the identification of component groups susceptible of common cause failure.

- Choice of modelling approach (beta factor, alpha factor, etc.).

- Method of inclusion of CCF basic events in the logic model (fault trees), e.g. inclusion of all CCF terms, or inclusion of only the terms required to satisfy the failure criterion.

- Method for parameter estimation for both screening and detailed analyses. Data sources applicable.

- Methods used, if any, to assess the efficiency of existing defensive measures against common cause failures and to consider plant specific experience.

Key elements of the task documentation (task analysis file)

Once the modelling approach has been decided upon, the major effort in performing the analysis is generally in the identification of the CCF component groups and the estimation of the parameters of the model. The documentation of these activities needs to include:

- Qualitative screening analysis indicating reasons for identifying certain CCF groups, and also, the reasons why potential CCF contributions are not considered for other groups of components.

- If a quantitative screening approach has been adopted, the screening criteria used to determine when a detailed analysis is to be performed needs to be specified, and the screening values for the CCF model parameters justified. This will be necessary to determine whether a future modification has the potential for changing the number of groups that should be analysed.

- Method of parameter estimation. If generic CCF parameters are used, the reasons why the values are considered appropriate need to be explicit, so that the impact of any changes on the design and operation of the plant can be assessed. At a minimum, a demonstration that the component boundaries, failure modes and failure root causes are coherent with those assumed in the generic data source needs to be included.

- It is expected that plant specific data on CCFs will be scarce. Also, corrective measures are normally applied following the occurrence of a safety significant CCF, which therefore implies that the expected frequency of re-occurrence of such failure should be lower in the future. The approach to CCF analysis proposed in Refs [11] and [12] requires the creation of a pseudo-plant specific database by reinterpreting industry wide data for plant specific conditions. This involves some assessment of plant specific defences against CCFs relative to those expected for the plant from which the data were originally taken. It is important that these assessments are traceable so that, should operational practices at the plant change, any impact on the defences can be propagated through the analysis.

I.2.8. QUANTIFICATION AND INTERPRETATION OF THE RESULTS

Key elements of the work plan (task procedure)

The detailed quantification process is very much dependent on the computer software used to perform the analysis. A general description of the process is provided in Section 6 of Ref. [1]. The procedure for this task needs to address the following:

- For the quantification of individual system fault trees, a statement of whether to perform a conditional quantification and/or a quantification including the dependency on all support systems.

- Guidance to carry out the interface with other tasks. For example, provision of quantification results for the system analysts so that model revisions can be performed, if necessary, in order to eliminate circular logics or absurd results.

- Determination of the cut-off to be used at each stage of the quantification process.

- Features of the software used which require the analysts judgement, such as using rare event approximation, time dependent analysis etc.

- Guidance for minimal cut-set editing (e.g. deletion of impossible or non-allowed combinations, event probability substitutions, etc.) and treatment of minimal cut-set recovery, based on the results/input from other tasks such as HRA.

- Guidance on the performance of the importance, sensitivity, and uncertainty analysis.

Key elements of the task documentation (task analysis file)

The task analysis file needs to include the following:

- Table of all fault trees quantified, including the name of the top gates quantified, the cut-off applied, the quantified value and the number of cut-sets, as well as a list of all boundary conditions or a reference to where this can be found (house event settings, attributes, exchange events, etc.).

- Description of the way in which circular logic has been removed between front line/support and support/support system fault trees if done within the quantification process.

- Table of all event tree headings (functions) quantified, if this differs from the fault trees quantified in the first step, with the same supporting information.

- Results of all sequences quantified, with a list of the dominant cut-sets.

- Table of all initiating events quantified and their relative contributions to the overall results.

- Details on the analysis and interpretation of results. Details on the importance, sensitivity and uncertainty analyses performed. These are tools that can be used to analyse the results of the LPSA and they are particularly useful when performing an application.

  There are many sources of uncertainty, but they may conveniently be categorized into three groups such as parameter uncertainty, model uncertainty, and completeness uncertainty. Many PSA quantification tools allow the propagation of parameter uncertainty to the final results.

  The task analysis file needs to address the sources of uncertainty and assessments of their potential impact. These are associated with assumptions and approximations whose documentation is scattered throughout the LPSA. Although it may be worthwhile to gather all the uncertainties in one place, it is as a minimum essential that all identified sources of uncertainty be documented and the manner in which they are dealt with described.

I.3. LEVEL 2 LPSA

The development of Level 2 PSA is described in Ref. [2]. This section presupposes that the work required for a Level 1 PSA described in the previous sections has already been carried out. The main elements of a Level 2 LPSA are:

- Interface with Level 1 LPSA
- Containment strength analysis
- Accident progression analysis
- Source terms analysis.

The applicability of the above elements may be dependent on the plant design. The following sections describe the requirements for the documentation of these elements.

I.3.1. INTERFACE BETWEEN LEVEL 1 AND LEVEL 2 LPSA

Key elements of the work plan (task procedure)

The performance of the accident sequence analysis is described in Ref. [1]. The end point for each accident sequence will depend on the scope of the study. If it is Level 1 it would be core damage, or a variant of this (core boiling, limited cladding damage). In the case of a study beyond Level 1, the sequence end state may be different. For example, for plant designs with a containment system, the response of containment systems and the containment itself may be considered. In such a case, the inclusion of containment systems in the event tree would result in the identification of plant damage states. Whatever the original end states defined in the Level 1 study, the Level 1 interface procedure needs to address:

- Identification of modifications which need to be made in the Level 1 sequence analysis to address Level 2 issues. For example, for a PWR, attributes may include: accident progression prior to core damage; system status for accident phases after core damage; status of containment and containment safeguards; reactor pressure

vessel and containment conditions at the time of core melt and vessel lower head failure; timing of events; and reactor building, secondary containment status.

