IAEA-TECDOC-1101

A framework for a quality assurance programme for PSA

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

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).

A FRAMEWORK FOR A QUALITY ASSURANCE PROGRAMME FOR PSA
IAEA, VIENNA, 1999
IAEA-TECDOC-1101
ISSN 1011–4289

Printed by the IAEA in Austria
August 1999

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

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

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

- **Safety Fundamentals** (silver lettering) present basic objectives, concepts and principles of safety and protection in the development and application of atomic energy for peaceful purposes.
- **Safety Requirements** (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.
- **Safety Guides** (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

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

OTHER SAFETY RELATED PUBLICATIONS

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

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

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

FOREWORD

Reviews organized by the IAEA of probabilistic safety assessments (PSAs) of nuclear facilities have, in the past years, shown significant progress in the technical methods and data used for these studies. The IAEA has made a considerable effort to support the development of technical capabilities for PSA in Member States and in writing technical procedures for carrying out PSAs. However, the reviews have also shown significant deficiencies in quality assurance (QA) for PSAs, ranging from no QA at all to inappropriate, inefficient or unbalanced QA. As a PSA represents a very complex model which describes the risk associated with a nuclear facility, an appropriate and efficient QA programme is crucial to obtain a quality PSA.

Historically, in the first integral PSAs, many of the PSA elements were handled by independent groups. These elements were finally integrated and put together in the overall model. Many of the interfaces between the elements or tasks were handled as appropriate by exchanging information in oral or written form. Since WASH-1400, the first integral PSA, the process of constructing the PSA model has been further developed. PSA elements previously considered separately can now be handled together with the capable software developed in recent years. Software has made interface control and data transfer easier to perform, but also permits the development of more detailed and complex models. Previously, QA for PSA projects was organized in an ad hoc manner and was sometimes very limited. In recent years, increasingly comprehensive QA programmes have been developed and implemented for PSA projects. Today, a comprehensive, effective and performance-oriented QA is considered to be essential for a reliable and credible PSA.

This report describes the framework for developing an adequate QA programme for PSA studies. The framework is based on and is in accordance with the related QA guidelines of the IAEA for safety in nuclear power plants and other nuclear installations. The report identifies the key areas that are recommended to be addressed by a QA programme. For detailed technical descriptions of PSA methods, the reader should refer to the related IAEA PSA procedures.

This report was reviewed during a Technical Committee Meeting on PSA Applications to Improve NPP Safety held in Madrid, Spain, in February 1998.

The IAEA officer responsible for this report was R. Gubler 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

A probabilistic safety analysis (PSA) of a nuclear power plant represents a complex model of the plant. In recent international peer review service (IPERS) reviews of PSAs it was recognized that quality assurance (QA) for such studies is critical for the correctness and adequacy of a PSA model. Performing a PSA of a nuclear power plant is a difficult process. It involves multidisciplinary teamwork where participants with expertise in highly specialized areas provide the intimate knowledge of plant design, plant operations and PSA techniques and methods. Staff selection, internal and external project communication, computer software configuration control and document control are crucial to the effectiveness and quality of PSA projects. Therefore, it is recommended that a detailed QA programme be established and made effective in every PSA project. An effective QA programme will also enhance confidence in the PSA models and results.

Because PSA has developed to such a degree that it influences the design and operation of nuclear facilities, the requirement to establish and implement a QA programme for PSA is in accordance with and complements the overall QA guidelines of the IAEA for nuclear facilities. For the PSA 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 PSA, including explicit and implicit assumptions, modelling techniques, etc. are fully checked, documented and recorded. The purpose of the QA plan and procedures are to ensure that the necessary documentation is developed and that the review process for all work products is clearly specified.

The authors assume that the organizations involved in a PSA project adhere to an overall QA programme and that the QA of the PSA project is based on this overall QA programme. It is further assumed that general management principles exist which are used to locate and organize the responsibilities and staff for the PSA project. In many places PSA tasks are carried out by separate groups at different organizations. In such cases appropriate co-ordination and organization of interfaces have to be established in accordance with the practices followed at those places.

1.1. BACKGROUND

This report describes the framework for developing an adequate QA programme for PSA projects for nuclear facilities. The framework is consistent with and complements the requirements and recommendations of QA for safety in nuclear power plants, as described in Safety Series No. 50-C/SG-Q [1] The IAEA publications referred to in this report are listed in the references.

1.2. OBJECTIVE

This report is intended to provide guidance for developing and establishing a QA programme for conducting a PSA project for a nuclear facility. It describes the essential principles and elements of a QA programme for a PSA project, including managerial and organizational aspects to the extent useful and necessary. The report is intended to be of use to all persons involved in carrying out a PSA project, reviewing a PSA and applying a PSA.

For PSA, appropriate quality means an end product which adequately meets the objectives and fulfils the scope of the PSA. A QA programme for a PSA encompasses all the activities which are necessary to achieve the appropriate quality.

1.3. SCOPE

This report describes the QA aspects and approach for PSA projects and it applies to all organizations performing activities affecting the quality of the PSA and of its application. In addition, the report applies to the QA programme of the organization having overall responsibility for the PSA project as well as to any other organizational entity providing support to the PSA.

1.4. EXCLUSIONS

This publication does not provide a QA framework with regard to the use of PSA for continuous on-line monitoring and control of the risk of a facility. Additional QA requirements for this kind of PSA application go beyond the scope of the present report. Much of the guidance is applicable, but significant expansion is required for this application.

1.5. STRUCTURE

This report is divided into five sections and three appendices. Consistent with Ref. [1], the main body of the report addresses "management", "performance" and "assessment" (Sections 3, 4 and 5, respectively):

- Section 2 provides a description of specific characteristics and features of PSA projects important for QA.
- Section 3 provides guidance on the management of PSA activities. Management aspects include the development, implementation and maintenance of the QA programme, training and qualification of staff, PSA documents and configuration control, and non-conformance control and corrective actions.
- Section 4 provides guidance on the performance of PSA activities. Performance aspects deal with the work process and how it is carried out under controlled conditions.
- Section 5 provides guidance on the assessment of PSA activities. Assessment comprises measuring the effectiveness of management processes and the adequacy of work performance.
- Appendix I provides examples for the typical documents contained in a PSA QA manual.
- Appendix II provides an outline of a PSA project plan.
- Appendix III provides technical instructions for system analysis, as an example.

2. GENERAL CONSIDERATIONS

A PSA is an integral assessment of plant safety which goes beyond the conventional safety analyses of the deterministic type in that a complete set of events and combinations of events leading to core damage and to releases of radioactive materials are considered. It can be used to optimize plant design and operational features to enhance plant safety during all operational stages of the plant. Ideally, PSA work starts at the conceptual and design stage of a plant. At this stage generic data e.g. component failure parameters, have to be used in the models. Non plant-specific failure data parameters can introduce comparatively large

uncertainties in the PSA results. These uncertainties should be appropriately considered when applying the PSA information and results to the design studies of the plant.

