CATEGORIES IN THE IAEA SAFETY SERIES

A new hierarchical categorization scheme has been introduced, according to which the publications in the IAEA Safety Series are grouped as follows:

Safety Fundamentals (silver cover)

Basic objectives, concepts and principles to ensure safety.

Safety Standards (red cover)

Basic requirements which must be satisfied to ensure safety for particular activities or application areas.

Safety Guides (green cover)

Recommendations, on the basis of international experience, relating to the fulfilment of basic requirements.

Safety Practices (blue cover)

Practical examples and detailed methods which can be used for the application of Safety Standards or Safety Guides.

Safety Fundamentals and Safety Standards are issued with the approval of the IAEA Board of Governors; Safety Guides and Safety Practices are issued under the authority of the Director General of the IAEA.

An additional category, Safety Reports (purple cover), comprises independent reports of expert groups on safety matters, including the development of new principles, advanced concepts and major issues and events. These reports are issued under the authority of the Director General of the IAEA.

There are other publications of the IAEA which also contain information important to safety, in particular in the Proceedings Series (papers presented at symposia and conferences), the Technical Reports Series (emphasis on technological aspects) and the IAEA-TECDOC Series (information usually in a preliminary form).
PROCEDURES FOR CONDUCTING
PROBABILISTIC SAFETY
ASSESSMENTS OF
NUCLEAR POWER PLANTS
(LEVEL 1)

A Safety Practice
The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ARGENTINA
AUSTRALIA
AUSTRIA
BANGLADESH
BELARUS
BELGIUM
BOLIVIA
BRAZIL
BULGARIA
CAMBODIA
CAMEROON
CANADA
CHILE
CHINA
COLOMBIA
COSTA RICA
COTE D'IVOIRE
CUBA
CYPRUS
CZECHOSLOVAKIA
DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LUXEMBOURG
MADAGASCAR
MALAYSIA
Mali
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SIERRA LEONE
SINGAPORE
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
THAILAND
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
VENEZUELA
VIET NAM
YUGOSLAVIA
ZAIRE
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is “to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world”.

© IAEA, 1992

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria
July 1992
SAFETY SERIES No. 50-P-4

PROCEDURES FOR CONDUCTING PROBABILISTIC SAFETY ASSESSMENTS OF NUCLEAR POWER PLANTS (LEVEL 1)

A Safety Practice

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1992
VIC Library Cataloguing in Publication Data


p. ; 24 cm. — (Safety series, ISSN 0074-1892 ; 50-P-4)

STI/PUB/888

ISBN 92-0-102392-8

Includes bibliographical references.


VICL 92-00024
FOREWORD

Probabilistic safety assessment (PSA) is increasingly important in the safe design and operation of nuclear power plants. The activities of the International Atomic Energy Agency in this area are focused on facilitating the use of PSA by reviewing the techniques developed in Member States, assisting in the formulation of procedures and helping Member States to apply such procedures to enhance the safety of nuclear power plants.

In this context a set of publications is being prepared to establish a consistent framework for conducting a PSA and forms of documentation that would facilitate the review and utilization of the results. Since December 1986 several Advisory Group meetings, Technical Committee meetings and Consultants meetings have been convened by the IAEA in order to prepare the publications.

The lead publication for this set establishes the role of PSA and probabilistic safety criteria in nuclear power plant safety. Other publications present procedures for the conduct of PSA in nuclear power plants and recognized practices for specific areas of PSA, such as the analysis of common cause failures, human errors and external hazards and collection and analysis of reliability data.

The publications are intended to assist technical persons performing or managing PSAs. They often refer to the existing PSA literature, which should be consulted for more specific information on the modelling details. Therefore, only those technical areas deemed to be less well documented in the literature have been expanded upon. The publications do not prescribe particular methods but they describe the advantages and limitations of various methods and indicate the ones most widely used to date. However, they are not intended to discourage the use of new or alternative methods; in fact the advancement of all methods that achieve the objectives of PSA is encouraged.

The IAEA wishes to convey its thanks to all those who participated in the drafting and review of the publication, in particular I.A. Papazoglou of the National Centre for Scientific Research Demokritos of Greece, who was the principal contributor.
EDITORIAL NOTE

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

1. INTRODUCTION ........................................................................................................ 1

   1.1. Background ........................................................................................................ 1
   1.2. Objective and purpose of the report ................................................................. 2
   1.3. Scope of the report ........................................................................................... 2
   1.4. Structure of the report ....................................................................................... 3

2. MANAGEMENT AND ORGANIZATION ................................................................. 6

   2.1. Task 1: Definition of the objectives of the PSA ............................................. 6
   2.2. Task 2: Definition of the scope of the PSA ................................................... 10
   2.3. Task 3: Project management ............................................................................. 13
   2.4. Task 4: Selection of methods and establishment of procedures ................... 16
   2.5. Task 5: Team selection and organization ....................................................... 16
   2.6. Task 6: Training of the team ........................................................................... 18
   2.7. Task 7: Funding and scheduling ..................................................................... 19
   2.8. Task 8: Establishment of a quality assurance programme and interactive peer review ............................................................... 22

3. IDENTIFICATION OF SOURCES OF RADIOACTIVE RELEASES AND ACCIDENT INITIATORS ........................................... 24

   3.1. Task 9: Familiarization with the plant and PSA and information gathering .... 24
   3.2. Task 10: Identification and selection of site sources of radioactive releases .... 27
   3.3. Task 11: Determination and selection of plant operating states .................... 27
   3.4. Task 12: Definition of core damage states or other consequences ................ 27
   3.5. Task 13: Selection of initiating events .............................................................. 28
   3.6. Task 14: Determination of safety functions .................................................... 30
   3.7. Task 15: Assessment of function/system relationships .................................... 32
   3.8. Task 16: Assessment of plant system requirements ........................................ 35
   3.9. Task 17: Grouping of the initiating events ....................................................... 39
This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
1. INTRODUCTION

1.1. BACKGROUND

The first comprehensive application of methods and techniques of probabilistic safety assessment (PSA) dates back to 1975 to the United States Nuclear Regulatory Commission's Reactor Safety Study (WASH-1400) [1]. Since that landmark study, there has been substantial methodological development, and PSA techniques have become a standard tool in safety evaluation of nuclear power plants (NPPs). The main benefit of PSA is to provide insights into plant design, performance and environmental impacts, including the identification of dominant risk contributors and the comparison of options for reducing risk. PSA provides a consistent and integrated model of nuclear power plant safety. Consequently, PSA offers a consistent and integrated framework for safety related decision making. Changes or alternatives in different design and engineering areas in a nuclear power plant can be compared on a common basis, namely the quantitative estimate of risk provided by PSAs. Furthermore, PSA is a conceptual and mathematical tool for deriving numerical estimates of risk for nuclear plants and industrial installations in general. PSA can also quantify the uncertainties in these estimates. PSA methods continue to be developed and improvements will reduce uncertainties; however, present PSA methods are quite capable of providing meaningful numerical results.

PSA differs from traditional deterministic safety analysis in that it provides a methodological approach to identifying accident sequences that can follow from a broad range of initiating events and it includes the systematic and realistic determination of accident frequencies and consequences. A major advantage of PSA is that it allows for the quantification of uncertainties in safety assessments together with the quantification of expert opinion and/or judgement. Finally, PSA has been shown to provide important safety insights in addition to those provided by deterministic analysis.

In international practice three levels of PSA have evolved:

Level 1: The assessment of plant failures leading to the determination of core damage frequency.

Level 2: The assessment of containment response leading, together with Level 1 results, to the determination of containment release frequencies.

Level 3: The assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimates of public risks.

A Level 1 PSA provides insights into design weaknesses and into ways of preventing core damage, which in most cases is the precursor to accidents leading to major radioactive releases with potential health and environmental consequences.
A Level 2 PSA provides additional insight into the relative importances of accident sequences leading to core damage in terms of the severity of the radioactive releases they might cause, and insight into weaknesses in and ways of improving the mitigation and management of core damage accidents. Finally, a Level 3 PSA provides insights into the relative importances of accident prevention and mitigatory measures expressed in terms of the adverse consequences for the health of both plant workers and the public, and the contamination of land, air, water and foodstuffs. In addition, a Level 3 PSA provides insights into the relative effectiveness of aspects of accident management related to emergency response planning.

PSA can provide useful insights and inputs to decisions on (a) design and backfitting; (b) plant operations; (c) safety analysis and research; and (d) regulatory issues. Details on these possible functions of a PSA are given in Section 2.1 of this report.

1.2. OBJECTIVE AND PURPOSE OF THE REPORT

This Safety Practices report provides guidance on conducting a Level 1 PSA for internal events in NPPs. The main emphasis is on procedural steps of the PSA rather than the details of the corresponding methods. The report is intended to assist technical persons managing or performing PSAs. A particular aim is to promote a standardized framework, terminology and form of documentation for PSAs so as to facilitate external review of the results of such studies. The report not only describes methods, but also considers advantages and limitations of alternative approaches and indicates those most widely used to date. The publication of this and other related reports is not intended to pre-empt the use of new or alternative methods; on the contrary, the promotion of all methods of achieving the objectives of PSA is encouraged.

1.3. SCOPE OF THE REPORT

The report provides guidance for conducting a Level 1 PSA; that is, a PSA concerned with events leading to core damage. The scope of this report is confined to internal initiating events (excluding internal fires and floods). No specific guidelines are given for the procedural steps of a PSA for external initiators (e.g. earthquakes, external fires, external floods, heavy winds, etc.). This is by no means a statement of the recommended scope of a Level 1 PSA. On the contrary, a PSA is not complete unless all significant initiators are included. Experience indicates that external hazards should not be excluded as a group, but should be included

---

1 Internal fires and floods as well as external hazards are beyond the scope of this report.
to provide a complete picture of the plant risk. Guidance on the treatment of external events, however, is given in another IAEA publication [2]. The present report refers to issues related to external events only if this is necessary for enhancing the efficiency of the analysis when external events are to be treated in a later phase of the PSA.

While extensive reference is made in this report to existing literature on PSA describing modelling details, some methodological (non-procedural) aspects of PSA are discussed in greater depth than others. These are technical areas that the experts who contributed to this report considered to be less well documented in the literature.

1.4. STRUCTURE OF THE REPORT

This report is divided into sections corresponding to the six major procedural steps for a Level 1 PSA. These are as follows:

Management and organization

This step includes the actions and activities necessary for the organization and management of the study. It includes the definition of the objectives, the scope and the project management scheme of the PSA, the selection of the methods and establishment of procedures, the selection of personnel and the organization of the team that will perform the PSA, the training of the team, the preparation of a PSA project schedule, the estimation and securing of the necessary funds, and the establishment of quality assurance (QA) and peer review procedures.

Identification of sources of radioactive releases and accident initiators

Most aspects of problem definition are included in this step. The potential sources of radioactive releases to the environment are identified, the potential states of the plant to be analysed are determined, and the safety functions incorporated in the plant are identified. The accident initiators that can challenge these functions as well as the systems that serve them are identified. The relationships between initiating events, safety functions and systems are established and categorized. During this step, the analysis team becomes familiar with the plant to be analysed and the methods to be used and collects much of the required information on which to base subsequent analysis.

Accident sequence modelling

The third procedural step deals with the construction of a model that simulates the initiation of an accident and the response of the plant. This model consists mainly
FIG. 1. Major procedural steps of a Level 1 PSA.
of combinations of events that comprise initiating events, possibly some external, system failures and human errors that will lead to the undesirable consequences. These combinations of events are called accident sequences and the objective of this step is to define them. Models for the detailed analysis of system failures and of human errors are developed. A qualitative analysis for inclusion of possible dependences in the models is also performed in this step.

Data assessment and parameter estimation

This procedural step acquires and/or generates all information necessary for quantification of the model that was constructed in the third step. In particular, the fundamental elements of the plant model and the parameters that need to be estimated are identified. The data necessary to produce these estimates and their associated uncertainties are collected and treated appropriately. The parameters that are estimated can be divided into three major categories: frequencies of initiating events, component unavailabilities and human error probabilities. Parameters necessary for the modelling of potential dependences among various events (initiating events, hardware failures or human errors) are also estimated.

Accident sequence quantification

In this step, the model (constructed in the third step) is quantified using the results of the fourth step. The result of this step is the assessment of the frequency of accident sequences. Normally this is accompanied by an assessment of the associated uncertainties. Sensitivity studies are made for the important assumptions and the relative importances of the various contributors to the calculated results are indicated.

Documentation of the analysis: display and interpretation of results

The results of the analysis are thoroughly documented in each step. In this step the results are displayed in the way that best meets the needs of the end users. This includes the interpretation of the results, in line with the objectives of the PSA.

The general flow of work/information among these steps is shown in Fig. 1. It is important to recognize that this flow is not always linear and that there are many iterative loops among the various steps. In turn the procedural steps are divided into tasks which form the framework of the PSA procedures.
2. MANAGEMENT AND ORGANIZATION

In Section 2, the first major procedural step of a PSA, namely the step dealing with the management and organization of the study, is presented and discussed. Although this major step precedes the others in this report and in the actual development of the PSA, it continues for the duration of the study.

There are eight tasks that can be identified as forming the procedural step of 'management and organization'. These tasks are depicted in Fig. 2.

2.1. TASK 1: DEFINITION OF THE OBJECTIVES OF THE PSA

Determination of the objectives of the PSA together with its intended and potential uses is the single most important step in the process of performing a PSA. The objectives and uses of the PSA will determine in turn the scope of the analysis, the necessary procedures and methods, and the personnel, expertise, funding and time required for the analysis, as well as the documentation requirements. Timely and precise decisions on the objectives of the PSA are therefore very important.