- Definition of categories of end states for event tree sequences (plant damage states in some methodologies).

- Allocation of event tree sequences to the relevant end state categories.

Key elements of the task documentation (task analysis file)

The documentation must provide a clear understanding of the development of each accident sequence in the event tree, sufficient information to set up the boundary conditions for the quantification of each sequence, and the rationale for the choice of end state categories defined and the allocation of sequences to these categories. This needs to include:

- Description of the revised event tree sequences.

- Description of the end state categories.

- Listing of the allocation of sequences to end state categories.

- Description of the criteria used to group event tree sequences into end state categories.

- If the binning process (allocation of sequences to end state categories) is automated, an auditable record of this process should be generated.

I.3.2. CONTAINMENT STRENGTH ANALYSIS

Key elements of the work plan (task procedure)

Containment performance analysis is described in Section 5 of Ref. [2]. The task procedure needs to address the following:

- Scope of the analysis. Identification of the loads to be studied, e.g. pressure, temperature or dynamic loads.

- Identification of the output required from the analysis, e.g. composite fragility curve, individual fragility curves, whether the fragility curves are to represent modelling uncertainty and/or dispersion in input data.

- Identification of methods to be used for modelling containment structural response, e.g. finite element methods.

- Identification of basic models to be used to characterize the loss of containment integrity, threshold model and/or leak before break.

- Identification of how to treat the analysis of the failure of penetrations.

Key elements of the task documentation (task analysis file)

The document must provide sufficient information on the containment structure and the method of analysis to enable any changes to the structure or its design to be investigated. This needs to include:

- References to the finite element analysis, the code and revision number used, input data, and results.

- Containment database, developed as the input deck for any analysis involving information on the containment.

- Uncertainty analysis performed to take account of uncertainties associated with the capacity of the containment under extremes of temperature, combinations of pressure and temperature, localized dynamic loading, thermo-mechanical erosion, and transient peak loading (hydrogen burn).

- Process and results of any expert judgement used to derive the containment capacity and uncertainty parameters.

I.3.3. ACCIDENT PROGRESSION ANALYSIS

Key elements of the work plan (task procedure)

Guidance for performing this task is given in Section 5 of Ref. [2]. The task procedure for the accident progression analysis needs to address the following:

- Definition of the method to be used for grouping accident sequences into plant damage states, providing an important interface with the Level 1 LPSA.

- Definition of the approach to the development of a containment event tree (CET).

- Identification of the method(s) to be used for analysing the progression of severe accidents.

- Definition of the CET quantification approach, including the treatment of uncertainty.

- Guidance on sensitivity studies and/or uncertainty propagation. The current state of knowledge regarding many aspects of severe accident progression and containment performance is imprecise. Therefore, an assessment of the impact of uncertainties on the results is particularly important for establishing the robustness of decisions when using the LPSA as a decision-making tool.

Key elements of the task documentation (task analysis file)

To describe the probabilistic containment performance analysis the following needs to be documented:

- Full description of the containment event tree structure, identifying which phenomena have been addressed (hydrogen generation and combustion, induced failure of the reactor coolant system pressure boundary, debris bed coolability and core concrete interactions, fuel-coolant interactions, melt debris ejection following reactor vessel failure, etc.) and how. Since these issues are subject to uncertainty, care needs to be taken to discuss what has been done in response to this uncertainty (make specific assumptions, incorporate several possibilities in the CET structure, etc.).

  If specific assumptions have been made, the rationale for choosing those assumptions and for rejecting alternatives needs to be explained. It is important for a decision maker to be aware of any assumptions that conservatively or non-conservatively bias the outcomes of the analysis.

  A justification of issues which were excluded from the CET needs to be included.

- Description of the technical basis for the assignment of the probabilities assigned to the events of the CET. In this assignment, care needs to be taken in particular to document whether the assignments are on the basis of analytical or system models or purely on the basis of expert judgement. It is important to distinguish between aleatory and epistemic uncertainty. For example, if several options are included for the outcomes of some of the phenomena, are they being described as the result of random processes (aleatory), or as different hypotheses (epistemic).

- Since they are the most likely subjects of change, systems design and operability issues, and assumptions about operator actions need to be clearly described. For example, assumptions about the completeness or relevance of emergency or other operating procedures to the severe accident regime should be noted.

- When deterministic analyses are used to support the development of the CET, the plant parameters and assumptions used must be clearly specified, so that if any changes are made, their impact can be assessed.

- The quantification process must be clearly described and the results obtained recorded.

- The accident sequence progression analysis interfaces with the Level 1 LPSA quantification task and the tasks of the Level 3 LPSA. There may be an interface with the Level 1 LPSA system analysis, HRA and data tasks, too. The information exchanged with these tasks needs to be recorded.

I.3.4. SOURCE TERM ANALYSIS

Key elements of the work plan (task procedure)

The source term analysis includes two processes, the binning of the end states of the containment event tree into release categories or "bins", and the evaluation of the source term for each of the bins. These two activities are iterative as information on the release mechanisms is required to define a source term and sequences with similar source terms are

binned together. The two steps are described in Sections 5.4 and 6 of Ref. [2]. The procedure for the task needs to address the following:

- Method to be used for assigning severe accident sequences to release categories.
- Definition of information to be provided for each release category (e.g. which fission products, how these are grouped, release timing, height and energy). The information requirements will be affected by the requirements of the Level 3 PSA analysis.
- Guidance on selection of accident sequences to represent each bin and for which source term calculations will be performed.
- Guidance on input assumptions for calculations.
- Plant specific analyses to be performed and surrogate information to be used.
- Computer tools to be used.