At a later stage, during construction and final detailed design for example, the PSA is updated to reflect the latest available information. The potential uses for the PSA at this stage are for improvements in the detailed design or for the development of operational procedures. For the commissioning phase, the PSA can be used to improve the commissioning programme in order to concentrate on critical components and on operating specifications for commissioning which reflect the requirements for important accident sequences. During the operating phase experience data are collected and the PSA is updated periodically to reflect the increasing experience basis. This is the 'living PSA' concept.

A PSA project may consider a full scope PSA study, covering Levels 1, 2 and 3, all operational conditions including shutdown conditions and all kinds of initial disturbances or initiating events. It also may be limited to a particular aspect, level or scope.

The PSA project plan and QA programme should identify the intended users and recipients for the PSA and identify the expected benefit for each user.

A considerable effort has been made at the IAEA in recent years with respect to the development and documentation of state of the art methods and data for PSAs of nuclear facilities. The IAEA has published detailed technical reports which provide guidance on the selection and application of adequate methods and data and on the appropriate modelling of the technical and operational features of the plants.

The establishment of a QA programme is an essential aspect of good management and is fundamental to achieving a quality PSA. The QA programme sets forth the methods, resources, controls and procedures, and defines the responsibilities and lines of communication for activities affecting the quality of a PSA. These communication arrangements should include consideration of interfaces both within the PSA team and between the PSA team and external sources of information. Arrangements for control and documentation of information from sources external to the PSA team should be included in the QA programme.

Owing to the different situations which exist in Member States for PSA projects, the present report is restricted to the description of the principles and elements of QA for PSA and relies on typical examples in terms of the QA programme documents. In this regard, it must be stated that the principles of the QA programme described herein need to be specifically developed and adapted for a particular PSA project and associated organizations, based on the guidelines of the overall QA programmes which might be applicable and on the PSA practices available. The QA programme should be designed to apply to all phases of the PSA project and should include, with appropriate detail, all the tasks in the PSA project.

In particular the living PSA concept depends on the effective application during all PSA phases of a well developed and maintained QA programme. Success in developing a living PSA is a direct result of the initial QA measures taken. Inadequate QA measures employed in the early stages of a PSA may lead to loss of information and may severely limit the usefulness of the living PSA.

Most PSAs are carried out by a PSA team with as a minimum a small group at the plant which is responsible for collecting and providing plant information and for actual applications of

the PSA at the plant. The size and structure of the PSA team which carries out the PSA can vary from a very small and homogeneous team to a large team composed of individuals from several organizations. This aspect needs to be adequately reflected in the QA programme. For a PSA team which is split into several organizations, the structure, responsibilities, communications, working instructions, procedures and information control require particular attention.

Because too many practices and situations may apply for such a project in Member States, the present report does not outline the management structure to be established for a PSA project. This aspect remains the responsibility of the users of this report. It is incumbent on them to assure that the management structure is such that it provides planning, direction, resources and support to achieve the objectives of the project. However, once the organization is specified, the structures and functions of organization and management are subject to QA and are spelled out in the QA documents of the PSA project as needed.

The functional requirements and rigour of a QA programme apply universally. QA for a PSA project should not be seen as a static task which, once established, can be applied in a schematic fashion. It should be performance oriented, efficient and open for improvements in an ordered manner.

3. MANAGEMENT

3.1. QA PROGRAMME

The responsible organization should develop and implement a QA programme which includes details on how the work of the PSA project is to be managed, performed and assessed. It covers the organizational structure, functional responsibilities, levels of authority and interfaces for those managing, performing and assessing the work. It addresses management measures, including planning, scheduling and resource considerations as well as working procedures that provide guidance on actual work performance. The documentation structure of a QA programme for a PSA project is illustrated in Fig. 1. Particular attention should be given to the following areas:

- Development of a thorough understanding by the PSA team of design and operational features of the plant and access to complete plant information;
- Clearly defined objectives and purpose of the PSA;
- A PSA project plan including a project approach with a clear definition of the scope, type and depth of analysis;
- Appropriate selection and identification of the methodology and data to be employed;
- Organization, qualification and commitment of the project team and expertise and skill of task leaders and individual analysts;
- Appropriate document and configuration management;
- Thorough control with respect to interfaces between tasks and staff involved in the PSA;
- A comprehensive technical review programme.

The QA programme should cover all the envisaged phases of the PSA project and the associated management controls. This includes, for example, QA planning, information control,

organization and training, and it should provide for the assessment of all the functions. Organizational responsibilities and authorities for the conduct and approval of activities affecting quality should also be defined. General guidance for the programme can be found in Section 2 of the Safety Standard "Quality assurance for nuclear power plants and other nuclear installations" and Section 3 of the Safety Guide Q1, both contained in 50-C/SG-Q [1].