2.1.1. General objectives of PSA

Probabilistic safety analysis is one of the most efficient and effective tools to assist decision making for safety and risk management in nuclear power plants. As such, it can have one or more of the following three major objectives:

— to assess the level of safety of the plant and to identify the most effective areas for improvement;
— to assess the level of safety and compare it with explicit or implicit standards;
— to assess the level of safety to assist plant operation.

The first general objective aims at extending and widening the understanding of the important issues that affect the safety of a nuclear power plant. By so doing, design or operational problems can be identified and areas for improvement or future study can be identified. The second objective contains the element of overall adequacy, in that it is deemed desirable to compare the assessed safety related capabilities of a plant against standards. These standards might be explicitly defined (fixed) criteria or implicitly defined criteria, as for example is the case if the comparison is made against existing 'accepted as safe' plants and/or designs. The third general objective aims at providing information that can assist plant operations. For example, this may be in the form of improved technical specifications, models and criteria for monitoring operational reliability, or advice for accident management.
FIG. 2. Procedural tasks in the management and organization of a PSA.
2.1.2. Stages of the plant life-cycle

A PSA can be performed at any stage of the plant life-cycle, namely:

— the plant at conceptual/early design stage;
— the plant at the final design stage;
— the operating plant.

It is generally considered desirable to start the PSA process as early in the plant life-cycle as possible. Design or procedural weaknesses that are recognized early can be corrected or improved less expensively than those that remain until the plant is in operation. While a PSA can be started during any of the given life-cycle stages, it is recommended that the PSA models and documentation be maintained and updated throughout the operating life of the plant to provide continued benefit.

A PSA conducted for any of the given stages can have any combination of the general objectives outlined in subsection 2.1.1. The specific objectives and the intended uses, however, may vary. The specific objectives/uses of PSA are discussed in subsection 2.1.3.

2.1.3. Specific objectives and uses of PSA

Specific objectives and corresponding uses of PSA related to the first general objective of assessing the level of safety of a plant to identify areas for improvement are as follows:

— **Identification of dominant accident sequences.** Those combinations of initiating events and hardware and human failures are identified that can lead with significant frequency to undesirable consequences.

— **Identification of systems, components and human actions important for safety.** Analysis of the results of the PSA, i.e. of the identified accident sequences, leads to the assessment of the relative importances of the various systems, components and operational and maintenance procedures, together with their uncertainties.

— **Assessment of important dependences (system and man–machine).** Important dependences between systems, and between humans and systems, that affect the safety of the plant are assessed. These include common cause initiating events, common cause failures and multiple dependent human errors that decrease the intended degree of redundancy in the plant design and thus the safety of the plant.

— **Identification and evaluation of new safety issues.** As a result of a PSA, important new plant specific safety issues and generic safety issues may be identified. Furthermore, the PSA can be used as a tool for evaluating the relative importance of any new issues as well as the importance of existing safety issues.
— **Analysis of severe accidents.** The results of PSA can help in identifying the important accident sequences that should be considered as ‘design basis’ accidents, and other sequences that lead to ‘beyond design basis’ accidents and which might require further analysis.

— **Decisions on backfitting of generic and plant specific items.** PSAs can be used to quantify the relative importances of specific backfitting options in operating plants. This evaluation can not only rank the possible backfitting options in terms of their potential for increasing safety, but also provide a cost effective way of deciding which modifications should be made.

— **Design modifications.** PSA results for plants at the design stage can be used to evaluate various design modifications. This ‘optimization’ is usually an iterative process.

— **Prioritization of regulations and safety research.** PSA insights can guide in the prioritization of regulatory requirements and/or safety research. The prioritization may be guided by the PSA’s identification of plant features or procedures which affect safety, or of areas of uncertainty in the plant performance or physical process models.

These subobjectives are applicable to all three stages of the plant life cycle. The extent to which they can be met varies, however, with the stage of the plant design, as is discussed further in Section 2.2.

Specific objectives and corresponding uses of PSA related to the second general objective of comparison with some implicitly or explicitly accepted standards are:

— **Comparison with target values.** If target values or probabilistic safety criteria are available, the PSA can be used to compare the performance of the analysed plant against these criteria. The criteria could be either at a high level (e.g. health risk, core damage frequency) or at lower level (e.g. safety function and/or system unavailability or unreliability).

— **Comparison with ‘accepted’ design.** If a design or operating plant has been assessed and accepted as safe, and a PSA has been performed for this design or plant, then the level of safety of another plant can be compared with that of the ‘accepted’ design or plant by means of the results of a PSA. Caution should always be exercised in comparing PSA results as failure to take account of differences in scope and methods can lead to erroneous conclusions.

— **Comparison of ‘alternative’ designs.** PSA can be used to compare alternative design concepts at any stage of the design process, thus providing information for design decisions.

The foregoing uses are applicable to all three life-cycle stages, although with different levels of confidence. It is important to recognize, however, that such comparisons are only meaningful if the assumptions, techniques, models and data used in the different PSAs are compatible.
Specific objectives and corresponding uses of PSA related to the third general objective of assessing plant safety to assist plant operation are:

— *Evaluation of plant technical specifications and limiting conditions of operations.* Technical specifications represent a set of parameters according to which systems should be operated, tested, maintained and repaired. The reliability of these systems depends on most of these parameters. PSAs provide a framework for decisions on appropriate values of these parameters and/or on relevant policies. Where limiting conditions of operation have not been predetermined, the significance of off-normal plant states (for example, with some equipment out of service) can be evaluated with the assistance of PSA results.

— *Prioritization of inspection/testing activities.* PSA results can be used to help prioritize required startup and in-service inspection activities. At the same time, PSA results can be used to determine system or component reliability requirements for performance monitoring for various systems and/or components during operation.

— *Evaluation of operating experience.* Operating experience can be assessed in a systematic way using the PSA results. Implications of trends and ‘near misses’ can be determined. By following a ‘living PSA’ programme, the significance of changes in failure data and operational procedures can be evaluated.

— *Accident management.* Results and associated insights from PSA provide a very effective framework for training operators and developing operational procedures and a rational basis for emergency planning. Associated personnel can also use PSA results for training purposes.

This is not a comprehensive list of potential objectives and corresponding uses of PSA. Examples of additional, more specific objectives and possible uses of PSA are given in a list of important safety issues (as defined by the regulatory body of one Member State) in Ref. [3]. The same reference describes the relation between the resolution of these issues and the methods, tools and results of a PSA.

2.2. TASK 2: DEFINITION OF THE SCOPE OF THE PSA

After defining objectives, the definition of the scope of the PSA study is the second most important element in the management and organization of the PSA.

The scope of a Level 1 PSA can be described mainly in terms of the following parameters:

(i) potential sources of radioactive releases;
(ii) core damage states;
(iii) plant operational states;
(iv) initiating events;
(v) the extent of the analysis of special issues.

The main factors that determine the extent to which these parameters are included in the PSA are:

(i) the objectives and intended uses of the PSA;
(ii) the availability of appropriate information;
(iii) the available resources and expertise.

2.2.1. Parameters describing the scope of a PSA

The first parameter that characterizes the scope of a PSA is the sources of radioactive releases in the plant. The most important sources (applicable to all types of plants) are:

— the reactor core;
— the spent fuel storage pool;
— the spent fuel handling facilities;
— the radioactive waste storage tanks.

A PSA can be performed for any combination of these sources, although historically most PSAs have been confined to the reactor core.

The second parameter that characterizes the scope of a PSA is the core damage states and final consequences to be considered. For a Level 1 PSA, one or more levels of core damage may be considered, although most PSAs for light water reactors (LWRs) define only one level of core damage. In this case, the unique level of core damage is sufficiently severe to breach the reactor vessel boundary. Conservatively, this core damage level is assumed to be reached by any event sequence that is not successfully terminated. (See Section 3.4.)

The third parameter that characterizes the scope of the PSA refers to the operational states of the plant that are considered at the moment the accident is initiated. These states can include:

— nominal full power operation;
— reduced power operation;
— reactor critical, turbine not operating;
— reactor subcritical, primary circuit pressure above the pressure under residual heat removal conditions;
— reactor subcritical, low pressure residual heat removal systems in operation;
— reactor subcritical, main circuit open (for example, for refuelling, steam generator maintenance or primary pump maintenance).

---

2 A formal definition of an operational state is given in the definitions section of Ref. [4].
It should be noted, however, that most PSAs performed to date have considered only one plant operational state, namely that of full power.

The fourth parameter that characterizes the scope of the PSA is the type of initiating events considered. Historically, again, the initiating events have been distinguished as internal to the plant and external to the plant. Internal initiating events include the loss of off-site power and, in recent listings, fires and floods generated inside the plant. The latter were initially classified as external hazards (initiators) together with earthquakes and other severe environmental phenomena.

The final parameter characterizing the scope of the analysis is the extent to which special issues are treated in the PSA. Some of these special issues and corresponding considerations are given in the following:

- **Depth of treatment of human actions.** Use of (conservative) screening or best estimate human error probabilities, extent of inclusion of operator and/or maintenance personnel errors, extent of inclusion of operator recovery and repair actions, extent of treatment of errors of commission.

- **Rigour of dependence analysis.** Search of accident sequences to identify human error dependences, explicit modelling of impacts of environmental conditions associated with specific initiating events, degree of fault tree linking to uncover equipment dependences.

- **Scope of uncertainty and sensitivity analysis.** Sensitivity or uncertainty analyses can be performed qualitatively or quantitatively. For a quantitative approach, the effort needed can depend considerably on the types of uncertainty to be quantified.

- **Time duration of analysis.** Different time periods (mission time) following the initiating events can be considered (such as one day, one week, one month), as necessitated by the impact on important accident sequences and their predicted frequencies. This may influence capability and reliability considerations for systems and components.

### 2.2.2. Factors influencing the scope of a PSA

The following factors should be considered in determining the scope of the PSA:

1. The objectives and the intended uses of the PSA generally set its scope. It is important to note that significant benefits can be obtained from a PSA even if not all parameters identified as characterizing its scope are examined. External initiators ought to be included in the scope if there is a need to compare the plant against 'all sources' probabilistic safety criteria.

2. The second factor influencing the scope of the PSA is the availability of the information required for a particular scope. The availability of information is most often coupled with the 'design stage' of the plant. Thus, for a conceptual
design there is sometimes little or no information on the interface between the nuclear island and the balance of plant equipment. Operational procedures, test and maintenance procedures or other technical specifications may not be available. Furthermore, the site of the plant might not have been determined. Without a specific site, an external event analysis is constrained. At an early design stage, the lack of detailed information on layouts, hardware interfaces and operational procedures often reduces the scope of the analysis of the dependence between systems. The modelling of the man-machine interface will be limited and analysis of events will often be confined to those internally initiated, excluding fires and internal floods. Recovery cannot be modelled in detail. Note that in this context 'recovery' means the recovery from a human error or hardware failure event within the accident sequence. The recovery of the plant to a normal operating state is beyond the scope of a PSA in normal circumstances. As the design stage progresses towards an operating plant, most of these limitations will no longer apply. Thus, for example, at a final design stage, internal fires and floods can be covered in greater detail, as can external hazards.

(3) The availability of expertise and resources constitutes the third factor influencing the scope of a PSA. Frequently, the required resources (including adequate computer resources) and expertise for performing a PSA of a desired scope are not available, necessitating a more limited scope. In such cases a phased approach is frequently adopted, by which the PSA is expanded in scope at a later time.

A PSA is not complete unless all important initiators are included. Experience indicates that external hazards should not be excluded as a group, but must be included to provide a full picture of the plant risk. Of course, certain specific hazards can be eliminated if they are known to be unimportant for the particular site.

In summary, it is essential that, at the outset of the planning of the study, the scope of the PSA is precisely defined. The scope should be compatible with both the objectives of the study and the available resources and information. It is not necessary for achieving significant benefit that the PSA's scope be the widest possible.

2.3. TASK 3: PROJECT MANAGEMENT

The PSA management scheme strongly depends on the specific conditions in a country, namely:

— organizations participating in the PSA project;
— type and extent of the involvement of the participating organizations;
— objectives and scope of the PSA study.
A PSA study is normally commissioned by one of the following:

— the plant designer;
— the utility;
— the regulatory body.

The PSA can be performed by these groups or by consultants, research institutes, universities, or a combination of these. In any case, the utility should always participate as a source of operational knowledge as well as a beneficiary from the insights obtained.

If the responsibility for technical management is assigned to a single institution, a straightforward management hierarchy is possible. A project manager is assigned direct control of all activities. The project manager in turn is responsible to the appropriate point in the line structure of the institution or to a management co-ordinating group established for this purpose. In this scheme the general technical management of the organization assigns and co-ordinates the subtasks.

If a number of institutions are involved, a co-ordinating group of representatives of these organizations and the project and technical managers of the PSA study should be designated. A higher level Supervisory Committee can be established if necessary.

**Supervisory Committee**

The Supervisory Committee (SC) is composed of senior representatives of the participating institutions and can be responsible for:

— establishing the policies for the programme;
— approving the programme plan;
— approving programme changes;
— securing the necessary economic and technical means to carry on the programme;
— nominating a project co-ordination group which includes the administrative and technical project managers;
— delegating authority to the project co-ordination group;
— monitoring the development of the project;
— approving the final project report.