Key elements of the task documentation (task analysis file)

The documentation must provide a clear understanding of the development and definitions the release categories/bins and of the calculation of the source term for each of these. This documentation needs to include the following:

- Binning of severe accident sequences and rationale for this.
- Radionuclide grouping scheme used and the assumptions made to obtain it.
- Time periods considered for the release and the rationale for the choice.
- Representative accident sequence selected for each release category and value (depending on scope, fission product releases, energy, timing, etc.) calculated or estimated for the source term for each release category.
- Summary of all computer code calculations used as the basis for estimating plant-specific source terms for selected accident sequences. This needs to include a description of modelling methods and input data used to perform plant specific analyses and a description of the method by which source terms were estimated when computer code calculations were not performed. For example, if analyses of a surrogate (i.e. "similar") plant are used for treating any aspect of radionuclide release, references to, or copies of, the original analysis, and a justification for assuming the applicability of results need to be provided.
- Treatment of uncertainties in the characterization of the source terms.

I.4. LEVEL 3 LPSA

The development of Level 3 PSA is described in Ref. [3]. This section pre-supposes that the work described in the previous section as being required for a Level 2 LPSA has already been carried out.

Key elements of the work plan (task procedure)

The procedure for the Level 3 LPSA needs to address the following:

- Definition of the approach for release category determination considering the source term characteristics, such as magnitude of radionuclides, release timing, release frequency and height.

- Identification of the specific items of data needed to perform probabilistic consequence analysis (meteorological, population, agricultural production, land, food distribution, economic and countermeasures data).

- Identification of method(s) to be used for calculation of:

  - atmospheric dispersion (release of plume, direction and dispersion of plume),
  - surface deposition,
  - calculation of dose (external, inhalation, ingestion),
  - calculation of health effects (early and late fatalities),
  - calculation of economic consequences.

Key elements of the task documentation (task analysis file)

The documentation needs to provide a clear explanation of the derivation of the consequences of an accidental release of radioactivity to the environment. This should include the following:

- Description of the site specific data and assumptions used to perform the consequence calculations.

- Description of modelling methods used to assign consequences to individual accident sequences represented in the probabilistic logic model; this includes a description of the method by which the full spectrum of severe accident source terms generated as part of the uncertainty analysis are linked to a limited number of actual consequence calculations.

- Description of the computational process used to integrate the entire LPSA model (Level 1 through Level 3).

- Summary of all calculated results including frequency distributions for each risk measure.

I.5. HAZARDS ANALYSIS

I.5.1. GENERAL: PLANT WALKDOWNS

Hazard analyses can effectively be supported by local plant walkdowns in order to obtain site specific and plant specific information. The results of the walkdowns may be used during the screening or detailed analyses. Since plant walkdowns are a very significant input to the analyses, guidance on how to conduct them needs to be included in the different task procedures and their results adequately documented in the analysis files.

I.5.2. ANALYSIS OF INTERNAL FIRES

Key elements of the work plan (task procedure)

The starting point for the fire PSA is generally the Level 1 PSA model of the plant. To include the fire induced consequences into the plant response model, the following new aspects need to be addressed in the task procedure (see Ref. [14]):

- General assumptions of the fire analysis.
- Guidance for the identification and definition of fire compartments and cells.
- Screening criteria to be applied during the analysis based on fire impact and frequency.
- Guidance for:
  - Identification of fire sources and ignition mechanisms, and determination of their characteristics (fire severity and duration).
  - Estimation of fire frequencies for both fixed and transient sources.
  - Identification and location of fire targets, especially cable routing.
  - Identification of fire protection measures.
  - Evaluation of fire brigade effectiveness (response times during un-announced drills).
- Method to be used for developing fire growth, suppression and impact analysis, including automatic/manual fire fighting actions, for those scenarios not screened out.
- Guidance for the survey of internal initiating events to identify which can be caused by fire, and the treatment of areas in which there is the potential for more than one initiating event and for the identification of new initiating events.
- Method for the estimation of impact of fires on technological (mechanical, I&C, electrical) equipment with special emphasis on cables and sensitive electronics, to enable correct amendment of system fault trees, safety functions and accident sequences.

- Approach to be used to modify event trees and fault trees for fire scenarios.

- Approach to HRA for fire scenarios.

Key elements of the task documentation (task analysis file)

The fire LPSA documentation needs to be consistent with other parts of the LPSA. In both cases the analysis files must contain clear and explicit information on what assumptions have been made and how these assumptions have been applied to develop the given specific part of the LPSA model. Special attention should be devoted to the following issues:

- Details of the qualitative pre-screening (with reference to the rules in the task plan).

- Description of all fire compartments including information on equipment allocation, potential fire sources and targets, control programmes for combustible and ignition sources, fire load, passive protections, detection and suppression equipment, fire spreading paths, e.g. failed barriers or ventilation ducts, and other information necessary for the analysis. Cable routing information is especially important and should be stored in an adequate database.

- Fire barrier and propagation analysis (barrier penetration analysis).

- Fire severity and frequency analysis:

  - generic hazard data references,
  - plant specific fire characteristics (including assessment of transient combustibles),
  - computation of plant specific fire frequency.

- Details of the screening of fire compartments (with reference to the rules in the task plan).