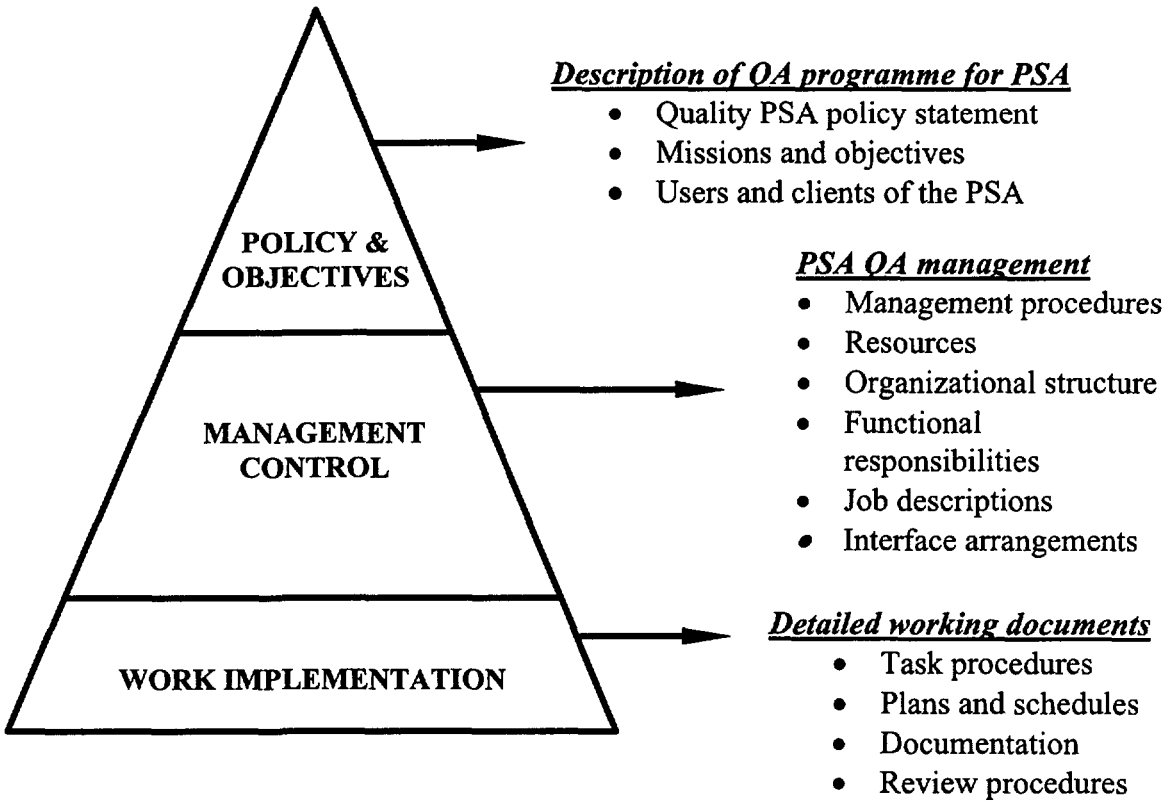

FIG. 1. Typical documentation structure of the QA programme for PSA, adapted from Ref. [1].

3.1.1. QA programme documentation

As described in the Safety Guide Q1 [1], Section 3, the PSA project QA programme should be developed to cover:

- QA programme description
- Management documents
- Working documents.

Section 3 of Ref. [1] gives guidance in the preparation of the QA documentation. The documentation of the QA programme should include standards, QA procedures, the PSA project plan, and related work procedures and instructions. Special project procedures should be generated or adopted for the project, for example, the preferred language, defining QA policy, requirements and responsibilities.

Preparation of the QA programme is required at the outset of the PSA project. It should incorporate, as appropriate, a flow chart or sequential narrative listing of steps and tasks which are to be performed in the development of the PSA. It should indicate the interfaces required between the constituent parts and the different phases of the PSA project and the necessary information flow between them. The information should be described in terms of the data required as input and the form and detail of the results required as output for each part or phase.

The programme should also identify procedures, work instructions, and assessment (audit) and review specifications which are to be used in the development of the PSA. The technical instructions are detailed directives on how general or specific activities are to be performed. They delineate the explicit methods and processes to be used to ensure that the work performance and recorded results will comply with requirements. The QA activity and task procedures for any part of the PSA project should be issued prior to the commencement of any work on that part of the project and should be subject to review and approval before issue.

3.1.1.1. QA programme description

The QA programme description should establish a basis for the PSA project management by including the following:

(1) *A statement of the overall QA programme of the responsible organization.* This paragraph states which overall QA programme applies. Possible interfaces with other QA programmes should be addressed.

(2) *A statement of the PSA project objectives and requirements.* This part should summarize the objective, scope and users of the PSA in terms of the results to be obtained and the uses to which the results are to be applied, the level of detail to be modelled, overall detail required in the results, and any special features required. This information is typically contained in more detail in the PSA project plan (see Appendix II for a sample outline of a PSA project plan). This item can be replaced by a reference to the project plan.

(3) *Organization, responsibilities and resources for the project.* Describes in detail the functions, authority, responsibilities and accountabilities of units and individuals within the organization. The interactions among the groups involved in the PSA project and with other groups, for example the review organizations, are to be established. A description of the PSA project organization should be included.

(4) *Integration of QA programmes.* These include the QA programmes associated with portions of the overall programme delegated to participants for implementation. They cover the responsibilities in each organization or group for the delivery of the different work packages. The QA programme may also consider other items which can affect the quality of the PSA, including purchasing of items and services (e.g. consulting contracts). The responsible organization should retain the overall responsibility for the implementation and effectiveness of the PSA QA programme.

(5) *The lines of internal and external communications and interface arrangements.* This includes the co-ordination of activities required among the different organizations and groups and defines the interfacing between the constituent parts of the analysis.

(6) *Requirements for staff training and special expertise.* The training of staff and levels of expertise required to achieve the appropriate quality for each activity should be described and substantiated.

(7) *Working documents.* The QA programme description should include a commitment to develop the necessary working documents.

(8) *Assessment.* The QA programme should summarize the processes for evaluating the PSA work in relation to the following characteristics:

- Completeness
- Consistency
- Accuracy.

An important element of this assessment are reviews at the various levels and stages of the work performed. If necessary, the activities should also include details of the QA for the software used in the PSA.

(9) *Documented review process.* Review processes should be spelled out in a document to this effect. For each review findings and the resolution process should be documented.

3.1.1.2. Management documents

These documents are administrative in nature, as for example, in the area of planning and scheduling of activities. In combination they will provide the schedule of activities for the overall QA programme of the PSA project and for its management throughout the development, resourcing, analysis, and application of the PSA.

3.1.1.3. Working documents

Work procedures and instructions can be large documents. Appendix III contains an example of the technical instructions for system analysis. The purpose of this example is not to describe the technical state of the art of system analysis, as technical methods evolve constantly, but to show the level of detail and the kind of controls implemented in the task process. Where existing standards are adopted, the work procedures should indicate the source and the sections applicable. For the development of the technical instructions, the descriptions given in the general PSA procedures (e.g. Refs [2, 3]) normally need to be complemented and expanded by inclusion of the detailed practices used for the PSA project. The degree of specification of methods in the general PSA procedures is usually insufficient because these procedures allow for different methods or variants of methods to be used for many PSA tasks. Work procedures and instructions for a PSA project should be specific as to the approach used for PSA tasks. Also, the individual activities related to QA need to be included in detail. A list of typical procedures contained in a QA programme for a PSA project is provided in Appendix I.

3.1.2. Establishment and implementation of the QA programme

To establish the QA programme, reference should be made to Ref. [1].

3.2. ORGANIZATION

The responsible organization should establish the organizational structure, laying down clearly defined responsibilities, levels of authority and lines of communication. The originating organization retains responsibility for the following areas:

- Establishment of the overall QA programme for the PSA;
- PSA project plan (see Appendix II for the outline of a typical plan);
- Involvement in technical reviews;
- Approval of reports.

The position of the QA function in relation to the project organization should be clearly indicated, including lines of reporting to higher management and communication with other organizational units. For complex PSA teams it might be necessary to establish special groups or positions in the programme for co-ordination and review. This may be particularly appropriate, for example, where dispersed groups of specialists are involved. A description of functions and organizational responsibilities can be found in the Level 1 PSA procedures (Ref. [2], page 13).