**Co-ordination Group**

The Co-ordination Group (CG) consists of the project and technical managers of the technical team as well as working level representatives of some or all of the
participating institutions. It reports directly to the SC, is chaired by the project manager and has the following responsibilities:

- to establish and submit for approval to the SC the plans for project implementation;
- to propose and submit for approval to the SC changes in the programme plan;
- to recruit and train technical staff for the project;
- to keep the SC informed about the progress of the project;
- to promote working meetings with the technical staff with the objectives of:
  - maintaining continuity of the project
  - verifying accordance with specified project objectives and scope
  - verifying the progress of individual tasks
  - identifying logistical and personnel needs for the project
  - identifying the need for advisory services
  - submitting the partial and final reports to the SC.

The specific responsibilities of the technical manager are:

- to develop the format of the report;
- to ensure that the technical quality of the work is high;
- to approve the use of methods, models and procedures;
- to promote the development of alternative methods, models and procedures whenever necessary;
- to ensure a timely implementation and conclusion of the work;
- to approve the preliminary and final results;
- to co-ordinate the preparation of preliminary and final reports;
- to chair working meetings with the technical staff;
- to co-ordinate the work of subcontractors and consultants.

If a co-ordination group composed of delegates from the participating organizations is responsible for the technical management of the study, a permanent chairman should be designated. If many technical groups are participating it is essential to document clearly the responsibility and information transfer interfaces among each group. A detailed project schedule that clearly defines tasks and responsibilities is the best way to manage these interfaces.

It is possible to combine the SC and the CG for a simpler management structure.

A programme plan should be prepared early in a PSA to document such things as scope, objectives, methods, responsibilities, schedules, management schemes and QA in a single report.
2.4. TASK 4: SELECTION OF METHODS AND ESTABLISHMENT OF PROCEDURES

This task includes all the details of selection of methods and the establishment of corresponding procedures (see Fig. 2). It is essential that workable methods and procedures be established at the outset of the project and that there is a minimum of modification to these procedures during the project. Unnecessary iterations in methods and procedures cause expensive delays in projects.

Guidance for the methodological tools of PSA and the corresponding procedural steps is given in the following sections of this report. Once the methods have been selected, the various procedural steps must be interfaced with the tasks of QA and training to produce a detailed plan of the tasks, including a discrete schedule.

2.5. TASK 5: TEAM SELECTION AND ORGANIZATION

The members of the team that will perform the PSA can be characterized by two distinct features.

— the organization they represent;
— the technical expertise they provide.

Once the necessary personnel have been identified, lines of communication should be set up and specific tasks should be assigned. The training necessary should be determined and planned together with the activities of the PSA. The task of team formation and training is closely associated with the corresponding tasks of QA.

2.5.1. Team composition

The organizations to be represented in the PSA team depend on the life-cycle of the plant and on the specific conditions of regulation and utility operation in the particular country. Thus, for a PSA for a conceptual/early design, extensive participation of the designer of the plant is required as a supplier of basic information. For an operating plant, there will be major participation by the utility in the analysis.

An additional dimension is introduced by the extent of participation of the organization commissioning the study. The personnel making the study could be 'in-house' resources (of the commissioning organization) or external resources. In countries with only one or a few utilities, in-house resources might include resources from national research centres or other appropriate organizations affiliated with the utility (see also Section 2.3). The role of the licensing authority will vary depending on the regulatory system in a particular country as well as whether the PSA is being used directly in the licensing process. It is possible that the only involvement of the
licensing authority might be through an interactive review process. The actual participation of regulatory personnel in the team is also conceivable. In this case, a detailed procedure for dealing with potential issues concerning assumptions and the adoption of methodological tools must be established. The participation of and even leadership by the regulatory body is common for a country’s first PSA.

2.5.2. Team expertise

The expertise needed to conduct a PSA must provide two essential elements: intimate knowledge of the plant and knowledge of PSA techniques. This expertise can vary in depth, depending on the scope of the PSA, but the extensive participation of the plant designer and the utility is essential.

More specifically, the plant related expertise required consists of persons with intimate familiarity with the design and operation of the plant under normal and accident conditions. Ideally, this includes:

- **Systems analysts**: persons familiar with the design of fluid and electrical systems, operational aspects and plant layout. Disciplines usually include mechanical, electrical and instrumentation and control engineers.
- **PSA specialists**: persons familiar with event tree, fault tree methods and computer programmes.
- **Operators and operational analysts**: persons familiar with operating, test and maintenance procedures, administrative controls, control room layout and accident procedures.
- **Data analysts**: specialists in the collection and analysis of data.
- **Human factor analysts**: persons familiar with the identification and quantification of errors by operator and maintenance personnel.

Access to individuals specializing in statistics, reliability engineering and plant components is important. Access to information on plant transient responses is also required. Additional analysis may be required to eliminate conservatisms from available licensing analyses.

It is essential that individuals with operational experience participate in the PSA.

If external hazards are included in the analysis, appropriate expertise is required in specific disciplines, such as seismic and flood analysis.

Together with these two major types of expertise, a sufficient part of the team (including at least the project management) must offer the required managerial expertise.

2.5.3. Team organization

The exact organization of the PSA team into smaller groups for the specific tasks to be performed will depend on, and will follow, the establishment of detailed
procedures for the performance of the PSA and the definition of the specific tasks.

Three major groups should be defined in any PSA study:

— a managerial group;
— a systems analysis group;
— a model integration group.

The managerial group will be responsible for the management and the QA of the project, will liaise with other organizations and channels for information gathering and dissemination, and will be the focal point for the resolution of any managerial, procedural or technical issues.

The systems analysis group will be responsible for the tasks involving the modelling and quantification of the plant/system behaviour and the analysis of physical processes. It will comprise mainly personnel with expertise in system and reliability modelling.

The model integration group will be responsible for those tasks that require the integration of system models into an overall plant model and the generation of accident sequences and their quantification. This group will increase in size as the PSA progresses and may include personnel from the systems analysis group.

Although these three general groups will have been selected according to the expertise of their members, it is of the utmost importance that there is overlapping among them. Thus, some members of the PSA team must belong to more than one group and at least the heads of the systems analysis and model integration groups should participate in the managerial group. Specialized expertise (for example, from operational experts) will feed into all groups.

2.6. TASK 6: TRAINING OF THE TEAM

A team performing a PSA for the first time will require training to acquire the expertise necessary (see subsection 2.5.2) to complete the study successfully. Even if individual members of the team already have some of the expertise required, it is strongly recommended that some training precedes the study in order to achieve a common understanding of the objectives, procedures and methods of the PSA. The training can be organized along the lines of the required expertise, namely plant related and PSA related training. As a minimum, the following three types of courses should be given and attended by all PSA team members:

(1) Plant systems and operational procedures. This course (typically one to two weeks) should cover the basic aspects of system design (nuclear island and balance of plant), including operational procedures under normal and accident conditions. A condensed version of the corresponding operator training course given by the various vendors is an example of such a course. The objective
of this course is to establish a minimum common basis of understanding of plant behaviour for the members of the PSA team. Accident scenarios should be discussed in this course.

(2) **PSA techniques.** This course (typically one to two weeks) should cover the issues of event sequence and system modelling (for example, event trees and fault trees), quantification of accident sequences, uncertainty, importance and sensitivity analysis, data handling and human performance analysis. The objective of this course is to introduce the members of the team to PSA techniques and to present special methodological problems and techniques together with specific issues concerning the software to be used in the analysis. Again, the main objective here is to establish a common understanding of the techniques and a common terminology, and to resolve possible misconceptions about the advantages and disadvantages of the various methods. The course should be organized in parts, some more general, to be attended by all members of the PSA team, and some more specialized both in subject and in depth, to be attended by appropriate subgroups.

(3) **PSA procedures — comparative reviews of PSAs of similar plants.** This is a very important part of the preparation of the PSA team. It is strongly recommended that such training be given, even for teams with members highly qualified in plant systems, and good knowledge of operational procedures and PSA techniques. This course should take place as soon as possible before the commencement of the work. It should consist of a review of the complete PSA procedures, possibly after some initial consideration had been given to the procedures to be followed in the specific study, and of comparative reviews of PSAs that have been performed on plants of similar design. Again, the objective of this course is to enhance a common understanding of the PSA by the team members and to put into perspective the individual contributions to the study.

Complementary to the courses, team training can be enhanced by performing a pilot study which would consist of developing accident sequences and associated fault trees for one particular initiating event. This procedure exposes the team in a short time to all the issues to be faced in conducting the entire analysis.

### 2.7. TASK 7: FUNDING AND SCHEDULING

The resources in terms of manpower, computer time, calendar time and so on required to complete a PSA depend greatly on the scope of the PSA and on the available expertise in the PSA team. Scheduling of the activities must follow the establishment of detailed procedures and is affected by the availability of personnel. Guidance on these two issues is given in Section 2.4 of Ref. [5] and Section 2.5 of Ref. [3]. Indicative examples are included here.
Estimates of the manpower required for a Level 1 PSA are given in Table I, which is based on experience from PSAs. The lower estimate is representative of an experienced PSA team. The upper estimate is for a PSA team performing a PSA for the first time. It is not, of course, necessary that all the tasks lie within the ranges given in Table I. The exact value again depends on the expertise of the team and on the availability of the necessary information, methods and data. The need for computing resources should be recognized.

The calendar time required for the performance of the PSA depends on the personnel available and on the scope of the PSA. For any given scope, even with 'unlimited' personnel resources, some tasks have to be performed sequentially. Thus
there is a lower limit to the time necessary to complete the study. Table II provides lower and upper estimates of the time necessary to complete a PSA, together with the corresponding manpower composition.

The scheduling of the whole PSA project is of paramount importance. The schedule should cover:

— all tasks integral to the project (generally not broken down below tasks of one week in duration);
— the identification of the individual or individuals responsible for each task;
— the recognition of the dependences between tasks, including the definition of interfaces and inputs/outputs among the tasks;
— the expected duration of all tasks.

The schedule should be monitored and updated at regular intervals (typically monthly). A typical schedule for a Level 1 PSA is given in Appendix I.

If the work is carried out mainly by one or more consultants’ groups, a detailed work specification must be issued after completing the tasks relating to the study objectives, scope and selection of methods. The minimum requirements for such a document are given in Appendix II.

### TABLE II. ESTIMATE OF TEAM COMPOSITIONS REQUIRED

<table>
<thead>
<tr>
<th>Required personnel</th>
<th>Short schedule (18 months)</th>
<th>Long schedule (36 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team leader</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Systems analysts</td>
<td>8–10</td>
<td>5</td>
</tr>
<tr>
<td>PSA methodologists/quantification specialists</td>
<td>3–4</td>
<td>2</td>
</tr>
<tr>
<td>Human performance analysts</td>
<td>1–2</td>
<td>1</td>
</tr>
<tr>
<td>Data analysts</td>
<td>1–2</td>
<td>1</td>
</tr>
<tr>
<td>External hazard analysts</td>
<td>2</td>
<td>1–2</td>
</tr>
</tbody>
</table>

* Some of these personnel may not be required for the complete duration of the study or may be involved in more than one task.
It is also possible that a consultant might advise the commissioning organization on the possible objectives, scope and methods/procedures before the work specification is prepared.

2.8. TASK 8: ESTABLISHMENT OF A QUALITY ASSURANCE PROGRAMME AND INTERACTIVE PEER REVIEW

The quality assurance programme of a PSA encompasses the activities that are necessary to achieve the appropriate quality of the PSA and those that are necessary for verifying that the required quality is achieved (see Section 103 of Ref. [6]). For a PSA, appropriate quality means an end product that is correct, usable and meets the objectives and fills the scope of the PSA.

Quality assurance is an essential aspect of 'good management' (see Section 104 of Ref. [6]). Good management contributes to the achievement of quality through thorough analysis of the tasks to be performed, identification of the skills required, selection and training of appropriate personnel, use of appropriate procedures, creation of a satisfactory environment in which activities can be performed and recognition of the responsibility of the individual who is to perform each task. Briefly stated, the QA programme shall provide for a disciplined approach to all activities affecting the quality of the PSA, including, where appropriate, verification that each task has been satisfactorily performed and that the necessary corrective actions have been implemented.

Quality assurance of the PSA should be viewed and established as an integral part of the PSA project and the QA procedures should be an integral part of the PSA procedures. The QA procedures should provide for control of the constituent activities associated with a PSA, which can be distinguished in the following three areas: organization, technical work and documentation. Specific aspects of QA procedures in these three areas are presented in Appendix III and are discussed in the following paragraphs.

As mentioned earlier, QA is an essential aspect of good management and in that sense all the tasks of the major procedural steps of a PSA are subject to the QA procedures concerning the organization and management of the PSA.

Quality assurance procedures also apply to the technical work, ensuring consistency between goals, scope, methods and assumptions, as well as accuracy in the application of methods and in calculations.

Quality assurance procedures include control of the documentation of the PSA. General requirements for document control are given in Section 4 of Ref. [6]. The term 'PSA documentation', as used in this report and in the establishment of QA procedures in particular, includes work files, computer output, correspondence, interim reports and the final report. Documentation should also be complete to the extent that the progress of the study is traceable, and should be retained to ensure
that traceability continues for a specific period of time. In general, QA activities concerning the documentation of the PSA will also contribute to enhancing its clarity and its traceability.

An important issue related to the verification aspect of QA activities is that of interactive, external peer review of the PSA. That is, a review of the study while it is in progress by either a consulting group or a licensing authority or both. These two groups are mentioned here to highlight the two major reasons for interactive review. The first is that external peer review of technical work in progress can make a positive contribution to the validity of the results, particularly when the work is being performed by a group for the first time. The second applies more to cases in which the intended use of the PSA is dictated not by the organization performing the study, but by another organization; for example, a licensing authority. In this case, an interactive review will ensure that the study properly addresses the concerns of the external users, that its content is useful to them, and that it will provide early and effective feedback to the analysis team.