- Detailed compartment analysis: definition of fire scenarios (source, propagation, detection, human response, damage):

  - breakdown of compartments into cells (sub-compartments), if appropriate,
  - definition of specific sources and targets,
  - fire growth analysis within each cell,
  - identification of automatic and manual actions to prevent fire propagation between cells,
  - analysis of fire impact in each fire compartment defined, i.e. equipment damaged, generation of plant transients (identification of initiating events in each compartment as the result of the hazard), additional effects such as smoke and heat effects and their propagation to neighbouring compartments, etc.

- Accident sequence modelling and quantification:

  - development of fire progression trees showing fire source, defined fire growing stages, success/failure of fire suppression before reaching a given damage stage or triggering of an initiating event,
  - selection of an initiating event per compartment to be the base for the quantification,
  - modification of system models and accident sequences (if necessary) to take into account the impact of fire on safety systems and operating crew response at each defined fire damage stage,
  - quantification of the models.

- Details of the human reliability analysis for fire scenarios.

- Results of the analysis, sensitivity, uncertainty and importance analyses.

I.5.3. ANALYSIS OF INTERNAL FLOODING

Key elements of the work plan (task procedure)

The procedure for the flooding task needs to address the following:

- General assumptions of the flood analysis.

- Guidance for the identification and division of the plant into flood compartments.

- Screening criteria to be applied during the analysis based on flood impact and frequency.

- Guidance for:

  - identification of flood sources,
  - identification of compartment relevant characteristics, e.g. area, drains, communication paths to other compartments, flood barriers, etc.,
  - identification of flood susceptible equipment, and minimal flooding level to produce equipment damage,
  - identification of relevant aspects for flood detection and isolation,
  - estimation of flood frequencies,
  - estimation of flow rates.

- Guidance for the characterization of possible flood scenarios, including flood source and flood rate, affected compartments, evaluation of flood level in affected compartments, identification of time dependent flood impacts, e.g. transient generation, equipment damages, flood symptoms generation, etc., and definition of flood progression stages.

- Guidance for the analysis of human actions for detection and isolation of flood sources as well as for accident mitigation.

- Method for performing the detailed flood analysis. Definition of initiating events and models to be used to characterize flood progression stages.

- Approach to be used to modify event trees and fault trees for flood scenarios.

Key elements of the task documentation (task analysis file)

The following aspects of the analyses already addressed in the task procedure need to be adequately documented:

- Details of the qualitative pre-screening analysis.

- Description of all flood compartments, including information on equipment located in each of them, flood barriers and flood propagation paths, relevant construction details, potential flood sources, minimal water volume needed to affect water-sensitive equipment by immersion, possible flood effects in each compartment (e.g. initiating events, damages to safety equipment) and in neighbouring compartments to which the flooding may propagate, etc.

- Nature of assumed flood causes, e.g. maintenance activities, pipe breaks, expansion joint breaks, etc. Estimation of maximal flow rates and flooding volume that can be delivered by each plant system.

- Location and characterization of flood sources, describing: flooding system, source location, estimation of flood frequencies, relative frequency for the types of pipe break sections considered (e.g. small break, medium break, large break), calculations of flow rate and maximal flood volume, grouping of similar flood cases in flood scenarios, and assumptions made in these processes.

- Details of the quantitative screening of flood scenarios based on criteria established in the task procedure.

- For the detailed assessment of flood scenarios, the following aspects must be documented:

  - for each compartment involved in flood scenarios, evolution in time of flooding level,
  - equipment which is assumed to be damaged by water spray from flood source,
  - flood effects (initiating events, equipment damage) caused by equipment immersion and effects in neighbouring compartments towards which the flooding may propagate.
  - flood progression stages defined, based on progressive damage to relevant equipment,
  - events which can provide flood symptoms and allow for flood detection and isolation. Actions needed for flood isolation,
  - HRA of actions needed to detect and isolate the flood before a given flood progression stage is reached.

- Documentation of the accident sequence modelling and quantification:

  - flood progression event tree, if necessary, showing flood source considered, and flood progression stages reached (leading to an initiating event or relevant system damages) depending on the success or failure of flood isolation actions,
  - for each flood scenario, the initiating event caused by the flood selected to be the base of the quantification,
  - details on the modification of accident sequences and system models (if appropriate) needed to calculate the probability of achieving safe shutdown once the flood has been stopped at a certain progression stage, taking into account the impact of the flood on safety systems and operating crew actions,
  - quantification of the models,
  - assumptions made in all these steps.

- Details of the human reliability modelling for flood scenarios.

- Interpretation of results, sensitivity, uncertainty and importance analyses.

I.5.4. SEISMIC ANALYSIS

Key elements of the work plan (task procedure)

Information required to perform this task is contained in Refs [15, 16]. The task procedure needs to address the following:

- Approach to evaluating and representing the hazard from earthquakes (usually in the form of a frequency of exceedance as a function of some measure of acceleration). This is only likely to change if new information becomes available on the sources and frequency of earthquakes.

- Ground spectra assumed for the earthquake at the site, and damping criteria for the various levels in the structure.

- Approach to evaluating the impact of the earthquake on the plant structures and components (usually represented as fragility curves, that is curves representing the probability of failure as a function of strength of the earthquake).

- Since there is a large number of components which can be affected, it may be that some form of screening is performed to limit the number of failures explicitly included in the model. The screening criteria need to be defined.

- Method for evaluating plant risk by modification of the internal events plant model.