Responsibilities for the establishment and implementation of an effective QA programme need to be clearly defined following the practices applicable to the organizations where the PSA project is carried out. General guidance is given in Ref. [1]. The duties, authorities and responsibilities of all members of the PSA project must be clearly identified and documented for each phase of the project. Typical duties, authorities and responsibilities for the key activities in a Level 1 PSA project are given in Ref. [2], Section 2.

3.3. INTERFACES

Due to the complexity of a PSA project, various internal and external interfaces have to be carefully considered and defined in detail in appropriate procedures. For the control of interfaces, reference should be made to Annex II of Ref. [1].

3.4. STAFFING, TRAINING AND QUALIFICATION

The quality of the PSA is directly related to the competence of the individuals developing the PSA. Therefore, plant familiarization and training in appropriate PSA aspects and PSA QA is essential for all personnel performing and verifying the activities affecting the quality of the PSA. Also, senior management should be strongly committed to and supportive of training. Appropriate statements of the responsible organization should be issued expressing commitment and support for training. The basic principles regarding training and qualification are described in Ref. [1], which recommends the establishment of job descriptions and their inclusion in the documentation of the QA programme.

The expertise needed to conduct a PSA must consist of two essential elements : the knowledge of PSA techniques and an intimate knowledge of the plant. This expertise can vary in depth, depending on the scope of the PSA, but the participation of the utility is essential as well as the availability of design information. For a description of the typical areas of expertise required (see paragraph 2.5.2 of Ref. [2].

3.5. PLANNING

Project planning should take place at the earliest opportunity before the start of PSA activities. Activities should be defined in the project plan (see Appendix II). Technical details can be found in the Level 1 PSA procedures (IAEA Safety Series No. 50-P-4 [2]).

3.6. NON-CONFORMANCE CONTROL AND CORRECTIVE ACTION

Control of non-conformance and the corresponding organization of corrective actions are described in Ref. [1]. The focus of this guide is non-conformance which could have a direct and immediate safety impact on the nuclear facility. The guide allows for a graded approach to handling non-conformance. Typically, for a PSA project there is no immediate and direct safety impact of the project work. Nevertheless, non-conformance could have a major impact on the quality of the PSA and hence on the safety related decisions taken. Therefore, regarding the grading scheme given in Ref. [1], a Grade 2 or 3 approach seems appropriate for a PSA project depending on the severity of the non-conformance noted, on the size of the PSA team and on its organizational complexity.

Systematic control should be maintained over the identification, documentation and disposition of non-conforming items. Procedures and working instructions specify checks and reviews which should identify deficiencies and provide assurance that only acceptable outputs are obtained. The handling of non-conforming work is controlled in accordance with applicable procedures and working instructions.

If a deficiency or non-conformance to specific requirements is identified during the course of the project, then provision is made by the person responsible for carrying out the work to assess the situation. Once the cause of the deficiency is identified, corrective action is taken if necessary.

If a deficiency in the QA programme or in associated procedures is identified, then the person responsible for the function found to be deficient takes the necessary corrective action. This corrective action should be approved by the person responsible for the QA programme for the PSA project. The person responsible for ensuring that corrective actions are agreed and implemented is identified in the appropriate procedure.

3.7. PSA DOCUMENT AND INFORMATION CONTROL

3.7.1. General considerations

The objective of this process is to control and document all the steps of the work.

A large amount of information is available as of the start of the project. This information must be quality assured and well documented. This information typically includes:

- Project scope, definition and objectives
- Input data
- Pre-performed analyses and calculations to be used for the PSA (deterministic analysis, success criteria, etc.).

During the actual work, information control covers items such as:

- Documentation of assumptions
- Data file control
- Consistency of data used during the work

- Traceability of the sources for information and data used in the different tasks
- Access to relevant information for all parties involved in the project (internal interfaces)
- Controlled documentation on changes, updating, new assumptions that lead to iterations in the work process.

Management of information control needs to be organized in such a way as to support iterations in the work process.

The outcome of the work can be intermediate or final. All results should be properly quality assured. The outcome consists typically of:

- The PSA report(s)
- The PSA model with all the corresponding data files.

The PSA analysis and calculations should be documented following processes equivalent to those described in Ref. [1]. Special attention should be paid to the detailed documentation of input data from outside the PSA project and the detailed documentation of all assumptions, criteria and calculations, including exclusion criteria or screening analyses, performed during the development of the model.

3.7.2. Source information control

The fundamental source of data for the PSA is the information from the plant. This means that a system should be in place to assure that all the information needed for the PSA is received or made available to the PSA team (see Ref. [2], Tables III and XIII for lists of typical documents handled in the PSA). When the information is actually transmitted to the PSA team a control covering the documentation received should be in place. Whenever information is used which is only available at the plant, appropriate measures should be taken to assure that the actual documents used are identifiable.

For consistency of the PSA models it is convenient that plant design and operating documentation represent a picture of the plant at a frozen date, e.g. startup, 7th refuelling outage, etc.

3.7.3. Work control

Control of information and documents developed during the project process needs to be subject to appropriate QA.

Regular updating of the PSA has to be subject to a QA programme equivalent to the one applied during the development phase. This updating should not be mingled with PSA simulations or variants performed as part of the PSA applications: documentation which does not correspond to the configuration date selected for the PSA should be clearly identified and segregated. When many exceptions to a specified plant configuration date are permitted, it is recommended that a system be in place to identify them. For PSA updates, new information should be screened to determine its PSA relevance.

PSA models can be subject to iteration processes due to the following:

- Identification of errors or mistakes
- Refinement of assumptions, criteria or availability of additional input data
- Revision of input data (e. g. plant procedures, plant design, etc.) or further refinement after obtaining preliminary PSA results.

The impact of these iterations on PSA models should be documented with the same level of detail as the preliminary analysis and calculation and should be subject to the configuration management requirements established in the PSA project.

Computer data files, e.g. event and fault trees, reliability data, etc. used for calculating PSA results should be subject to a review process equivalent to that applied to PSA reports; the modifications should be subject to the same configuration management requirements and controls that are applied to other PSA reports.

3.8. CONFIGURATION MANAGEMENT

3.8.1. General

The purpose of PSA model configuration management is to ensure that any change in a part of the model is reflected in an appropriate manner in all other associated PSA parts.

Configuration management is applied to PSA information and its documentation throughout the whole life-cycle to ensure that the models, data, specifications, verification evidence, documentation, and software used are all mutually identified and at a known status.

The status is usually defined by allocating issue/revision/version identifiers and a date and time stamp.

3.8.2. Identification, labelling, cataloguing

A project should establish controls and procedures to ensure that all versions of the information are accurately identified. Controls should also be established to record any change in the configuration status of PSA information. Mechanisms should be provided to assign and track the identification of the models, data and documentation, including their revision. An authorized signature list should be in place for released documentation. Logs and records should be maintained relating to the distribution, inventory, configuration control and status accounting for all received and deliverable items.