To avoid undue disruption of the study, interactive reviews should be performed at selected ‘milestones’. The specific areas of the PSA that could benefit from a review are:

1. The methods selected and associated assumptions and their adequacy to meet defined objectives and to fulfil the scope of the PSA. If the selected methods contain novel elements there might be a need to demonstrate their validity.
2. Selection of initiators and plant operational states and identification of sources of radioactive releases.
3. Grouping of initiators and event tree construction, including definition and documentation of mission success criteria.
4. Plant system modelling (e.g. fault tree construction).
5. Approach to human reliability and dependency analysis.
6. Database selection/development and parameter estimation.
7. Identification and quantification of accident sequences.
8. Results obtained.
9. Uncertainty, importance analysis and sensitivity analysis.
10. External event analysis (if performed).

Natural milestones for interactive review would be the completion of each of the six major procedural steps (see Section 1).

Specific guidance on peer review is given in an IAEA publication [7].

Responding to the needs of Member States, the IAEA provides International Peer Review Services (IPERS) which bring international PSA experience into the review process.

Appendix III provides further guidance for the establishment of the QA procedures.
3. IDENTIFICATION OF SOURCES OF RADIOACTIVE RELEASES AND ACCIDENT INITIATORS

Section 3 describes the second major procedural step of a PSA. The main purpose of this step is to produce a list of initiating events (IEs) that should be subject to analysis and then to group these IEs in order to reduce the tasks of accident sequence modelling and quantification described in Sections 4 and 6. Initially, however, Section 3 also describes tasks that follow on from those in Section 2 related to familiarization with the plant and to the objectives and scope of the PSA.

Some of the tasks described here that are necessary for the process of grouping initiating events are developed further and more definitively after the tasks described in Section 4. It must be recognized that the process is an iterative one and, in particular, that the grouping will need to be reviewed after the detailed accident sequence modelling step has been completed (and perhaps also after the quantification step).

The following nine tasks in this step can be distinguished and a schematic representation is given in Fig. 3. (The task numbering follows consecutively from Section 2.)

3.1. TASK 9: FAMILIARIZATION WITH THE PLANT AND PSA AND INFORMATION GATHERING

The purpose of this task is to provide the members of the team with the information necessary for performing the second and third major procedural steps. To complete this task successfully, the PSA team should become familiar with the design and operation of the plant, including the emergency procedures and the test and maintenance procedures.

Since some team members will probably be familiar with the plant but not with PSA techniques, and others familiar with the methods but not with the plant, members will require familiarization in different areas. One of the objectives of this task is to provide the entire team with a balanced overview of the basic issues in carrying out a PSA. This will be accomplished with the completion of this task together with the team training (see Section 2.6).

In addition to providing all team members with a balanced overview of the basic issues, the other major objective of this task is to gather all the information necessary for the study. Consequently, team members will acquire, according to their expertise and assigned area, knowledge in depth of the plant and of PSA methods, together with the necessary documentation and other information.

A system for keeping track of and updating the acquired documentation should be developed.
FIG. 3. Procedural tasks for the identification of sources of radioactive releases and accident initiators.
TABLE III. INFORMATION SOURCES NEEDED\(^a\) FOR FAMILIARIZATION WITH THE PLANT

1. Final safety analysis report  
2. Plant technical specifications and other regulatory requirements  
3. System descriptions  
4. As built (as is) system drawings (piping and instrumentation diagrams)  
5. Electrical line drawings including circuit diagrams and trip criteria for the electrical bus protection system  
6. Control and actuation circuit drawings  
7. Normal, emergency, test and maintenance procedures  
8. Analyses pertinent to the determinants of mission success criteria of systems  
9. Plant visits  
10. Reviews with operating staff  
11. Licensee event reports from the plant or from similar plants in the same or other countries, plant incident reports and analyses  
12. Plant layout drawings  
13. Piping location and routing drawings  
14. Cable location and routing drawings

\(\text{\(a\) Some of this information will not be available in the early stages of a design, and in some cases not until the plant is in service.}\)

Table III provides a list of some of the sources of the information necessary for the plant familiarization task. Review of the past history of the plant would contribute to the completeness of the plant model (e.g. by including in the modelling certain dependences shown by actual events) as well as providing information useful in the quantification of the model.

References [5, 8–11] may be consulted for purposes of familiarization with PSA.

Members of the team would benefit from studying past PSA analyses, particularly those that have undergone detailed review. In addition to gaining a better sense of what were the objectives and the means to fulfil them, it is useful to understand the main criticisms that have been made of the analyses and how they have been responded to. Such a compendium of issues that led to questions in various reviews is presented in the Probabilistic Risk Assessment Review Manual [11].
3.2. TASK 10: IDENTIFICATION AND SELECTION OF SITE SOURCES OF RADIOACTIVE RELEASES

A list should be made of all sources of radioactive releases (including content and form) from which accidental releases could be postulated. For example, for an LWR this list should include the reactor core, the refuelling pool, spent fuel handling facilities and waste storage tanks. If any of these sources are excluded from detailed consideration in the PSA, the exclusion should be justified in the study. This task interacts with Task 2 on the definition of the scope of the PSA.

3.3. TASK 11: DETERMINATION AND SELECTION OF PLANT OPERATING STATES

Probabilistic safety assessments have often considered only one plant operating state in which an accident may be initiated, that of normal full power operation. There are, however, other plant operating states in which either other accident initiators might occur or the success criteria for and/or the unavailability of some systems might differ from those for full power operation.

Plant operating states of concern are listed in subsection 2.2.1. Exclusion of any operating state(s) of the plant from further analysis should be justified. The justification may be based on the scope of the PSA. The justification may also be based on a judgement that certain operating states are of lesser importance in contributing to the overall risk and may also relate to economic or resource constraints.

3.4. TASK 12: DEFINITION OF CORE DAMAGE STATES OR OTHER CONSEQUENCES

A Level 1 PSA usually implies assessing plant failures leading to severe core damage and the corresponding frequencies. Additional events of concern that may be appropriately included in a Level 1 PSA, however, are those that cause partial core damage or lesser releases from the primary coolant or from ex-core sources. The consequences of concern to be included in the study are first determined during Tasks 2 and 10, in which the scope of the study is assessed. In Task 12 the undesirable end states of the analysis are defined in greater detail.

The most important definition that must be made in this task is that of core damage. There are several possible degrees of 'core damage', the severity depending on the extent of core damage and on the magnitude of the resulting radioactive releases from the core. It should be emphasized that the final quantitative result, i.e. the frequency of core damage, greatly depends on the definition of what constitutes...
core damage. The conditions for core damage need to be translated into system failure states to allow the PSA to proceed, and where possible this should be based on realistic analyses. In the absence of such analyses, core damage may be conservatively assumed to occur if the design basis of the plant is exceeded. In most past PSAs a successful end state of the plant (e.g. stable hot shutdown or stable cold shutdown) is defined and every accident sequence that does not lead to this successful end state is assumed to lead to core damage.

Resolution of suspected conservatisms concerning the end result of an accident sequence may be more efficient — in terms of time and resources — if realistic analyses are conducted at a later stage of the PSA, after a sensitivity analysis has assessed the relative importance of the various accident sequences. It would then be possible to judge the importance of resolving whether a particular sequence of events could or could not lead to core damage as initially assumed.

In addition to core damage, radioactive releases without core damage may be of concern; for example, if they are sufficient to trigger emergency responses off the site. Minor radioactive releases of concern may be from in-core sources or from radionuclides resident in the primary coolant circuit. As most PSAs to date have only considered core damage, in the remainder of these guidelines the product of this task will be referred to as core damage.

3.5. TASK 13: SELECTION OF INITIATING EVENTS

The end product of this task is a list of initiating events (IEs) that is as complete as possible. It should be recognized, however, that it is not possible to establish that any such list is complete. A judgement is required that any IEs not identified would make only a small contribution to the total risk. The scope of the PSA could also constrain the initiating events that are to be considered.

An initiating event is an event that creates a disturbance in the plant and has the potential to lead to core damage, depending on the successful operation of the various mitigating systems in the plant. Also, events that are sometimes claimed to be of such low frequency that they need not be considered should be addressed (e.g. major structural failure of a pressure vessel).

There are several approaches to the selection of IEs, each of which has its limitations. Since the aim is to produce a list that is as complete as possible, it is

---

3 The term initiating event as used in these guidelines for PSA purposes is equivalent to the term postulated initiating event defined in Section 4.4 and Appendix A of Ref. [12] or the Appendix of Ref. [4]. It must be emphasized, however, that the list of initiating events in a PSA is by no means confined to any list of events postulated for design and licensing purposes, nor is it associated with qualitative qualifiers such as ‘credible’ or ‘anticipated’.
recommended that all of the approaches should be followed, although one may be selected as the main approach. The approaches are as follows:

(1) **Engineering evaluation.** The plant systems (operational and safety) and major components are systematically reviewed to see whether any of the failure modes (e.g. failure to operate, spurious operation, breach, disruption, collapse) could lead directly, or in combination with other failures, to core damage. Partial failures of systems should also be considered since, although they are generally less severe than complete failure, they are of higher frequency and are often less readily detected. Special attention should be given to common cause initiators.

(2) **Reference to previous lists.** It is useful to refer to lists of IEs drawn up for previous PSAs on similar plants and for the safety analysis report. This may in fact be the starting point. Reference [13], for example, provides a list for transient initiators for LWRs.

(3) **Deductive analysis.** In this approach, core damage is made the top event in a diagram which has the appearance of a fault tree (although it is not one in the usual sense). This top event is successively broken down into all possible categories of events that could cause it to occur. Successful operation of safety systems and other preventive actions are not included. The events at the most fundamental level are then candidates for the list of IEs for the plant. An example of such a diagram is the master logic diagram described in Refs [5] and [10]. This approach is also documented in Ref. [14], subsection 5.2.2, where its use for transient initiators is systematically described. The use of a master logic diagram can also assist in the definition of safety functions (Task 14).

(4) **Operational experience.** In this approach, the operational history (if any) of the plant in question and of similar plants elsewhere is reviewed for any events that should be added to the list of IEs. This approach is supplementary and would not be expected to reveal low frequency events, but it could show common cause IEs.

Initiating events are generally classified into internal IEs and hazards (internal and external). Internal IEs are hardware failures in the plant or faulty operations of plant hardware through human error or computer software deficiencies. External hazards (which may also be termed external events) are events that create extreme environments common to several plant systems. External hazards include earthquakes, floods, high winds and aircraft crashes. Internal hazards include internal flooding, fire and missile impact.

Loss of connection to the grid (complete or partial) is sometimes classified as an external hazard, but it is recommended that it should be considered as an internal IE. Electrical supply faults such as excessive variations in grid voltage and frequency should also be included.
Advice on the treatment of hazards is given in Ref. [2]. It is important to provide a justification for the exclusion from the PSA of any identified hazards.

Guidance for the selection of internal IEs for LWRs is given in Ref. [3] (subsection 3.4.2), Ref. [5] (subsection 3.4.2) and Ref. [15] (subsection 1.3.2). For LWRs, the accident initiators fall into two major categories: loss of coolant accident (LOCA) initiators and transient initiators.

Loss of coolant accident initiators are all events that directly cause loss of integrity of the primary coolant pressure boundary. Of particular importance are events in systems that have an interface with the primary coolant system and lead to LOCAs outside the containment (interfacing systems LOCAs). A second category of LOCA of special importance includes those breaks that occur at locations that can entirely or partially disable systems that are needed for mitigating the accident.

Transient initiators are those that could create the need for a reactor power reduction or shutdown and subsequent removal of decay heat. Of particular interest are events that can cause a transient and at the same time can cause the total or partial failure of a system needed for mitigating consequences. A special subset of this type of transients is those that are caused by complete or partial failure of support systems.

When the list of IEs has been made as comprehensive as possible, it should be reviewed to remove any repetitions or overlaps and given a further check for any inadvertent omissions.

Once identified, the IEs are normally listed in a systematic way, e.g.:

1. LOCA break sizes;
2. interfacing system LOCAs;
3. LOCAs that affect mitigating systems;
4. transients applicable to the plant;
5. transients initiated by support system faults which affect mitigating systems;
6. hazards (internal and external).

It should be recognized that the subsequent steps in the PSA analysis may reveal further IEs.

3.6. TASK 14: DETERMINATION OF SAFETY FUNCTIONS

This section on safety functions and the following sections on safety function/system relationships (Section 3.7) and plant system requirements (Section 3.8) are included in Section 3 because of the need to investigate these areas before grouping initiating events. This is because initiating events can only be grouped if the demands they place on safety functions, front line systems and support systems are the same. Much of the knowledge acquired in the conduct of these tasks will be directly usable in the accident sequence modelling step in Section 4.
For each IE, the safety functions that need to be performed in order to prevent core damage should be identified. The concept of a safety function is described in Ref. [16].

Several definitions of safety functions are possible, depending on the degree of resolution of the initial general safety objective. It is useful to consider safety functions as elements of a hierarchy of objectives; that is, a system of levels of objectives which at each level contribute to the fulfilment of the objectives of the higher level. Different definitions of safety functions result if this deductive process is stopped at different levels of decomposition. It is useful, therefore, to generate such a hierarchy, which may be depicted in a master logic diagram, as described in Section 3.5.

Refs [3] and [5] list safety functions for LWRs used in PSAs, while Ref. [15] provides a more general list of safety functions. A modified list of safety functions for PSA purposes is given in Table IV.