Key elements of the task documentation (task analysis file)

The analysis documentation needs to describe the following:

- Description of the method used to determine the seismic hazard.
- Reference to all historical data used.
- Assumptions and models for aspects such as the characterization of sources and attenuation relationships need to be clearly identified so that the impact of changes in the state of knowledge can be assessed in seismic hazards analysis.
- Fragility analysis and design parameters used for the derivation.
- Modification of the logic model to incorporate the impact of the earthquake on the plant. Special attention needs to be paid to the following:
  - Details of the screening process performed to limit the number of failures explicitly included in the model. This is important so that modifications which might lead to changes in fragility descriptions can be readily assessed.
  - Any assumptions made regarding the correlation between failures of like or neighbouring components or structures need to be identified.
- Quantification, results of the analysis, sensitivity, uncertainty and importance analyses.

I.5.5. ANALYSIS OF OTHER HAZARDS

Key elements of the work plan (task procedure)

Information required to perform this task can be found in Ref. [16]. The task procedure needs to address the following:

- Identification of hazards.
- Approach and criteria for the screening of hazards.
- Approach/method for the analysis of hazards, including modification of plant model to incorporate the impact of the hazard and quantification, HRA analysis, etc.

Key elements of the task documentation (task analysis file)

The documentation must contain the following:

- Clear explanation of why the list of hazards chosen is applicable to the site. Particularly man-made hazards need to be identified to facilitate assessment of changes in any future activities in the plant vicinity.

- For each hazard that is screened in, a characterization of the hazard and the reason for inclusion. If, in the screening, specific design features of the plant have been treated, such as physical barriers or mitigating systems, or credit has been taken for operator action, it is essential that these be identified. The results of the screening process need to be documented, as future changes to the plant could result in a different assessment.

- When a detailed analysis has been performed, the following needs to be documented:
  - Parameter(s) used to characterize the strength of the hazard, and any assumptions made in the development of the hazard curve (characterization of frequency of hazard as a function of strength of impact) along with the method of analysis.
  - Assessment of the impact of the hazard on the plant, as a function of strength of the hazard if appropriate, again including any assumptions made concerning the barriers to impact.
  - Specific modifications to the plant model, particularly modifications to parameters such as human error probabilities.

I.6. NON-FULL POWER MODES LPSA

The LPSA requirements for full power operation are discussed in Sections I.2 through I.5. The same analyses (Level 1, 2, and 3, and external hazards) can be performed for all other modes of plant operation. In general, all the procedures and analysis files required for each of these tasks are also required for all such analyses repeated for the other operating modes.

If the shutdown analysis is being developed as a stand alone section of the LPSA, a complete set of task procedures and analysis files would have to be developed in accordance with the requirements of these sections. If, however, the model is being developed as a continuation of the at power model, which is the optimum way to do it, then it is possible to cover the work by issuing as many task procedures as necessary to cover all the tasks within the Level 1, 2, 3 and hazard analyses for non-full power mode LPSA. The description of the work plan and the development of the task documentation are discussed in the two following sections.

Key elements of the work plan (task procedures)

The task procedures need to address the following:

Level 1

- Radioactivity sources to be considered (in-vessel, fuel pool).
- Characterization of the plant modes and plant operational states (POS) for which the analysis is to be performed. The POS are usually subsets of the plant modes.
- Identification of the POS, defining process parameters, duration, and frequency.
- Identification of initiating events and radioactivity sources for each POS.

- Accident sequence delineation and end state definition (boiling, onset of cladding failure, fuel melt).
- Thermal-hydraulic analysis to be performed for determining timing of the defined end states.
- Assumptions and criteria for system modelling.
- Treatment of data, dependent failures and human reliability.
- Quantification and interpretation of results.

Hazards analysis

- Identification of any differences in the approach to be used for the non-power states in the identification of hazards and the relationship between hazards and the internal initiating events for the non-power modes.

Level 2

- Accident progression analyses to be performed for the various POS to determine the source terms for the various accident sequences.
- Modelling requirements for the determination of fission product pathways when the containment is open.

Level 3

- Treatment of additional source terms arising from the non-power operating modes (timing of release, etc.).

Key elements of the task documentation (task analysis files)

The documentation resulting from the analyses of the non-power modes can be stand alone or a part of the documentation for the analysis of events at power or a combination of the two. For example, the definition of the plant operating states and the rationale for the final number of states is not related to any of the *at power analyses,* so the development of new documentation is logical.

However, for the system analysis, it is easier to simply introduce an additional section to the existing documentation to cover the operation of the system in the non-power modes. New documentation may have to be developed for systems not considered earlier (such as fuel pool cooling). Whichever approach is adopted, the following information, directly related to the non-power modes, is required in the documentation for the various phases of the work.

Level 1

- Derivation of the POS and the information (plant specific or surrogate) used to determine the plant configuration, length of time in each mode and the number of times each mode occurs in a year.

- Analysis of initiating events for each POS, including the derivation of events based on plant operations and operator interactions.
- Event trees for each POS, the event heading and boundary conditions for each event in the event tree and its relation to the system fault tree(s) which make up the event.
- Reference to all maintenance procedures and work plans which are used to define the event tree boundary conditions or system status modelled in the fault trees.
- Derivation of the frequency of the initiating events.
- Treatment of component reliability data, and common cause failure used in the system models.
- Treatment of operator actions: modelling aspects and derivation of the quantified value for each action.
- Treatment of maintenance activities in the system models.
- Details of the modified system fault trees or substitution algorithms for each of the event tree functions for which the fault tree is modified.
- Results of all thermal-hydraulic analyses, including boundary conditions such as: time since shutdown, reactor coolant system water inventory, steam generator availability, core inventory, decay heat curve, and reference to the code used.
- Quantified results with the same level of information as provided for the internal events.