3.8.3. Documentation

Documentation for PSA related information should be subject to configuration management procedures. Provisions should be made for informing all PSA project team members of the latest changes in the PSA information. This includes documentation such as software user manuals, procedures for the development of models (e.g. event trees, fault trees), the coding system for input data, fault tree and event tree attributes, or any other documents, including the software codes and interfaces whenever changes are made. An effective way of implementing the distribution of documentation is to maintain an on-line system for documentation. It is the user's responsibility to access the on-line documentation whenever he is using the computerized PSA information in order to determine that he indeed does have the

latest documentation. An appropriate notification procedure may be implemented on-line to alert users to the fact that the documentation has been modified or updated.

The control of new versions of the PSA model, i.e. event and fault trees, the reliability database, the results of the quantification and supporting information should follow procedures similar to those mentioned above for the documentation of PSA related information. It is beneficial to use appropriate tools to stamp new versions in order to identify where the models or related information have been modified or updated.

3.8.4. Identification of configuration

All project information is required to be identified and identifiable. All identified information should also be subject to status control.

All software and electronically stored information should be subjected to configuration control. The purpose of each item, e.g. master copy, archive, should be recorded, together with the date generated, in the description of the item. A baseline status should be established which uniquely identifies all the items and all changes should be recorded and incorporated in an updated baseline.

3.9. MEDIA AND SERVICES CONTROL

For storage control, reference should be made to Ref. [1] and to Section 5.3. of the manual on QA for computer software related to the safety of nuclear power plants [4].

4. PERFORMANCE

A carefully developed PSA project plan represents a key management tool for the performance of a PSA (Ref. [2], Section 2). The PSA project plan contains concise descriptions of the project philosophy (e.g. reasons for performing the study), assumptions regarding intended applications, objectives, scope of work, technical approach, review and verification programme, cost estimate, schedule, work breakdown structure, organization and staffing, and project communications.

A PSA project is comprised of several individual tasks of different analytical activities. The relationship between tasks and the inputs and outputs of each task is described through a task flow structure. In the PSA project plan the overall PSA project is divided into several interrelated work tasks. For a typical list of tasks and task flow structures see for example Refs. [2, 3].

QA of the overall PSA work should be accomplished through QA of the task flow structure and of the individual and integrated work products. Each task is supported by a task plan and corresponding task instructions which identify the data and information input, technical approach with analysis techniques and methods and task output. The form and content of the output are described in the task instructions. The task instructions also interrelate the information flow between tasks and ensure that the task output is suitable for input to other designated tasks; this requires the adequate definition of interfaces.

The basis for QA of a PSA project derives from (a) QA of the task inputs (i.e. technical basis), (b) QA of the task performance, and (c) QA of the task output at the completion of the task. QA for each task will entail:

- Verification of compliance with the task instruction;
- Verification of the technical accuracy of results;
- Compliance with the required form and content for input to other tasks.

Appendix III contains, by way of example, a typical technical work instruction for system analysis for the performance of a Level 1 PSA.

4.1. USE OF VERIFIED INPUTS

QA must not only embrace the work activities of the PSA, but must necessarily control the quality of the information input for each task. Information input will come from either the output of other tasks, or from outside the PSA project. For the former, the QA of the previous tasks will ensure the quality of the input. For the latter, additional steps must be taken to ensure the quality of outside information. Examples of information inputs from outside the PSA are:

- Plant design and operational data;
- Thermal-hydraulic or core analysis;
- Plant operating and emergency procedures;
- Component failure data from other sources;
- Compilations of operational data;
- Information from other PSAs.

QA of information inputs requires that either (a) the information be subject to a QA process prior to being released for use, or (b) that information extracted from a recognized, published source be evaluated for applicability to the specific PSA. In the event that desired data does not meet either of these requirements, the quality of the data must be established by some means satisfactory to the project prior to its use in the PSA.

4.2. USE OF VERIFIED COMPUTER CODES

A number of computer codes and software packages are currently used for performing a PSA. Typically, an integrated software package is used in the Level 1 PSA analyses for the development and storage of system models, sequence models, failure data, and sequence quantification. Additionally, other computer codes may be used for the development of success criteria. Level 2 and Level 3 PSA analyses will also require the use of large computer codes. Finally, smaller pieces of software may be used for special analyses, conversion or transport of data. Increasingly, integrated software packages are developed and used, covering almost all levels and tasks of a PSA.

In order to ensure QA for the PSA, all computer codes used in the development of the PSA must be verified and validated, either in the course of their development or by the PSA group. Computer codes that are purchased commercially may be verified and validated by the code developer. For software that is not commercially procured but, for example, written internally in the PSA organization, a verification, validation and QA process should be performed. QA for computer software is described in Ref. [4].

4.3. VERIFICATION AND VALIDATION OF ANALYTICAL WORK PRODUCTS

A number of items in PSA analyses can be verified and validated. Verification entails ensuring that all input data have been properly selected and incorporated and that calculations are correct. Validation serves to examine how well models describe the system or plant behaviour. For example, a safety system failure model is usually based on a simplified model of the safety system. The simplified system model is intended to condense all essential design and operational information necessary for the failure model. The translation of the simplified system model into the system failure model can be verified, for example, with regard to coherence with the system analysis task procedures and rules. The failure model can also be validated, to a certain extent, in terms of the model's capability to reflect the system's failure behaviour in a manner sufficiently realistic bearing in mind the accident sequences for which system actuation is required and the context in which the specific system model is used in the overall model. However, validation to find out how well a system model reflects the real system is challenging. An appreciation of this kind of quality can best be developed through reviews by experienced experts. Therefore, reviews are crucial for assessing the PSA work (see Ref. [5]).

The QA programme should define appropriate means for verification and validation of each work product. Examples of requirements for verification and validation to be included in a QA programme are:

- The computer code for quantification is being used properly;
- Labelling of events is consistent and correct;
- The data sets for the computer code are complete, accurate and consistent;
- House events (flags, switches) are defined and set properly for all sequences;
- Assumptions, simplifications and exclusions.

Persons appointed for verification and validation should be individuals competent in the area to be verified and validated and who did not perform the original work. Verification and validation should be performed in accordance with a pre-established plan. Each output of each task should be checked in the most appropriate manner prior to being released for use in other tasks. Whenever possible, the intermediate results should also be considered in the verification and validation process.

4.4. PSA REVIEWS

A comprehensive review process accompanying the PSA project is essential for a quality PSA. Different types of reviews are carried out to consider the PSA model and results in an adequate way. Reviews can either be specialized to concentrate on details and individual models, or they can consider the broad aspects and overall results of the PSA. Their degree of formalization extends from informal, when they are carried out by the analyst on his own, to formalized high level peer reviews. For illustrative purposes, the reviews accompanying system analysis are described in Appendix III.