A cut-off criterion may be applied to separate out those IEs which are of very low frequency. This can only be done, of course, after Task 24 has been completed, at least in a preliminary way. The purpose is to avoid undue effort in systems analysis for low frequency IEs which will not make a significant contribution to the overall core damage frequency. Such IEs should not be discarded but should be recorded and a rough estimate of their contribution should be incorporated into the overall results. Low frequency IEs that can cause containment failure at a high probability may need to be considered in detail if the scope of the PSA is to be extended to a Level 2 analysis.
3.7. TASK 15: ASSESSMENT OF FUNCTION/SYSTEM RELATIONSHIPS

The systems that are directly or indirectly required for the proper performance of each safety function are identified in this task. The systems that directly perform a safety function are termed front line systems; those required for the proper functioning of the front line systems are termed support systems. The objective of this task is to obtain all the necessary information about the systems that will determine

TABLE V. SAFETY FUNCTIONS AND CORRESPONDING FRONT LINE SYSTEMS

<table>
<thead>
<tr>
<th>Safety function</th>
<th>Front line systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control reactivity</td>
<td>(a) Reactor protection system</td>
</tr>
<tr>
<td></td>
<td>(b) High pressure injection system</td>
</tr>
<tr>
<td>Remove core decay heat and stored heat</td>
<td>(a) Power conversion system</td>
</tr>
<tr>
<td></td>
<td>(b) Emergency feedwater system</td>
</tr>
<tr>
<td></td>
<td>(c) High pressure injection system and pressurizer safety relief valves</td>
</tr>
<tr>
<td></td>
<td>(d) Low pressure injection system</td>
</tr>
<tr>
<td></td>
<td>(e) Residual heat removal system</td>
</tr>
<tr>
<td>Maintain integrity of primary reactor coolant boundary</td>
<td>Pressurizer safety relief valves</td>
</tr>
<tr>
<td>(pressure control)</td>
<td></td>
</tr>
<tr>
<td>Maintain primary reactor coolant inventory</td>
<td>(a) High pressure injection system</td>
</tr>
<tr>
<td></td>
<td>(b) Low pressure injection system</td>
</tr>
<tr>
<td>Protect containment integrity</td>
<td>(a) Reactor building spray system</td>
</tr>
<tr>
<td>(isolation, overpressure)</td>
<td>(b) Reactor building cooling system</td>
</tr>
<tr>
<td>Scrub radioactive materials from containment atmosphere</td>
<td>Reactor building spray system</td>
</tr>
</tbody>
</table>

a Adapted from Ref. [15].
b The high pressure injection system may only support the reactivity control function if the reactor coolant system components survive the overpressure transient following reactor protection system failure.
c Only required for binning purposes; see Appendix VII.
TABLE VI. EXAMPLES OF FRONT LINE SYSTEMS FOR A PWR

1. Reactor protection system
2. Core flood system
3. High pressure injection/recirculation system
4. Low pressure injection/recirculation system
5. Reactor building spray injection/recirculation system
6. Reactor building cooling system
7. Power conversion system
8. Emergency feedwater system
9. Pressurizer safety relief valves

* Adapted from Ref. [15].

the plant response for a particular IE and assess in a preliminary way some of the existing dependences.

For each safety function, all the front line systems that perform this function, alone or in combination with other systems, should be identified and catalogued (see for example Table V). An explanation should be added if any of these systems can perform a safety function only under special conditions.

A list of all front line systems to be analysed should be generated (see Table VI) and all associated information should be gathered (by interaction with Task 9).

To gain an early understanding of the relationships between front line and support systems, a dependence table of front line/support systems (FL-SS) can be prepared. An example is given in Table VII.

A list of support systems is generated from the initial FL-SS table. All systems that are required for the proper functioning of each of these support systems are identified and added to the list of support systems. This process is continued until all systems that somehow affect the functioning of front line systems through this chain of dependences have been identified.

Any possible dependences among support systems are depicted in a dependence table of support systems versus support systems (SS-SS). This table is similar to the FL-SS table already mentioned.

The dependence table (FL-SS) is updated to include the additionally identified support systems and the corresponding dependences. Finally, the FL-SS dependence
<table>
<thead>
<tr>
<th>Front line systems</th>
<th>Support systems</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off-site AC power</td>
</tr>
<tr>
<td>Reactor protection system</td>
<td>x</td>
</tr>
<tr>
<td>Core flood system</td>
<td>x</td>
</tr>
<tr>
<td>High pressure injection/ recirculation</td>
<td>x</td>
</tr>
<tr>
<td>Low pressure injection/ recirculation</td>
<td>x</td>
</tr>
<tr>
<td>Reactor building spray injection/ recirculation</td>
<td>x</td>
</tr>
<tr>
<td>Reactor building cooling system</td>
<td>x</td>
</tr>
<tr>
<td>Power conversion system</td>
<td>x</td>
</tr>
<tr>
<td>Emergency feedwater system</td>
<td>x</td>
</tr>
<tr>
<td>Pressurizer safety relief valves</td>
<td>x</td>
</tr>
</tbody>
</table>

a Adapted from Ref. [15].
b All requirements for diesel generators assume loss of station power.
table would indicate dependences among FL systems, either because they depend on the same support systems or because they depend on different support systems which themselves depend on a common third system, and so on.

It should be noted that dependences identified in this step are rather obvious hardware or functional dependences and simply define areas that should be examined in detail in later steps and should be taken into consideration in the event sequence modelling (see Section 4.1).

The final results of this task are:

1. safety functions for each IE and a table of safety functions and combinations of front line systems that can perform each function;
2. a list of front line systems;
3. a list of support systems (all inclusive);
4. a dependence table among FLs and SSs;
5. A dependence table among SSs and SSs.

The systems identified in this task are those to be analysed in the accident sequence modelling and in the system modelling activities.

3.8. TASK 16: ASSESSMENT OF PLANT SYSTEM REQUIREMENTS

The performance required of a front line system depends in general on the IE. Required performance means the minimum system performance that will allow for the successful fulfilment of its safety function under the specific conditions created by the IE. The success criteria of front line systems are of particular importance for the PSA because they will define the top events or the starting point for the subsequent system modelling (see Section 4.2). The success criteria for front line systems will undergo a further narrower definition during the evaluation of the plant response, because they may depend not only on the initiator but also on additional system failures or successes in a particular accident sequence.

Success criteria can be unambiguously defined for front line systems, for which a clear success or failure in the performance of a safety function can be recognized. In addition to a performance definition (e.g. flow rate, response time, trip limits), the success criteria must be expressed in hardware terms, such as the number of required fluid flow paths, power trains, etc.

Success criteria for support systems cannot be so readily defined because in most cases they serve more than one front line system, and consequently each possible state of the system (e.g. three trains operating, two trains operating, one train operating, no train operating) has a different effect on the front line systems that perform a certain function. A particular support system state could therefore lead to a safety function success or failure depending on the particular state of the front line system with which it is combined.
### TABLE VIII. EXAMPLE OF GROUPING OF INITIATING EVENTS

<table>
<thead>
<tr>
<th>Boiling water reactors</th>
<th>Pressurized water reactors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Turbine trip</td>
<td>1. Large LOCA</td>
</tr>
<tr>
<td>2. Loss of feedwater flow</td>
<td>2. Medium LOCA</td>
</tr>
<tr>
<td>3. Closure of main steam isolation valve</td>
<td>3. Small LOCA</td>
</tr>
<tr>
<td>4. Loss of condenser</td>
<td>3(a) Interfacing system LOCA</td>
</tr>
<tr>
<td>5. Loss of off-site power</td>
<td>4. Steam generator tube rupture</td>
</tr>
<tr>
<td>6. Inadvertent opening of relief valves</td>
<td>5. Steam break inside containment</td>
</tr>
<tr>
<td>8. Loss of DC power bus(es)</td>
<td>7. Loss of main feedwater</td>
</tr>
<tr>
<td>9. Loss of instrument air</td>
<td>8. Trip of one MSIV</td>
</tr>
<tr>
<td>11. Loss of dry well cooling</td>
<td>10. Core power excursion</td>
</tr>
<tr>
<td>12. ATWS with turbine trip</td>
<td>11. Turbine trip</td>
</tr>
<tr>
<td>13. ATWS with closure of main steam isolation valve (MSIV)</td>
<td>11(a) Turbine trip — loss of off-site power</td>
</tr>
<tr>
<td>14. ATWS with loss of off-site power</td>
<td>11(b) Turbine trip — loss of service water</td>
</tr>
<tr>
<td>15. ATWS with inadvertently opened relief valve (IORV)</td>
<td>12(a) Reactor trip</td>
</tr>
<tr>
<td>16. ATWS with loss of DC power bus(es)</td>
<td>12(b) Reactor trip — loss of component cooling</td>
</tr>
<tr>
<td>17. Large LOCA inside containment</td>
<td>13. ATWS</td>
</tr>
<tr>
<td>18. Medium LOCA inside containment</td>
<td>14. Seismic event</td>
</tr>
<tr>
<td>19. Small LOCA inside containment</td>
<td>15. Flooding</td>
</tr>
<tr>
<td>20. LOCAs outside containment</td>
<td>16. Fires</td>
</tr>
<tr>
<td>21. Seismic event</td>
<td></td>
</tr>
<tr>
<td>22. Floods</td>
<td></td>
</tr>
<tr>
<td>23. Fires</td>
<td></td>
</tr>
</tbody>
</table>

Relevant information for the assessment of front line success criteria is given in the Final Safety Analysis Report (FSAR). Criteria derived from assumptions in the FSAR might be overly conservative, however. More realistic success criteria should be used if available. These realistic criteria should nevertheless be supported by analyses that document their validity. Existing analyses for the particular plant or for other similar plants can be used to derive success criteria more realistic than those derived from FSAR assumptions. These analyses should be clearly referenced and should be part of the PSA documentation (see Section 7) if the references are not accessible. Where very conservative success criteria are initially derived from
### TABLE IX. EXAMPLE OF INITIATING EVENT GROUPING FOR A CANDU NUCLEAR POWER PLANT

<table>
<thead>
<tr>
<th>Number</th>
<th>Initiating event group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Forced shutdown</td>
</tr>
<tr>
<td>2.</td>
<td>LOCAs</td>
</tr>
<tr>
<td>2.1.</td>
<td>Small LOCA inside containment</td>
</tr>
<tr>
<td>2.2.</td>
<td>Small LOCA outside containment</td>
</tr>
<tr>
<td>2.3.</td>
<td>Medium LOCA inside containment</td>
</tr>
<tr>
<td>2.4.</td>
<td>Medium LOCA outside containment</td>
</tr>
<tr>
<td>2.5.</td>
<td>Large LOCA</td>
</tr>
<tr>
<td>2.6.</td>
<td>Other LOCAs</td>
</tr>
<tr>
<td>3.</td>
<td>Pressure tube rupture</td>
</tr>
<tr>
<td>4.</td>
<td>End fitting failure</td>
</tr>
<tr>
<td>5.</td>
<td>Steam generator tube rupture</td>
</tr>
<tr>
<td>6.</td>
<td>Loss of high temperature pressure control (low)</td>
</tr>
<tr>
<td>7.</td>
<td>Loss of high temperature pressure control (high)</td>
</tr>
<tr>
<td>8.</td>
<td>Loss of pressure control (high) in solid mode due to loss of controller</td>
</tr>
<tr>
<td>9.</td>
<td>High temperature pressure and inventory control failures</td>
</tr>
<tr>
<td>10.</td>
<td>Any one primary heat transport pump trips</td>
</tr>
<tr>
<td>11.</td>
<td>Flow blockage (in an individual channel)</td>
</tr>
<tr>
<td>12.</td>
<td>Moderator failure</td>
</tr>
<tr>
<td>13.</td>
<td>Loss of end shield cooling</td>
</tr>
<tr>
<td>14.</td>
<td>Shutdown cooling failures</td>
</tr>
<tr>
<td>15.</td>
<td>Main steam line break</td>
</tr>
<tr>
<td>16.</td>
<td>Loss of feedwater to one or more steam generators</td>
</tr>
<tr>
<td>17.</td>
<td>Feedwater line break</td>
</tr>
<tr>
<td>18.</td>
<td>Turbine trip</td>
</tr>
<tr>
<td>19.</td>
<td>Loss of condenser vacuum</td>
</tr>
<tr>
<td>20.</td>
<td>Reheater drain line break</td>
</tr>
<tr>
<td>21.</td>
<td>Loss of condensate flow</td>
</tr>
</tbody>
</table>
TABLE IX. (cont.)

<table>
<thead>
<tr>
<th>Number</th>
<th>Initiating event group</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.</td>
<td>Unplanned bulk increase in reactivity</td>
</tr>
<tr>
<td>23.</td>
<td>Unplanned regional increase in reactivity</td>
</tr>
<tr>
<td>24.</td>
<td>Loss of computer control</td>
</tr>
<tr>
<td>25.</td>
<td>Loss of low pressure service water open system</td>
</tr>
<tr>
<td>26.</td>
<td>Loss of reactor cooling water system</td>
</tr>
<tr>
<td>27.</td>
<td>Loss of powerhouse upper level service water</td>
</tr>
<tr>
<td>28.</td>
<td>Loss of instrument air</td>
</tr>
<tr>
<td>29.</td>
<td>Loss of cooling to fuel machine in transit</td>
</tr>
<tr>
<td>30.</td>
<td>Loss of bulk electricity supply</td>
</tr>
<tr>
<td>31.</td>
<td>Loss of switchyard</td>
</tr>
<tr>
<td>32.</td>
<td>Loss of power to unit Class IV 13.8 kV bus</td>
</tr>
<tr>
<td>33.</td>
<td>Partial loss of unit Class IV power</td>
</tr>
<tr>
<td>34.</td>
<td>Partial loss of unit Class III 120 V power</td>
</tr>
<tr>
<td>35.</td>
<td>Partial loss of unit Class II 120 power</td>
</tr>
<tr>
<td>36.</td>
<td>Partial loss of unit Class II 45 V power</td>
</tr>
<tr>
<td>37.</td>
<td>Partial loss of unit 48 V power</td>
</tr>
<tr>
<td>38.</td>
<td>Loss of unit Class IV power while shut down</td>
</tr>
</tbody>
</table>

* Adapted from Ref. [17].