Hazards analysis

The process for the performance of the hazards analysis is the same for all plant modes, although details of the analysis will be different. Thus, it is expected that the documenting of all external events analysis for the non-power modes will parallel that of the at power analysis and therefore, result in the addition of new sections to the existing documentation (see Section I.5).

Level 2

The conditions within the reactor coolant system and containment, once the reactor is shut down and undergoing refuelling, are completely different from those which prevail when the reactor is operating at full power. Thus, the accident progression analysis will be very different and require a completely new analysis and analysis documentation. The documentation of the analysis needs to address the same aspects as described for the Level 2 LPSA in Section I.3 of this appendix.

Level 3

The addition of the new source terms and release categories associated with the shutdown accident sequences will result in a modified Level 3 analysis. The results need to be reported in the same way as the original work described in Section I.4 of this appendix.

Appendix II

COMPUTER CODES FOR LPSA — STATE OF THE ART AND DESIRABLE FEATURES

II.1. INTRODUCTION

As stated in Section 2, the LPSA is a risk model of the plant reflecting its current design and operational characteristics. Computerized tools and procedures play a part in the development, management, updating and use of the LPSA, and therefore the following categories of computer code are of interest:

- Computer codes for the development and maintenance of LPSA models
- Computer codes to assist in the performance of LPSA tasks
- Computer codes for management of LPSA documentation.

An ideal, as yet unrealized with the present generation of commercial codes, is that the latter two categories become integrated into the first. In other words, the LPSA computer model would include the supporting analyses and documentation. Although such an ideal is not practicable at present, the computational features which are used to support some LPSA tasks are already integrated into some of the codes available for model development and maintenance. As an example, several codes used for fault tree and event tree modelling incorporate functionality not only to manage the LPSA basic event database but also to calculate basic event values from lower level parameters. Furthermore, some codes provide facilities which allow documentation to be embedded within the LPSA model. For this reason, there is some overlap between the sections presented below.

All software used for LPSA should be supported by an appropriate level of verification and validation and configuration control. Ref. [5] provides guidance on these issues.

II.2. COMPUTER CODES TO SUPPORT THE DEVELOPMENT AND MAINTENANCE OF LPSA MODELS

II.2.1. GENERAL ISSUES FOR CODES TO SUPPORT THE DEVELOPMENT AND MAINTENANCE OF LPSA MODELS

There are two general questions which need to be asked about computer codes used to support the development and maintenance of LPSA models:

- What data does the code manipulate?
- What functionality does the code provide to manipulate that data?

The data manipulated by the code is not only what is traditionally thought of as the PSA database — i.e. the reliability data — but also the data which represents the fault tree and event tree model, together with any other information which might be considered part of the LPSA model. Examples of the latter are event and fault tree descriptions, model quantifications which were performed, information about analysts who have participated in the model development, logs of model changes, etc. A well designed database including the items mentioned will enhance the potential functionality of the software. Functionality is provided by the computational modules which make up the software.

Administration and protection of project data is one function that the software would ideally provide. If the codes are to be used in a multi-user environment, it is desirable to have access control features to restrict the areas in which a particular user can make changes. Thus, a data analyst might be prevented from making changes to fault and event tree models and a system analyst might be prevented from making changes to event trees and perhaps even to fault tree models developed by another analyst for a different system. Some users might be granted read only access to project data. Other related desirable features are back-up facilities and logging of LPSA changes (to allow trace-back of model versions).

The following sub-sections describe the functionality which may be provided by computer codes used for Level 1, Level 2 and Level 3 PSA model development and maintenance. These codes are usually separate codes. Nevertheless, in order to reduce the potential for errors, it is desirable for them to be properly integrated so that changes in intermediate results due to a change of input parameters in one part of the LPSA model are propagated to other dependent parts of the model.

II.2.2. COMPUTER CODES TO SUPPORT THE DEVELOPMENT AND MAINTENANCE OF LEVEL 1 LPSA MODELS

The following paragraphs provide a discussion of code capabilities. Cost and other non-technical features are not addressed in the following paragraphs. If the code selected does not have all the capabilities needed, additional software or programming of specific subjects may be required.

Model editing

The LPSA needs to be frequently, easily and safely updated. Therefore, the software platform must provide an appropriate set of model manipulation features and these should be readily accessible via a good users' interface. It should be easy to create and update fault tree and event tree models and to manage the project database (e.g. component and human reliability data). An essential feature is that the editing capabilities be well designed so as to reduce the probability of introducing mistakes. Good graphical editing capabilities are desirable, but not strictly necessary, for LPSA development and updating.

Quantification module

A quantification tool allowing fast quantification for models of the size and complexity of the PSA is essential. The quantification tool is a key element of the code. If the code cannot process the LPSA models quickly, excellence in other areas becomes irrelevant.

Cut-set editing

A cut-set editing tool is necessary in order to provide the means to modify basic event values dependent upon the cut-set in which they appear. For example, the introduction of recovery actions and treatment of dependent human errors require basic events to take different values when they appear in different cut-sets.

Results analysis: uncertainty, importance and sensitivity

It should be verified that the code computes the importance measures and handles, at least, the data distributions functions that are to be used.

The code should provide an acceptable way of displaying and analysing risk contributors.

Code output modules

Graphical printing capabilities of LPSA models should be provided. The code needs to have the capability to display a variety of results in the form of graphics and tables.

Other capabilities

Time dependent analysis, pre-installed LPSA applications and automatic fault tree construction can be important for particular cases, depending on the intended use of the PSA.