QA tasks and technical work aspects are intimately connected in PSA. Therefore, it is preferable in most cases that the reviews should cover both aspects. Regarding QA aspects, two types of reviews must be carried out. The first type of review certifies the suitability of the task instruction to produce the desired results, while the second certifies the level of compliance with the instruction and technical accuracy. Reviews by external experts can also be included at all levels in the review process.

4.5. PSA CHANGE CONTROL

Changes in PSA models, data, information and results, including changes to requirements, scope, 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 for carrying out the complete PSA. If appropriate, this effort can be limited to those parts and aspects of the PSA which are affected. Activities which should be performed include:

- PSA information control;
- PSA configuration control;
- PSA documentation control;
- Verification and validation;
- Review.

Depending on the type of changes, a new version or an update of the previous PSA 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.

4.6. PSA OUTPUTS

PSA outputs should be produced following the description given in the Level 1 PSA procedures (Ref. [2], Section 7).

5. ASSESSMENT

Reference should be made to Ref. [1], which describes the approach for self-assessment and independent assessment of the performance of the QA programme including organizational details. Measures should be in place for evaluating the PSA work in relation to the following characteristics:

- Completeness;
- Consistency;
- Accuracy;
- Document control;
- Configuration control.

This evaluation includes reviews at various levels and stages of the work performed. The activities should also include details of the QA of the software used in the PSA if necessary. It should include procedures for verification, documentation, and control of the software, whether procured from an external source or developed within the organization. These procedures will apply to both the computer programs used in the analysis and the models and data stored in electronic form.

REFERENCES

[1] 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).

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

[3] 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).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for Computer Software related to the Safety of Nuclear Power Plants, Technical Reports Series No. 282, IAEA, Vienna (1988).

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

Appendix I

TYPICAL DOCUMENTS FOR A PSA PROJECT QUALITY ASSURANCE PROGRAMME

A.1. QA programme description

- Quality assurance programme description
- Interfaces with other QA programmes.

A.2. Management documents

- Procedure for PSA information configuration management
- Procedures for control of organization, functional responsibilities, resources and job descriptions
- Procedure for document control
- Procedure for organizing and conducting internal and external reviews
- Procedure for handling interfaces
- Training framework
- Procedure for handling plant information.

A.3. Working documents

- Procedures for task specification
- Procedures for development of plans and schedules
- Procedures for review of all tasks
- Procedure for initiating event analysis (13, 17, 24)*
- Procedure for sequence analysis and development of event trees (14, 15, 16, 18)*
- Procedure for system analysis and development of fault trees (19)*
- Procedures for handling dependencies and common cause failures (21, 25b)*
- Procedure on human reliability assessment (20, 26)*
- Procedure for data collection, analysis, checking and computer input (25)*
- Procedure for fault tree and event tree integration and quantification (27, 28, 29)*
- Procedure for uncertainty and sensitivity analyses (30, 31)*
- Procedure for display and interpretation of results (32, 33, 34).*

* Task numbers in accordance with the IAEA Level 1 PSA procedures, Safety Series No. 50-P-4.

Similar procedures should to be established for Level 2, Level 3, external events and low power and shutdown PSA.

Appendix II

OUTLINE OF A PSA PROJECT PLAN

PROJECT OBJECTIVES

Contains a short and concise description of the objectives of the PSA project, a description of user requirements and expectations, and a description of the intended safety related applications of the PSA.

REGULATORY REQUIREMENTS AND APPLICABLE TECHNICAL STANDARDS

In a number of Member States regulatory requirements on PSA and its applications are in place which should be outlined. Other applicable standards should also be described under this item.

SCOPE

Contains a short and concise description of the context and extent of the work in the PSA project, including all agreed and identified exclusions from the scope.

CLIENTS

Identifies the recipients and users of the PSA project.

QUALITY ASSURANCE PROGRAMME

Describes the context and extent of the QA programme for the PSA project. Explicit references are made to the overall QA programme applicable to the project and to the specific QA programme documents for the PSA project.

The PSA project plan itself is subjected to QA. It should be ensured that the PSA project plan is reviewed and approved.

PSA PROJECT WORK PROCESS

A detailed delineation of the main steps and tasks of the PSA project. Explicit references to detailed task plans should be made. It should include scheduled evaluations, reviews and assessments, presentation of interim and final results.

If applicable there should be a description of unusual features, unusual techniques, special tools and the way these will be handled.

SCHEDULE AND MILESTONES

A schedule for the main steps and tasks of the PSA project. The main steps and tasks correspond to the ones described in the section entitled "PSA project process". Milestones should be given for these steps and tasks, and dependencies between steps and tasks should be clearly outlined. Special care needs to be devoted to steps and tasks which require an iterative process with other tasks. It should also include hold points for reviews.

PROJECT INTERFACES

Description of project interfaces with groups, organizations or projects not explicitly integrated within the PSA project. Examples are the interface with a permanently established group at the plant collecting and evaluating plant specific reliability data or work subcontracted to an external institution, e.g. thermal-hydraulic analyses.

PROJECT DELIVERABLES

Description of the reports, scope of the reports and relationship between the reports and the requirements of the identified recipients. Description of the computerized models, results and other information together with the main steps and tasks, as delineated in the section on the PSA project work process.

RESOURCE ALLOCATION

Describes the duration of work and how resources will be planned and allocated. This includes staff, budgets and equipment. There should be a description of facilities for carrying out the work and of required modifications or upgrades. There should also be a description of how support and technical personnel with the necessary experience and skill will be assigned to perform the work.

REFERENCES

List of references cited in the PSA project plan.

Appendix III

TECHNICAL INSTRUCTIONS SAMPLE FOR SYSTEM ANALYSIS

Important note: *The purpose of this example is not to describe the technical state of the art of system analysis or to prescribe a particular PSA approach, as technical methods evolve constantly, but rather , to show the level of detail and the kind of controls implemented in the task process.*

CONTENTS

1. PURPOSE

1.1. INTRODUCTION

System analysis determines the unavailability and unreliability of systems which are required during an accident sequence. It interfaces with the following PSA tasks:

- Sequence analysis and development of event trees, which delivers the conditions and requirements for the systems considered in system analysis.
- Reliability data compilation and evaluation, which inputs the reliability parameters for components and equipment to system analysis.
- Human reliability analysis, which contributes reliability assessments for human interactions to be considered in system analysis.
- Fault tree and event tree integration and quantification, which integrates the overall PSA model.

The main tool for system analysis is the fault tree technique, a deductive failure analysis which focuses on one particular undesired event (failure of a system to meet requirements) and which provides a method for determining causes for this event. Because of the interfaces with other PSA tasks, the work in system analysis is highly iterative and requires revisions of system analyses. Therefore, adherence to work instructions and document and version control are crucial for this task.