An FSAR analysis, it should be recognized that, at some stage in the PSA process, additional analyses may be necessary to support realistic success criteria for the final PSA models. An alternative course of action would be to investigate the effects of relaxing success criteria in a sensitivity analysis. A sensitivity analysis may precede and justify any major additional analysis (e.g. transient analysis) to support more realistic success criteria.

In addition to the success criteria imposed on the front line systems by the initiators, any other special conditions imposed by these initiators must also be assessed.
and recorded. Such special conditions may be effects on support systems, on symptoms displayed to the operator, on automatic actuation systems or on the potential for inducing dependent failures. These special conditions will be used in grouping the initiators into equivalent classes (see Section 3.9).

As a result of this task a table is prepared giving for each initiator the associated systems as identified earlier, their success criteria for that initiator, references to supporting documentation and special characteristics of the initiator which affect the modelling assumptions.

3.9. TASK 17: GROUPING OF THE INITIATING EVENTS

Once the task of assessing the requirements of the plant systems has been completed, the initiating events can be grouped in such a way that all events in the same group impose essentially the same success criteria on the front line systems as well as the same special conditions (challenges to the operator, to automatic plant responses, etc.) and thus can be modelled using the same event/fault tree analysis.

In the process of grouping, it will become clear that some categories of IE need to be subdivided. Dividing LOCAs by break size (and perhaps location) is a well known example but other cases should be expected: examples are steam line break by size, loss of flow by number of pumps failed and spurious control rod withdrawal by number of rods or rate of reactivity addition.

The subsequent analysis needed may be reduced by grouping together IEs that evoke the same type of plant response but for which the front line system success criteria are not identical. The success criteria applied to this group of events should then be the most onerous for any member of the group. The saving in effort must be weighed against the conservatism which this introduces.

Table VIII gives an example of initiator groupings for LWR plants and Table IX gives the initiator grouping used in a PSA of a Canadian plant with a CANDU reactor.

4. ACCIDENT SEQUENCE MODELLING

The third major procedural step includes all the aspects of model building for the plant. The culmination of this task is a model that defines the initiators of potential accidents, the response of the plant to these initiators and the spectrum of resulting plant damage states. Specific accident sequences are defined that consist of an initiating event group, specific system failures and successes, and their timings and human responses. These then produce a plant damage state. The system failures are
Impact of physical processes on development of logic models

Event sequence modelling

Classification of accident sequences into plant damage states

System modelling (fault trees or other)

Human performance analysis

Qualitative dependence analysis

FIG. 4. Procedural tasks for accident sequence modelling.
in turn modelled in terms of basic component unavailabilities and human errors to
identify their basic causes and to allow for the quantification of the system failure
probabilities (unavailabilities) and accident sequence frequencies.

Six tasks (18 to 23) can be distinguished for this procedural step. A schematic
representation of these tasks is shown in Fig. 4.

4.1. TASK 18: EVENT SEQUENCE MODELLING

Once accident initiating events have been identified and grouped, it is neces-
sary to determine the response of the plant to each group of initiating events. This
modelling of the responses results in the generation of event sequences. An event
sequence model provides sequences of events that, following an initiating event, lead
either to a successful state or to a core damage state. Event sequences are expressed
in terms of initiating events and successes or failures of mitigating systems. System
failures are subsequently represented by another set of models which are logical
combinations of simpler events. Particular models for event sequences and system
models are presented in Refs [3, 5, 9 and 15] and include:

(1) methods for event sequence modelling:
   — event trees (ET)
   — cause consequence diagrams (CCD)
   — event sequence diagrams.

(2) methods for system modelling:
   — fault tree (FT)
   — state space diagrams and Markov analysis
   — block diagram (BD)
   — go chart (GO).

Use of the combined event tree/fault tree method represents the recommended
basic modelling approach. Other methods mentioned are to be regarded as supple-
mentary and are of interest in specific modelling situations as outlined later in this
section.

One usual problem in selecting the method for a PSA is the determination of
the level of event resolution at which event sequence modelling stops and system
modelling begins. This problem has been exemplified in the event and fault tree
formats where two general tendencies have been identified:

(1) The so-called small event tree/large fault tree approach proposed in Ref. [11],
in which dependences between front line systems and support systems do not
appear in the event trees;

(2) The so-called large event tree/small fault tree approach described in Ref. [3],
in which dependences between front line systems and support systems do
appear in the event trees.
Both approaches are acceptable since in principle they are equivalent. In fact it is possible to incorporate both event sequence modelling and system modelling in any one of the methods mentioned, as is shown in Table X. The exact point of resolution for switching from event sequence development to system modelling is actually a matter of preference, availability of computational tools and familiarity of the analysts with one or another approach. Each method has advantages and disadvantages, and these are presented in the following subsections in which the various techniques are discussed. Whichever approach is adopted, adequate documentation must be supplied and the analysis must be verifiable and traceable.

The event sequence models simulate the response of the plant to an accident initiator and consequently are based on supporting transient and LOCA analyses which define the minimum successful response required from the various systems. The definition of this minimum successful response or 'success criterion' is the output of Task 16, discussed in Section 3.8. In the development of event sequence models, care must be taken to define the success criteria clearly for every mitigating system that appears in each accident sequence. This is important where the criteria for the same system differ for different accident sequences. Once this is done it is possible to characterize the end result of each event sequence as a success state (if the initiating event has been mitigated) or a failed state. A failed state has been

<table>
<thead>
<tr>
<th>TABLE X. POSSIBLE RANGES FOR MODELLING TECHNIQUES a</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Event tree</td>
</tr>
<tr>
<td>Cause consequence diagram</td>
</tr>
<tr>
<td>Fault tree</td>
</tr>
<tr>
<td>Block diagram</td>
</tr>
<tr>
<td>Go chart</td>
</tr>
<tr>
<td>State space (Markov)</td>
</tr>
</tbody>
</table>

a Adapted from Ref. [9]. Solid lines indicate the ranges most commonly used; broken lines indicate possible uses.
defined in Task 12 on the definition of core damage states and other consequences (Section 3.4). The event sequences that lead to core damage are termed accident sequences in these guidelines.

4.1.1. Event trees

Event trees are graphic models that order and reflect events according to the requirements for mitigation of each group of initiating events. Events or 'headings' of an event tree can be a safety function's status, a system's status, basic events occurring or operator actions.

Event trees display some of the functional dependences between the events or 'headings' of the tree; e.g. cases where failure of one system implies that another system cannot perform its function successfully. Such dependences result in omitted branch points. Omitted branch points also occur if the failure of a given system does not affect the plant damage state associated with a given accident sequence.

The event tree headings are normally arranged in either chronological or causal order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in an accident. Causal ordering means that events are arranged in the tree so that the number of omitted branch points is maximized.

As stated earlier, there are two general tendencies concerning the nature of the headings of the event trees and consequently their size: (a) small event trees; (b) large event trees.

4.1.1.1. Small event trees (large fault trees)

In the small event tree/large fault tree approach, event trees with safety functions as headings are first developed and then expanded to event trees with the status of front line systems as headings. The front line system fault tree models are developed down to suitable boundaries (see subsection 4.2.1) with support systems. The support system fault trees may be developed separately and integrated at a later stage into the front line system models. The dependence matrices developed in Task 15 are used here as a first indication of which support systems should be included in the front line system fault trees.

This approach generates event trees that are concise and that allow for a synthesized view of an accident sequence. Furthermore, subject to the availability of computer codes, the small event trees may be more readily computerized. However, dependences and the corresponding importance of support systems are not explicitly apparent. In addition, handling of large fault trees requires special codes. This might be a severe constraint, particularly if analysis of non-coherent fault trees is required through the inclusion of success states for systems.
4.1.1.2. Large event trees (small fault trees)

In the large event tree approach, all support system states appear explicitly in the event trees. The top events on the fault trees have associated boundary conditions; the boundary conditions include the assumption that the support system is in the particular state appropriate to the event sequence being evaluated. Separate fault trees must be used for a given system for each set of boundary conditions. These separate fault trees can be produced from a single fault tree that includes the support systems and that, before being associated with a particular sequence, is ‘conditioned’ on the support system state associated with this sequence [18].

This approach generates large event trees that explicitly represent the existing dependences. Since they are associated with smaller fault trees (i.e. front line systems without support systems) they are less demanding in terms of computer resources and code sophistication. However, the complexity of the event trees increases rapidly with the number of support systems and the number of support system states that are explicitly depicted in the tree. Furthermore, since computer codes for automated quantification of these trees are not readily available, the quantification process is more cumbersome and subject to possible omissions. An additional consideration is that the large event tree approach, in particular if impact vectors are defined [5], does not explicitly identify what specific combinations of support system failures lead to front line system failures.

4.1.2. Cause consequence diagrams

A cause consequence diagram (CCD) is a logic diagram that follows the chronological and causal order of the events [5]. It can contain more information than an event tree because it allows for more complex branching than on the Yes/No logical operator allowed in the event trees. In relatively complicated cases CCDs usually result in more compact models because parallel branches can be grouped together by logic gates and treated as a single entity.

The compactness of CCDs compared with event trees also has its drawbacks. Grouping of the branches makes sequence by sequence review difficult and some dependences may be overlooked. During quantification, the CCD must be restructured into alternative, mutually exclusive branches (i.e. in effect to an event tree) in order to account for the dependences. Thus the use of CCD is typically limited to qualitative analysis, or as an intermediate modelling stage prior to event tree construction.

4.1.3. Event sequence diagrams

Event sequence analysis is a variation of cause consequence analysis and is discussed in subsection 3.4.3.2 of Ref. [5]. Event sequence diagrams (ESDs) are devel-
oped for each group of initiating events. The purpose of the ESDs is (as with the CCDs) to illustrate all possible success paths from a particular accident initiating event to a safe shutdown condition. The ESDs tend to include a significant amount of design and operational information and are used as intermediate steps prior to the construction of event trees.

4.1.4. Standard nomenclature

The accident sequences identified by a PSA codify the important findings and safety implications of a particular plant design. A standard nomenclature for representation of accident sequences will provide reviewers and users of PSA studies with a concise, clear, understandable and intercomparable representation of the important characteristics of different power plants. An attempt towards such a standardized nomenclature is presented in Appendix IV.

4.2. TASK 19: SYSTEM MODELLING

Prior to this task, the response of the plant to the initiating events has been modelled by one of the available event sequence modelling techniques. The resulting models contain, as elements, events that need further analysis into detailed constituents. The most usual element of an event sequence model is the failure or success of a system. The details of the events can be analysed through one of the available system models (i.e. fault trees, state space diagrams, reliability block diagrams, go charts). Fault tree analysis is the most widely used method for developing system models; the use of the other techniques is mainly reserved for special cases, as discussed in the following subsections.

Before any specific method is applied, a very good understanding of the system operation as well as the operation of its components and the effects of their failure on system success is necessary. Such knowledge and understanding can be achieved through a qualitative analysis, e.g. a failure modes and effects analysis (FMEA). An example of the format used for FMEA is given in Appendix V.

4.2.1. System fault trees

Fault tree analysis is the most common method used for representing the failure logic of plant systems. It is a deductive failure analysis which can be simply described as an analytical technique whereby an undesired state of a system is specified, and the system is then analysed in the context of its environment and operation to find all credible ways in which the undesired state could be brought about. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The
faults can be events that are associated with component hardware failures, human errors, maintenance or test unavailabilities or any other pertinent events that can lead to the undesired state. A fault tree thus depicts the logical interrelations of basic events that lead to the undesired event, which is the top event of the fault tree.

The general techniques for constructing, manipulating and quantifying fault trees are described in Ref. [19].

The following issues merit special consideration in the development of fault trees:

(1) Methods and procedures for the construction of fault trees should be agreed to at the beginning of a PSA and should be followed by all analysts. This is necessary in order to guarantee consistency of the analysis. Items to be considered in this context are: system boundaries, logic symbols, event coding and representation of human errors and common cause failures.

(2) All assumptions made in the process of constructing a fault tree should be documented together with the source (and revision number) of all design information used. In this way, consistency will be promoted throughout the analysis and traceability will be maintained.

(3) When systems are not modelled in detail and system level reliability data are used, failure events in common with other systems should be separated out and explicitly considered.

(4) Computerized methods should be used for handling the solution and quantification of fault trees to ensure consistency, comprehensiveness, efficiency and quality. Information on the available computer codes for fault tree analysis is provided in Ref. [20].

(5) It is strongly recommended that clear and precise definitions of system boundaries be established before the analysis begins. These definitions should be adhered to during the analysis and should be included in the final documentation covering systems modelling. The interface points between front line systems and various support systems could, for example, be located as follows:

- for electrical power supply, at the buses from which components considered within the system are fed;
- for actuation signals, at the appropriate output cabinets of the actuation system;
- for support systems providing various media (water, oil, air), at the main header line of the support system.