II.2.3. COMPUTER CODES TO SUPPORT THE DEVELOPMENT AND MAINTENANCE OF LEVEL 2 PSA MODELS

The functionality that a Level 2 PSA code should provide are discussed in the following paragraphs.

Interface with Level 1 analysis

If a separate code is used for Level 2 analysis, it should be possible to import the sequence or cut-set definitions and frequencies from the Level 1 analysis. If the Level 1 code does not provide functionality to bin these sequences or cut-sets in plant damage states, this functionality should be provided by the Level 2 code. Ideally, binning would be an automatic process to reduce the potential for errors.

Event tree construction

The Level 2 code should provide the capability to construct and modify event tree models. The following features, not typically required for Level 1 LPSA, may be helpful when constructing a Level 2 LPSA event tree model:

- Multiple branches for a single event tree node
- Sub-models other than fault trees (e.g. event trees, user defined code)
- Global variables (e.g. to allow tracking of hydrogen generation and combustion at different points in an accident sequence).

Source term categories

It is advantageous for the code to provide a means to automatically bin containment event tree end points into source term categories in accordance with user defined criteria.

Sensitivity and uncertainty analysis

It should be possible to easily perform sensitivity studies to the value of parameters used in the model. A formal uncertainty analysis capability, using Monte Carlo type methods, would be advantageous.

Results analysis

It would be desirable to be able to tabulate the frequencies of source term categories and their contributors. It should be possible to analyse these contributors in terms of Level 1

and Level 2 accident sequences and initiating events. The ability to analyse source term results in terms of component (basic event) failures would also be an advantage.

II.2.4. COMPUTER CODES FOR LEVEL 3 PSA

Level 3 LPSA models usually consist of input files for complex probabilistic consequence analysis (PCA) codes. The advanced codes treat the separate phenomena (atmospheric dispersion, deposition, meteorological sampling, exposure pathways, countermeasures, health effects and scenario consequences) within an integrated structure. As a result, there is on-line transfer of data between calculational modules within the Level 3 model, although transfer of data from the Level 2 PSA may require manual intervention. Thus, the interfaces between Level 2 and Level 3 codes need to be carefully defined in order to reduce the possibility of introducing errors when translating the Level 2 output to the Level 3 input. Adequate configuration control of the model is also important.

It is desirable for the selected codes to use models which are as detailed as practically achievable. This is particularly applicable for the atmospheric dispersion model, where complex treatment requires detailed meteorological data which might not be available, while a single treatment of the dispersion may not be sufficient.

II.3. COMPUTER CODES TO SUPPORT LPSA TASKS

II.3.1. COMPUTER CODES TO SUPPORT LEVEL 1 PSA TASKS

There are several areas in which codes may be used to support Level 1 PSA tasks. Some of them are summarized below.

Data collection and analysis

Data management software and computational tools may be used to collect and store raw data. Moreover, software can play an important role in data processing, in particular in the binning and/or transfer of intermediate data and generation of numerical results. If the LPSA makes use of Bayesian statistical methods, a dedicated analysis module should exist to perform the necessary computations.

Fire and flooding analysis

Fire LPSA analyses may require supporting analyses to determine the times at which critical equipment may be damaged. Codes are available to support this activity: they calculate the heat generated by the fire and the temperature distribution as a function of time and space within the zone analysed.

Flooding LPSA analyses may require supporting analyses to determine the times at which critical levels (equipment damage levels) are reached in the regions analysed. A code to support this analysis need not be particularly sophisticated. It is necessary for the code to calculate the mass balance in the region analysed: on the one hand, flow enters the region due to the flood and on the other hand, mass leaves the region via connections to other regions (e.g. drains, doors).

Accident sequence delineation

Accident sequence delineation is usually supported by thermal-hydraulic analyses. Many specialist codes exist for this purpose. When selecting a thermal-hydraulic code, it is usually necessary to balance several different factors: the experience of the analysts who will use the codes, manpower and computational resources which can be dedicated to calculations, manpower and computational resources required to perform calculations, and the degree of accuracy required from the results.

II.3.2. COMPUTER CODES TO SUPPORT LEVEL 2 PSA TASKS

There are two major areas in which the development of Level 2 models is typically supported by the use of computer calculations:

- performance of accident progression/source term analyses using thermal-hydraulic/severe accident codes,
- analysis of containment structural integrity.

Regarding the first, to cover the whole range of phenomena considered in the Level 2 accident sequences, it would be desirable to have a Level 2 code with an integrated and modular structure. Within this code each separate physical process element can be described with sufficient detail and the intermediate results of separate calculations can be transferred between subsequent tasks in a controlled and well organized manner.

LPSA codes need to have reasonable running times. However, the codes used for containment strength analysis, accident progression analysis and source terms analysis are very complex if they are to model the phenomena treated in sufficient detail. Shorter running times would imply simpler models. To this end, a balance needs to be achieved between the level of detail of the process models used and the calculation times expected.

Types of codes used for severe accident analysis

The codes which model the phenomena of severe accidents can be divided, according to their capabilities, into the following three types:

- Mechanistic codes attempt to model the phenomena in as much detail as possible, and hence the running time of these codes is long. These codes are usually used to provide a benchmark for simpler codes.

- Faster running codes: in these codes the mathematical modelling is complemented by the use of experimental correlations to simplify the code structure and solution method. The user should not use the code outside the range of applicability of the correlation.

- Parametric codes are based on simple parametric models. This type of code is used when a large number of runs are needed to provide a simple overall picture of the case being examined.