1.2. OBJECTIVES

The purposes of these technical instructions are as follows:

(1) To specify an adequate set of procedures for the documentation, preparation, review and approval phases of system analysis;

(2) To specify an acceptable methodology for the development of system analysis;

(3) To specify the procedures and formats for the control of documentation in system analysis;

(4) To identify the individuals and groups involved in the development of system analysis.

2. SCOPE

These technical instructions apply to all system analyses prepared in the framework of the PSA, except initiating event analyses, which are governed by a special procedure.

3. REFERENCE DOCUMENTS

References covering quality assurance procedures, project documents and work instructions.

4. RESPONSIBILITIES

4.1. SYSTEM ANALYST

The system analyst:

- Identifies the document sources which contain the information needed for the analysis;
- Prepares and/or revises the system analyses, for the assigned systems, in accordance with the established work schedule;
- Is responsible for maintaining an adequate notebook and working documentation for her/his analyses;
- Is responsible for the accuracy of the system analyses and signs the cover sheet of the system analysis report.

4.2. SYSTEM ANALYSIS TASK LEADER

The system analysis task leader:

- Identifies the kind of documents to be used for system analysis;
- Assigns system analysts to prepare the system analyses;
- Prepares a work schedule for system analysis development and co-ordinates the development process in accordance with this schedule;
- Verifies the performance and accuracy of each step of system analysis development during review stages;
- Ensures the interface with other PSA tasks in order to solve problems which can occur during system analysis development;
- Ensures correctness of system analyses in terms of PSA modelling, especially with respect to "as built" or "as frozen" design;
- Ensures that the characteristics of system operation which have been credited in the system analysis for the PSA reflect the actual practices and conditions in the plant;
- Is responsible for the accuracy of the system analyses and signs as reviewer the cover sheet of the system analysis report;
- Is responsible for the controlled versions of the computerized system analysis models;
- follows up the proper actions to ensure approval of the system analyses;
- Is responsible for maintaining and updating of the procedure for system analysis;
- Is responsible for the implementation and effectiveness of the procedure for system analysis.

4.3. PSA PROJECT MANAGER

The PSA project manager:

- Is responsible for the acquisition of the necessary documents;
- Is responsible for ensuring the interface with other PSA tasks;
- Reviews and verifies the correctness of the study from an overall PSA point of view;
- Is responsible for the correctness of system analyses regarding PSA modelling with respect to "as built" or "as frozen" design, organizes review in a formalized way by design engineers;

- is responsible that the characteristics of system operation which have been credited in the system analysis for the PSA reflect the actual practices and conditions in the plant, organizes review in a formalized way by operation engineers;
- Reviews and approves system analyses, signs the cover sheet indicating approval of the system analysis report;
- Approves updating of the procedure for system analysis.

4.4. DOCUMENT CONTROL MANAGER

The document control manager:

- Distributes copies of system analysis reports in conformity with the established distribution list;
- Archives all originals and maintains a list of all system analysis reports with their revision number.

5. PROCEDURE

5.1. JUSTIFICATION AND AUTHORIZATION

System analyses are prepared as part of and in support of the overall PSA. Preparation or revision of system analyses are authorized by the PSA project manager.

5.2. ORGANIZATION OF THE REPORT

The system analysis report is a controlled document. It is issued in a standard format as follows:

Cover sheet
Review transmittal sheet

Chapter I. Purpose

Chapter II. System description

- II.1. General description
- II.2. Design description
- II.3. Operation description

Chapter III. Fault tree development

- III.1. Systems success/failure criteria
- III.2. Operational conditions
- III.3. Support and supply systems interface, system boundaries as specified for the PSA model
- III.4. Human reliability aspects important for systems analysis
- III.5. Test, surveillance and maintenance practices, requirements and procedures
- III.6. Technical specifications
- III.7. Fault tree modelling assumptions

III.8. HRA models and data
III.9. Fault tree models and reliability models for components
III.10. House events or switches used and related scenarios (if applicable)
III.11. Potential dependent failures, models and data

Chapter IV. System fault tree evaluation and quantification

IV.1. Reliability parameters, data sources and operating experience, including uncertainty data (if applicable)
IV.2. Qualitative and quantitative evaluation, minimal cut-sets, system level importances

Chapter V. Interpretation, insights and conclusions

Chapter VI. References

List of all documents used for the development of the study with their revision date and number including appraisals for their applicability and actuality.

Appendix A — System drawings
Appendix B — Fault tree plot
Appendix C — Reliability data table, including human interactions data
Appendix D — Tables of results, cut-sets, importances

5.3. PERFORMANCE OF SYSTEM ANALYSIS

The development of the system analyses follows the steps listed below:

5.3.1. Procurement of system documentation

Procurement of system documentation and information (design documents, operating documents, safety documentation, system design diagrams, electrical diagrams, instrumentation and control diagrams, equipment information, layout drawings, plant walk-downs, interviews with staff from the plant and manufacturers if necessary).

The system analyst maintains an up-to-date list of relevant design, operational and safety documentation which must include the document number, title and current revision numbers as a minimum requirement. Access to, and review of, these documents is necessary for performing the analysis. As far as characterized by "as built" or "as frozen" criteria, the document list must be updated during the period of analysis as additional or more recent information is incorporated into the study.

5.3.2. System familiarization

At this stage the analyst becomes familiar with the details of system design and operation. The analyst studies the system documentation and other documents needed for a better understanding of the system. Also, in case of problems, discussions are arranged with system engineers and control room operators. It is important at this point to understand how the system is operated, tested and maintained.

5.3.3. Modelling assumptions

Based on the scenario and the specifications provided by the task group on *"sequence analysis and development of event trees"* and utilizing the system information the system analyst defines the analysis modelling assumptions. At this point the analyst defines the fault trees top event(s) and the characteristics and conditions for the system. This step requires frequent interactions with the task group on *"sequence analysis and development of event trees"*. System dependencies and the connections to supply and support systems are identified and documented. A review is performed of available system models for supply and support systems.

5.3.4. First stage review

A progress review is conducted by the system analysis task leader when activities 5.3.1 to 5.3.3 have been completed. At that stage, the scope, the failure criteria and the pertinent system boundaries have been documented by the system analyst. Approval of this work by the system analysis task leader is required before the system analyst may proceed with the remaining activities. The level of resolution for the study is also considered during the review.

It has to be pointed out that continuous interaction with the task group on *"sequence analysis and development of event trees"* and other task groups is necessary during system analysis. These interactions, however, do not replace the staged reviews.

5.3.5. Fault tree development and evaluation

The system analyst develops a first fault tree logic model according to the "fault tree guide", see Annex A. This includes the identification and modelling of explicit and implicit dependencies and human interactions. Models of implicit dependencies (common cause failures, CCF) and for human interactions can be simple at this stage for later refinement after screening. Qualitative screening, which must be documented, can be used to limit the number of CCF events and human interactions introduced in the model.