In cases where equipment or piping is shared between several systems, guidance with respect to proper establishment of boundary conditions is usually provided by system descriptions and drawings. This aspect should be carefully checked in order to avoid possible omissions and/or double counting.

(6) It is important that a standardized format be employed for coding basic events in the fault trees. Whichever scheme is used, it should be compatible with the
computer code selected for the systems analysis and also enable the basic
events to be clearly related to the following:
— component failure mode;
— specific component identification and type;
— specific system in which the component is located;
— plant codings for the components.
To prepare the system models for a concurrent or subsequent evaluation of
environmental effects, the system models will need to contain information on
component location and susceptibility to the environmental effects of interest,
e.g. earthquake, fire or flooding. It is strongly urged that information of this
type be encoded within the component name or provided on separate tables
correlating events with applicable information.
To assist the analysis of dependent failures (other than those caused by extreme
environments), the coding scheme should include information on location,
designation of generic type, and test and maintenance procedures.

(7) The fault trees should reflect all possible failure modes that may contribute to
the system’s unavailability. This should include contributions due to outages
for testing and maintenance. Human errors associated with failure to restore
equipment to its operable state following testing and maintenance and human
errors associated with accident response should also be included where
applicable. Considerations of potential operator recovery actions are often
specific to accident sequences and component failure modes and are best
treated as described in the accident sequence quantification task.

(8) The following aspects of dependent failures should be reflected in the fault
trees:
— interrelations between initiating events and system response;
— common support system faults affecting more than one front line system or
  component through functional dependences;
— human errors associated with common test and maintenance activities;
— components shared among front line systems.
Dependent events should be modelled explicitly and implicitly as reflected in
the following points:
(a) Multiple failure events for which a clear cause–effect relation can be
identified should be explicitly modelled in the system model: the root
cause events should be included in the system fault tree so that no further
special dependent failure model is necessary. This applies to multiple
failures caused by internal equipment failure (such as cascade failures
and functional unavailability events caused by components) and multiple
failures due to clearly identifiable human error (such as human error in
the steps of a prescribed procedure).
(b) Multiple failure events that are susceptible to dependences, and for which no clear root cause event can be identified, can be modelled using implicit methods such as the parametric models (see Appendix VI).

(c) Between the two previous extremes, there is a set of multiple failure events for which the explicit modelling of the cause, even if in principle feasible, is not performed because it would be too onerous; it is preferred to encapsulate the events in a parametric model. The decision to do this is taken by the analyst on the basis of experience and judgement, taking into consideration the aim and scope of the analysis. Moreover, explicit modelling may in some cases be impracticable because the component failure data do not allow different failure causes to be distinguished. Explicit modelling should in principle go as far as reasonable, depending on, among other things, the resources for the analysis and the level of detail. For the remaining dependences, at least an upper bound should be assessed and for this parametric modelling can be used. The analyst should clearly document what has gone into the parametric modelling and what has been modelled explicitly.

The sensitivity studies suggested in Section 6.5 include assessment of the systems’ potential vulnerability to dependent failures not implicitly or explicitly represented in the developed system models. Such failures may be associated with components which are (a) similar; (b) in the same room; (c) tested or maintained in the same way. Therefore, when basic events are being documented, the information supplied should include location, designation of generic type, indication of test or maintenance procedures in which the component itself is tested or maintained, and indication of test or maintenance procedures in which the component’s state is altered. Reference to these procedures (or summaries) should be included in the documentation.

(9) To permit proper quantification of accident sequences in which the initiating event may affect the operability of a responding system, the impact of initiating events (e.g. LOCA events, loss of off-site power) on the operability of the system should be explicitly included as appropriate in each system fault tree. In the small event tree/large fault tree approach, the impact of the initiating events may occur at the component level. Alternatively, the failure probabilities for basic events will be modified in order to take account of the impact of the particular initiating event. In the large event tree/small fault tree approach, the initiators may appear as boundary conditions on the top event.

(10) To simplify and reduce the size of the fault trees, certain events are often excluded owing to their low probability in comparison with other events. Examples of simplifying assumptions include the following:
— Flow diversion paths for fluid systems should be considered only if they could seriously degrade or fail the system (a general rule is that if the pipe
diameter of the diversion path is less than one third of the primary flow path, the diversion path may be ignored for failure to start).

— Spurious control faults for components after initial operation should be considered only if the component is expected to receive an additional signal during the course of the accident to readjust or change its operating state.

— Position faults prior to an accident are not included if the component receives an automatic signal to return to its operable state under accident conditions.

These examples are mentioned only as illustrations. Assumptions of this type must be justified in the PSA report.

(11) The testing procedures used in the plant must be closely examined to see whether they introduce potential failure modes. All such potential failure modes identified must be documented. An example of such a failure would be if in the course of testing, the flowpath through a valve is isolated, and at the end of the test the flowpath remains closed (possibly due to human error) and there is no indication that the flowpath is still closed.

(12) Trips of pumps and other safeguards intended to protect a component must be carefully identified. These can be a source of common mode failure. For example, spurious trips of auxiliary feedwater pumps on low suction pressure can lead to system failure if recovery does not occur.

(13) In a sequence in which some systems succeed while others fail, it is important to make the system failures correctly conditional on the other systems’ successes. Success trees may be used, but this method is not the only one; and it may be awkward. Certain advantages are offered by algorithms which operate on the top event simply by deleting cut sets that violate the system success specified in the sequence (see subsection 6.4.2).

The analyst should also examine all available information collated in the plant familiarization step (Section 3.1), which contains descriptions of all types of failures that have occurred at the plant being analysed and at similar plants, in order to gain a direct awareness of the potential for independent or dependent failures in the systems and of the potential for system interactions.

4.2.2. State space diagrams and Markov analysis

State space analysis, either with or without Markov process solutions, can be a very useful tool for modelling scenarios in which system states change cyclically with time. It may be used for availability estimations, particularly for systems subjected to periodic testing and maintenance as well as a failure and repair cycle.

The state space diagram is a logic model depicting the various states of a system and the paths along which the system can transfer from one state to another.
It is possible to represent a state space diagram by a set of simultaneous
differential equations representing the change with time of the probabilities of the
states. However, for a general case, it is not possible to obtain a closed analytical
solution to such a set of equations. Simulation techniques would have to be used. In
the case of systems with a failure, repair, test and maintenance cycle, it is possible
to make a special case by assuming that the transfers from state to state follow a
Markov process.

A Markov process is a process in which the probability that a system will trans-
fer from one particular state to another depends only on the initial and final states
of the transition. The assumption of a Markov process allows major simplification
of the simultaneous equations describing the state space diagrams. The terms of the
equations for each state in this case depend only on the state itself, the possible
immediately preceding and following states, and the rates of transfer between these
states. However, even these simpler equations may not be soluble in closed form if
the rates of transfer between states are time dependent functions. Solutions would
have to be found by iterative, numerical methods and the solution for each state
would be a function describing the variation with time of the probability of that state.

4.2.3. Reliability block diagrams

Reliability block diagrams show the logical relation among system components
in order to indicate which elements (blocks) of the system must operate successfully
for the system to perform its intended function.

Each block represents an individual component or a convenient grouping of
components of the system. The block diagrams consist of blocks in series, parallel,
series-parallel or in ‘m out of n’ configuration. Blocks representing redundant com-
ponents are shown in parallel. Individual components whose failure causes system
failure are placed in series. It is usually convenient to arrange blocks on a reliability
block diagram in the sequence in which their functions are performed.

The main disadvantages of reliability block diagrams are:

(a) it is difficult to model support systems adequately;
(b) causes of failure are not systematically identified (this is particularly relevant
for human errors and common cause failures (CCFs)).

4.2.4. Go chart

The go chart (GO) method [5, 21] is a success oriented systems analysis tech-
nique. The GO method parallels that of the CCDs and ESDs (see subsections 4.1.2
and 4.1.3) in that it follows an inductive success oriented logic.
A GO model represents the engineering function of a component, subsystem or system through a series of logic operators and symbols. It can generally be constructed from engineering drawings by replacing components (valves, switches, etc.) with one or more GO symbols, which are combined to represent system function and logic. A computer code has been developed that quantifies the model, calculates system reliability and availability and identifies fault sequences [21].

The main advantage of the GO model is that it is easily created from system engineering drawings and follows the normal flow path. It lacks, however, the inquisitive nature of the fault tree deductive logic which asks "How can it fail?". Thus it can only be used to evaluate failures that are implied by the simple logical structure of the system as conveyed by the engineering drawings.

4.3. TASK 20: HUMAN PERFORMANCE ANALYSIS

This task analyses the human performance that relates to the initiating events and subsequent system responses. Human acts covered by this analysis are all those identified during the course of model development as having a potential impact on the structure and output of the models. This section is based on a review of existing models used in PSA for human reliability analysis (HRA) and data requirements, conducted by the IAEA [22]. The treatment of human performance in a PSA is still evolving owing to the complexity of human behaviour and to a general lack of relevant data. There is a growing consensus, however, on the usefulness and applicability of certain techniques such as those described in Ref. [22] and in an IAEA report providing guidance on human reliability analysis [23]. As an example of such techniques and of how to integrate HRA into PSA, Section 4.3 outlines the systematic human action reliability procedure (SHARP) presented in Ref. [24].

4.3.1. Classification of human actions

Human interactions that can affect both the cause and the frequency of an event sequence can take place before, during or after the initiation of the event sequence and can either mitigate or exacerbate an accident. Accordingly, this can be, and has been in past PSAs, treated in different parts of the event sequencing modelling. On the basis of these considerations, the following classification scheme is possible:

**Type 1:** Before an initiating event, plant personnel can affect availability and safety by inadvertently disabling equipment during testing, maintenance or calibration.

**Type 2:** By committing some error, plant personnel can initiate an accident.

**Type 3:** By following procedures during the course of an accident, plant personnel can operate standby equipment that will terminate the accident.
Type 4: Plant personnel, in attempting to follow procedures, can make an error that exacerbates the situation or fails to terminate the accident.

Type 5: By improvising, plant personnel can restore and operate initially unavailable equipment to terminate the accident.

Type 1 interactions consist of testing and maintenance actions that degrade system availability. These factors are expressed as a probability of leaving components in an inoperable condition (e.g. misaligned valves). This source of unavailability is added to other contributions at the level of basic component inputs in the fault trees. Particularly important are actions that result in the concurrent failure of multiple trains of safety related systems and thus contribute to common cause failures. These events must be co-ordinated closely with the analysis of common cause failures to avoid double counting of multiple failures and to connect them properly to the logic structure of the fault tree.

Type 2 interactions are generally implicit in the selection of initiating events. An example of an initiating event caused by human actions is a plant trip following a mistake in a testing procedure. Such events can usually be found in the plant outage frequency database, but are not always identified as having specific human causes. Because of their identification with initiating events, they are accounted for by adding contributions to the initiating event frequencies or by assuming that such frequencies already contain human caused contributions. Most important are errors that not only precipitate an accident initiation but also concurrently cause systems related to safety to fail, either front line safety systems or support systems. There should be particular emphasis on such common cause initiators that are caused by human error.

Type 3 interactions concern success and failure in following procedures or rules known to the operators in response to an accident sequence. Type 3 interactions are incorporated explicitly into fault and/or event trees by the systems analysts.

Type 4 interactions are a special set of errors, usually of commission, that occur during Type 3 and 5 interactions and are the most difficult to identify and model. Only iterations between the human reliability analysts and the systems analysts can identify these interactions. One such type of interaction occurs when the operator mistakes the plant's actual state and takes actions appropriate to a different event. Another form of Type 4 action occurs when the operator correctly diagnoses the event, but chooses a non-optimal strategy for dealing with it. Only a few PSA studies have attempted to include this type of interaction, and even these only to a limited degree. Once the actions have been identified, they can usually be incorporated into an event tree. Very few data are available for predicting these types of human interactions; however, a retrospective analysis of actual events can usually identify those that have occurred.

Type 5 interactions consist of recovery actions, which are generally only included in accident sequences that dominate risk profiles. These actions may include
The general procedural steps in the human performance analysis into the PSA are those proposed by the human action reliability procedure or SHARP [24]. The responsibility for incorporating human interactions is shared between the systems analysts and the human reliability analysts. The systems analyst analysing human performance is expected to have some knowledge of models of human behaviour (including cognitive behaviour), although the emphasis is on knowledge of the system. The human reliability analyst is expected to have some knowledge of human reliability analysis methods and nuclear power plant operations, and to bring specialized knowledge of the plant and the system to bear. Additional review and discussion with operator training personnel is recommended. Quite often input will be needed from human factors experts in assessing human performance and human reliability analysis methods. The systems analyst and the human reliability analyst also need to have some knowledge of the system and the plant and plant operations.

Each of the five types of event described in subsection 4.3.1 can be included in the PSA through seven procedural tasks as proposed in Ref. [24]. These tasks are:

- Category A (Type 1) actions concerning errors made before an accident sequence has begun.
- Category B (Type 2) actions that cause initiating events and especially those that concurrently fail safety related systems.
- Category C (Types 3, 4 and 5) actions that concern response to an accident sequence.
- Category D (Type 6) actions concerning errors made after an accident sequence.
- Category E (Type 7) actions concerning errors made during an accident sequence.

The human factors team should include full time members from the control room operations personnel. This person is a key member and should have up to date knowledge of the plant and plant operations and in making judgements on human factor aspects of recovery. The team should provide assistance in structuring interviews with operations personnel and in making judgements on human factor aspects of recovery.
briefly presented here for convenience, although they belong to different major procedural tasks of the PSA.

The goals for each step are as follows:

1. **Definition:** To ensure that all candidate human interactions of the different types are adequately considered in the study.