Verification and validation

As for other LPSA areas, the Level 2 analysis should be carried out using well verified and validated computer codes. However, the extreme conditions that occur in a severe accident are difficult to obtain experimentally. Therefore, the user should be aware of the degree of accuracy and uncertainties associated with the selected computer code.

Use of codes

The codes should not be treated as 'black boxes'. It is essential that the analysts have a reasonable knowledge of the phenomena associated with severe accidents, the modelling assumptions and the input/output data files. Since the severe accident phenomena addressed are of a complex nature, the LPSA team needs to know how the phenomena are represented and solved within the code.

Details of Level 2 computer codes are given in Ref. [2].

II.4. COMPUTER CODES FOR LPSA DOCUMENTATION MANAGEMENT

There are two ways in which information technology tools can support documentation management:

- Electronic documentation
- Configuration control of documentation.

At present, few codes are available which are specifically designed for LPSA documentation management. However, much of the functionality described below can be obtained using general information processing software packages which are commercially available.

Electronic documentation would use modern media and information technology to maintain the LPSA documentation in an easily retrievable format (e.g. CD-ROM or more advanced systems). In an ideal system, this documentation would be the entire LPSA; it would include all the files and the computer models for the initial LPSA and subsequent updated models. An electronic documentation system would simplify the tracking and correction of errors which may be introduced at some point. Electronic documentation would also provide some usability advantages over paper documentation. For example, hypertext features would facilitate traceability between different parts of the documentation. A good electronic documentation system would simplify updating of the LPSA. In particular, it would play an important role in ensuring that all changes needed were made in all the affected parts of the LPSA documentation.

Beyond the form of storage chosen for the LPSA documentation — i.e. whether it is paper based or electronic — all of the documents which are necessary for future use and development of the LPSA should be placed under a configuration management system, as indicated in Ref. [5]. Such a system need not necessarily be a software based system. Nevertheless, an electronic database offers the advantage of enhancing information availability and retrievability.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

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

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

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

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

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

[9] GERTMAN, D.I., BLACKMAN, H., Human Reliability, a Safety Analysis Data Handbook, John Wiley and Sons, New York (1994).

[10] UNITED STATES NUCLEAR REGULATORY COMMISSION, Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Rep. NUREG/CR-1278, USNRC, Washington, DC (1983).

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

[12] UNITED STATES NUCLEAR REGULATORY COMMISSION, Procedures for Treating Common Cause Failure in Safety and Reliability Studies, Vols 1 & 2, Rep. NUREG/CR-4780, USNRC, Washington, DC (1988, 1989).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478, Vienna (1988).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Reports Series No. 10, IAEA, Vienna (1998).

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessments for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1998).

[17] COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS (CSNI) OF THE OECD NUCLEAR ENERGY AGENCY, State of Living PSA and Further Development — Final Draft, NEA/CSNI/R(98)11, Paris (1999).

[18] SWEDISH NUCLEAR POWER INSPECTORATE, Safety Evaluation by Living PSA, SKI Report 94:2, Stockholm (1994).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

ABBREVIATIONS

CCF	common cause failure
CET	containment event tree
HFE	human failure event
HRA	human reliability analysis
I&C	instrumentation and control
LOCA	loss of coolant accident
LPSA	living probabilistic safety assessment
P&ID	piping and instrumentation diagram
PCA	probabilistic consequence analysis
POS	plant operational states
PSA	probabilistic safety assessment
PSF	performance shaping factors
PWR	pressurized water reactor
QA	quality assurance
SPSA	shutdown probabilistic safety assessment

CONTRIBUTORS TO DRAFTING AND REVIEW

Afzali, A.	Scientech Inc., United States of America
Bento, J.P.	KSU, Swedish Nuclear Training & Safety Centre, Sweden
Boneham, P.S.	ENCONET Consulting Gmb., Austria
Désille, H.	Technicatome, France
Dewailly, J.	Electricité de France, France
El-Shanawany, M.	Nuclear Installation Inspectorate, United Kingdom
Evans, M.G.K.	Scientech, Inc., United Kingdom
Fornero, D.A.	Nucleoeléctrica Argentina S.A., Argentina
Gómez Cobo, A.	International Atomic Energy Agency
Graham, A.	Nuclear Electric Ltd, United Kingdom
Guymer, P.	Scientech, Inc., United Kingdom
Holló, E.	VEIKI Institute for Electrical Power Research, Hungary
Kafka, P.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Germany
Kattainen, M.	IVO Power Engineering, Finland
Kovács, Z.	RELKO Ltd, Slovakia
Lioubarski, A.	SEC NRS of Gosatomnadzor of Russia, Russian Federation
Martorell, S.	Universidad Politécnica de Valencia, Spain
Meslin, T.	Centre Nucléaire de Production d'Electricité de Saint Laurent-des-Eaux, France
Parry, G.	United States Nuclear Regulatory Commission, United States of America
Preston, J.	Electrowatt Engineering (UK) Ltd, United Kingdom
Rivero Oliva, J.	Instituto Superior de Ciencias y Tecnología Nucleares (ISCTN), Cuba
Seebregts, A.	Netherlands Energy Research Foundation (ECN), Netherlands

Versteeg, M.F.	Ministry of Social Affairs, SZW/KFD, Netherlands
Xue, D.	Institute of Nuclear Energy and Technology, Tsinghua University, China
Yllera, J.	Consejo de Seguridad Nuclear, Spain

Consultants Meetings

Vienna, Austria: 3–7 June 1996, 16–20 June 1997, 26–30 January 1998, 8–12 June 1998

Technical Committee Meeting

Madrid, Spain: 23–27 February 1998