The analyst identifies the data needs and inputs screening values into the reliability models. The preliminary system model is then evaluated and checked with the software tool used for the project. Checking includes logical correctness, completeness and determining whether design and operational features are adequately depicted by the model.

Input of operational parameters is expedited by direct liaison between the system analyst and appropriate plant personnel wherever practicable. The system analysis task leader takes steps to ensure that as many of the operational preferences and constraints as possible are transmitted to the system analyst during the modelling period.

In order to evaluate system unavailability, the system analyst selects together with the task group on *"reliability data compilation and evaluation"* the appropriate quantitative reliability data. A comprehensive cross-reference between the system components included in the model, the selected reliability data and the original data sources is established and maintained. The interface with the task group on *"reliability data compilation and evaluation"* is described in a separate procedure.

The selected reliability data is applied to the fault tree events of the model, and analytical evaluations of the model are carried out with the software tool used for the project. The

evaluations include qualitative and quantitative analysis, minimal cut-sets, and system level importances and interpretation. Finally the system analyst performs the interpretation and prepares insights and conclusions and the draft report.

5.3.6. Second stage review, review of the draft report

A second progress review is performed by the system analysis task leader, or his delegate, when the activity 5.3.5 has been completed, to confirm that the model is an acceptable representation of the system and of the requirements given by the task group *"sequence analysis and development of event trees"*. The review also has to ensure, to the extent practicable, that the set of quantitative data used in the study is internally consistent and appropriate. This review also serves to confirm that the intended objectives and scope of the study have been properly addressed.

The draft report is reviewed by the system analysis task leader, or his delegate, for acceptability of the document for distribution to other appropriate reviewers. The PSA project leader reviews and verifies the correctness of the system analysis draft report from an overall PSA point of view. He co-ordinates the review of the draft report by persons whose input is considered appropriate to ensure that system operational practices and characteristics have been adequately taken into account in the report. The review process is accompanied by a formal review transmittal sheet. An external review by independent reviewers can be organized at this point.

Before the draft report is distributed, the review has to ensure that the evaluation and interpretation of the model is consistent and appropriate.

5.3.7. Preparation of the final report

The system analyst and the system analysis task leader review all comments received on the draft report. The system analyst resolves any conflicting comments and modifies the draft report accordingly. Whenever extensive modification of the draft report is required, follow-up actions may include redistribution of the revised draft report for an additional round, at the discretion of the system analysis task leader. Any reissue of the draft report must bear a unique dating information and clearly indicate the immediately previous issue from which it was derived. If changes require alterations of the controlled version of the computerized fault tree model, an updated version is produced with a new identification stamp and the system analyst notifies the system analysis task leader.

When the system analyst is satisfied that his work meets the requirements laid down for it, he forwards his study as a draft final report to the system analysis task leader.

5.4. APPROVAL PROCESS

When the draft report of the system analysis is acceptable to the system analysis task leader, then it is forwarded to the PSA project leader for formal approval.

5.5. REVISIONS AND CANCELLATIONS

5.5.1. Revisions

Revision of an existing system analysis study is undertaken to support changes in the PSA model or changes in the plant. Revision to an existing system analysis is undertaken either in part or in whole when required. A formalized and controlled procedure for total or partial revision needs to be followed. Document control handles revisions the same way as new studies are handled.

5.5.2. Cancellations

A form announcing the cancellation of any earlier issue and identifying its successor is sent to all listed recipients of a superseded document.

5.6. DISTRIBUTION

Formal transmittals of system analysis are accompanied by a completed copy of a distribution form. The original of each study is sent to document control for retention. Each study performed is numbered according to a centralized numbering system. A cover page containing the title of the report/study, author, reviewer and approval, along with the report number, revision number and date of issue is added to the front of the document.

Annex A

FAULT TREE GUIDE, EXAMPLE OF CONTENTS

CONTENTS

4. SYSTEM DEFINITION

4.1. Limit of resolution (internal boundary)
4.2. Interfaces (external boundary)
4.2.1. Control systems
4.2.2. Electrical systems
4.2.3. Water systems
4.2.4. Air systems

5. RULES AND PROCEDURES

5.1. Fault tree procedure
5.2. Fault tree modelling considerations
5.3. Fault tree event labelling scheme
5.3.1. Alphanumeric conventions
5.3.2. Intermediate (Gate) events
5.3.3. Basic events
5.3.4. Undeveloped events
5.3.5. External (House) events
5.3.6. Conditioning events
5.3.7. Developed events (Double Diamond Events)
5.4. Special labelling considerations
5.5. Rules on time durations required in fault trees
5.6. Modelling common cause or hostile environment induced failures

6. EVALUATION OF HUMAN INTERACTIONS

6.1. Types of human interactions
6.2. Guidelines for the inclusion of human interactions in fault trees
6.3. Documentation

7. DATA ASSIGNMENT

7.1. Sources of component reliability data
7.2. Data assignment software
7.3. Treatment of dominant contributors

8. FAULT TREE EVALUATION

8.1. General
8.2. Information required for fault tree evaluation
8.3. Evaluation process
8.4. Fault tree drafting
8.5. Review of fault tree analysis results

9. INFORMATION SOURCES AND USAGE

9.1. System information
9.2. Quantitative reliability data

CONTRIBUTORS TO DRAFTING AND REVIEW

Bertucio, R.	Scientech, Inc., United States of America
Boiadjiev, A.	Risk Engineering Ltd, Bulgaria
Carretero, J.A.	Empresarios Agrupados A.I.E, Spain
Cuallado, G.	IBERDROLA Ingeniería y Consultoría, Spain
Facer, R.I.	EQE International Limited, United Kingdom
Georgescu, G.S.	Centre of Technology and Engineering for Nuclear Projects, Romania
Gubler, R.	International Atomic Energy Agency
Horne, B.	Electrowatt Engineering (UK) Ltd, United Kingdom
Ingemarson, J.G.I.	Barsebäck Kraft AB, Sweden
Lydell, B.	RSA Technologies, United States of America
Mladý, O	Temelin NPP, Czech Republic
Mohammadi Tochaie, M.T.	Atomic Energy Organization of Iran (AEOI), Islamic Republic of Iran
Nielsen L.	Norwegian Petroleum Directorate, Norway
Rodríguez A.	Comisión Nacional de Seguridad Nuclear y Salvaguardias (CNSNS), Mexico
Rösli B.	Kernkraftwerk Leibstadt AG, Switzerland
Šuránsky L.	Mochovce NPP, Slovak Republic

Consultants Meetings

Vienna, Austria: 10–14 June 1996, 14–18 April 1997

Technical Committee Meeting

Madrid, Spain: 23–27 February 1998