   This first task is actually the preliminary phase of Task 20, in which the identified human errors of the various types are included in the appropriate event sequence and system models.

2. **Screening:** To identify the human interactions that are potentially significant to the safety of the plant.

   Screening helps in concentrating efforts on the key interactions and in the prevention of waste of resources for the analysis. There can be two kinds of screening: (1) qualitative judgemental screening, and (2) quantitative screening. The first is done at the stage of event sequence and/or system model development, where it can be judged that the effect of a particular human error on the model is not going to be significant. The second type of screening is done during the preliminary quantification of accident sequences (see Task 28 in Section 6.2). Human errors that contribute significantly to the frequency of core damage are then studied further as part of the second phase of the human performance analysis.

3. **Qualitative analysis:** To develop a detailed description of important human interactions by defining the key factors necessary to complete the modelling.

4. **Representation:** To select and construct the most appropriate logic representations (models) to describe the important human interactions.

5. **Impact/integration:** To adjust (if necessary) the event sequences and system models into potentially new impacts on the system responses, introduced (or identified) by the detailed qualitative analysis and the representational modelling of human actions.

6. **Quantification:** To apply appropriate data or other quantification methods in the assignment of probabilities to the various human actions considered. Also to determine sensitivities and to establish uncertainty ranges.

   This step, together with representation, forms Task 26 (Section 5.5).

7. **Documentation:** To include all the necessary information for the assessment to be traceable, understandable and reproducible. Guidelines are included in the major procedural step of the documentation of PSA presented in Section 7.

   Details on these steps are given in Ref. [23].
4.4. TASK 21: QUALITATIVE DEPENDENCE ANALYSIS

Dependence analysis is treated separately in this report in order to give the subject special emphasis, not because it is to be performed separately from event sequence analysis and systems analysis. Indeed, identification of dependences is the essence of the event trees, fault tree and other subtasks of event modelling development.

Qualitative analysis oriented towards the recognition of dependent failures can in itself be valuable for yielding insight into the strong and weak points of system design and operation.

Qualitative analysis allows one to make a judgement on the quality of the defences against dependent events built into the plant.

All the identified dependences should be listed separately and reported according to the reporting requirements of Section 7. These dependences should also be properly included in the logic models (see Section 6) in order to evaluate correctly their impact on the level of risk.

Dependences should be identified as follows (note: in the following definitions, the term ‘device’ is used in a generic sense to mean system, train, subsystem or component):

Type 1. *Functional dependences.* Dependences among devices due to the sharing of hardware or to a process coupling. Shared hardware refers to the dependence of multiple devices on the same equipment. In process coupling, the function of one device depends directly or indirectly on the function of another. A direct dependence exists when the output of one device constitutes an input to another. An indirect dependence exists when the functional requirements of one device depend on the state of another. Possible direct process coupling between devices include electrical, hydraulic, pneumatic and mechanical connections.

Type 2. *Physical dependences.* There are two types of physical dependence:

— those dependences causing an initiating event and also possibly failure of plant mitigating systems due to the same influence, e.g. external hazards, internal events. Such events are certain transients, earthquakes, fires and floods, etc. They require special treatment and are discussed in Ref. [2].

— those dependences which increase the probability of multiple system failures. Often they are associated with extreme environmental stresses created by the failure of one or more systems after an initiating event or by the initiating event directly. Examples are fluid jets and environmental effects caused by LOCAs or, for a Level 2 PSA, interactions of the core melt with structural components within the containment.
It should be emphasized that proximity is not the only 'environmental' coupling inducing physical dependence. A ventilation duct, for example, might create an environmental coupling among devices located in seemingly decoupled locations. Radiation coupling and electromagnetic coupling are two other forms not directly associated with a common spatial domain.

Type 3. Human interaction dependences. Two types of dependence introduced by human actions can be distinguished: those based on cognitive behavioural processes and those based on procedural behavioural processes (see also Section 4.3). Cognitive human errors can result in multiple faults once an event has been initiated. Dependences due to procedural human errors include multiple maintenance errors that result in dependent faults with effects that may not be immediately apparent (e.g. miscalibration of redundant components).

Common cause failures (CCFs), as the term is used in PSAs, represent all dependences that are not explicitly modelled in the event sequence and system models, i.e. they are the residual dependences. Common cause failures can therefore belong to any of the aforementioned types.

The present report recommends the inclusion of CCF contributions in the fault tree model whenever feasible. This should be done in an explicit manner in the logical models to the highest degree possible. Care must be taken in order to ensure no overlapping between the explicit and implicit modelling.

Common cause failure contributions incorporated into the fault trees in the early stages of fault tree development are usually limited to representing intrasystem dependences between redundant active components such as air operated and motor operated valves, pumps, diesel generators and different types of electrical equipment (e.g. relays, logic channels). The appropriate degree of coverage is, however, application dependent.

In addition, the present report proposes the use of sensitivity analysis for the selection of additional groups of components susceptible to common cause failures and for identification of CCF contributors with potentially significant impacts on the results. This means that accident sequences are searched for additional groups of components that might be subject to common cause failure. For all CCF contributions a rather conservative joint probability of failure is assumed and the effect on the probability of core damage is assessed. If this impact is substantial, then a more careful and detailed common cause failure analysis is performed. In practice, the impact of CCF contributions might be obvious in several cases and it would not be necessary to follow this procedure with respect to all steps; that is, a complete quantification of all sequences using conservative values is not always necessary to reach definite conclusions. Appendix VI presents an example of a detailed common cause failure procedure. References [26–30] present results of comparative analyses and
significant insights. Further guidance concerning CCF analysis may be found in an IAEA report on procedures for the treatment of CCFs [31].

The task of CCF analysis that conceptually and methodologically belongs in the qualitative dependence analysis is that of qualitative screening (see Appendix VI). In this step, a search is made for common attributes of components and mechanisms of failure that could lead to common cause events. This is an important task not only because it is required for the CCF, but also because the identification at this stage of the important attributes and mechanisms that could lead to CCF will allow the proper development of the logic models for the system so that the identification of CCF suspect groups of components will later be possible without restructuring the logic models (e.g. by proper basic event name coding or by inclusion of special basic events).

The objectives of the qualitative dependent event analysis can be summarized as follows:

(1) To gain an understanding of the mechanisms and factors that might determine dependence between systems or between the components of the system.

(2) To identify the important potential dependent failure events; this includes:
   (a) identifying failure events that might lead to the unavailability of multiple functions and delineating the systems and/or components that are effected by these events (Type 1 dependences);
   (b) identifying the root cause events and cause–effect chains leading to cascade failures and identifying the devices that are affected by the different root cause events (Type 1 and 2 dependences);
   (c) assessing the potential for human errors associated with test and maintenance or operation to affect two or more devices and identifying such equipment groups (Type 3 dependences);
   (d) delineating domains or combinations of components (common cause groups) which are important in terms of their likelihood of experiencing other kinds of CCF;
   (e) assessing the effectiveness of the defences built in to prevent dependent failures or to limit their likelihood.

(3) To rank the potential dependent failure events or to perform some screening in order to identify the most important ones. This is necessary since the list of potential dependent failures can be very long and will need to be shortened before proceeding to quantitative analysis. The screening can be based on qualitative or quantitative criteria.

(4) To provide an input for the screening of the raw data, to select those relevant to the subject plant and to use them in subsequent quantitative analysis.

The insights into system design and operation gained from the qualitative analysis must be reflected not only in the model used for the quantitative analysis but also in the quantification of the model.
Points 1 and 2 may be the only objectives if the qualitative analysis is carried out for the identification of potential dependent failures and for designing defences against them.

In order to assess the residual risk after having built in a certain number of defences, a quantitative analysis might follow. Methods for performing quantitative dependent event analysis are presented in Ref. [27].

4.5. TASK 22: IMPACT OF PHYSICAL PROCESSES ON DEVELOPMENT OF LOGIC MODELS

The purpose of Section 4.5 is to give recognition to physical processes and phenomena which should be incorporated into the development of accident sequences leading to core damage. These arise from initiating events that lead to alterations in environments that affect the performance of the required systems.

In order to incorporate correctly the effects of physical phenomena on the accident sequences leading to core damage, the operability of the active containment systems may need to be assessed. The accident sequences must therefore be extended to include the state of these active containment systems. Physical phenomena occurring after core melt are not studied in a Level 1 PSA, but it is important to include in such a study the effect of accidental environmental conditions on the engineering safety features and their support systems. The ability of the relevant pieces of equipment to withstand accident conditions must therefore be assessed even in a Level 1 PSA.

Following are some examples of situations in which environmental changes that are unfavourable to the performance of the essential systems (for LWRs) may occur:

(1) The potential for containment failure prior to core damage should be dealt with. A sudden depressurization of the containment building during an accident could lead to vaporization of recirculation water and potential pump cavitation and damage. It should be assumed that pumps will not be operable after such an event unless analysis demonstrates operability under these conditions.

(2) An assessment should be made of the effect of blowdown forces associated with a LOCA on equipment survivability and containment integrity. The temperature and pressure of the containment atmosphere should be assessed in a manner consistent with the operability of containment safeguards for the particular accident initiator. For example, for station blackout sequences, if the containment safeguards require AC power, the analysis should be performed under the conditions that arise with no containment safeguards. Particular care should be taken of accident conditions that affect active containment systems and corresponding support systems.
(3) Transients which may directly lead to the violation of the reactor coolant system pressure boundary should be identified. For example, an assessment should be made of system failures and/or conditions that could lead to vessel failure by pressurized thermal shock. Similarly, initiators that could lead to steam generator tube rupture events should be examined. In addition, the possibility of breaching the reactor coolant pressure boundary of a pressurized water reactor (PWR) following a range of anticipated transient without scram (ATWS) conditions should be considered.

4.6. TASK 23: CLASSIFICATION OF ACCIDENT SEQUENCES INTO PLANT DAMAGE STATES

The purpose of this Task is to assign event tree sequences to groups. In particular, if a Level 1 study is going to be extended to examine in-plant and ex-plant consequences of core damage events, it will be necessary to group accident sequences into plant damage states in order to consider the common impact on the containment. A summary of constraints or demands that an extension of the Level 1 PSA to Level 2 and Level 3 PSAs imposes on the Level 1 PSA is given in Appendix VII. To do this, the core damage accident sequences are characterized according to the general physical plant state to which each accident sequence leads. As a practical matter, it is extremely useful to group together those sequences whose states are sufficiently alike to justify Level 2 PSA analysis of the sequences together as a group.

The grouping of sequences into plant damage states is important for another reason also. Unless such a grouping is performed prior to the screening analysis for quantification of the accident sequences (see Section 6), some important sequences from the point of view of risk might be discarded as having a low frequency. Once the grouping is performed, however, the screening will be contained within the sequences of each plant damage state.

Input to this task includes the event sequences identified in Task 18 (Section 4.1). Also, information from other sources (e.g. from previous PSAs for similar plants) should be useful in constructing the plant damage states and for their assignment to release categories.

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

— initiating events (e.g. LOCAs, transients);
— failure of safety systems designed to cope with the initiating event (e.g. reactor protection system, emergency core cooling system (ECCS), containment systems).

For a particular reactor type (i.e. having a common vendor, of the same containment type, having the same special design features), these functions can be trans-
lated into suitable system failure and success descriptors. For example, containment safeguards, sprays, fan coolers, ice inventory and suppression pool subcooling should be considered as system decompositions. The following specific considerations may aid the analyst in defining plant damage states:

1. early core damage versus late core damage (relative to time of scram);
2. containment failed prior to or after core damage (both structural failure and isolation failure should be considered);
3. containment bypass (those sequences of interfacing system LOCA type);
4. LOCA with or without pressure suppression (boiling water reactors (BWRs));
5. pool subcooled or saturated when core damage occurs (BWRs);
6. vessel pressure when core slump occurs;
7. availability of containment sprays;
8. availability of containment heat removal;
9. availability of AC power and recovery times;
10. condition of reactor at vessel failure (water flooded or dry).

5. DATA ASSESSMENT AND PARAMETER ESTIMATION

The fourth major procedural step aims at acquiring and generating all information necessary for the quantification of the model constructed during the third step. Because inadequacy of the available data may affect the model, an iteration between the third and the fourth step may be needed.

The tasks of this step include the following considerations: identification of the various models that describe the stochastic nature of certain phenomena related to the events of interest and the corresponding parameters that need to be estimated; determination of the nature and sources of relevant data; and compilation and evaluation of the data to produce the necessary parameter estimations and associated uncertainties.

Three tasks (Tasks 24, 25 and 26) can be distinguished for this procedural step. A schematic representation of these tasks is given in Fig. 5.

5.1. COMMON PROCEDURES FOR PARAMETER ASSESSMENT

The procedural steps of data assessment and parameter estimation are concerned with the analysis of three major categories of data.

1. initiating event data;
2. component failure, repair, test, maintenance and common cause failure data;
3. human error data.
FIG. 5. Procedural steps for data assessment and quantifications of parameters and accident sequences.
For each of these major categories the following common subtasks are distinguished:

(1) event definition;
(2) model and parameter selection;
(3) identification of data sources and data gathering;
(4) selection and application of the estimation technique.

In Subtask 1, the analyst becomes familiar with the particular event of interest and establishes appropriate lines of communication and interfaces with the analysts of the relevant subtasks both in the accident sequence definition step (Section 4) and in the quantification step (Section 6).

In Subtask 2, the models that describe the stochastic behaviour of events of interest are selected by reviewing the models which: (1) are employed in the accident sequence modelling step (Section 4); (2) are appropriate to the quantification step (Section 6); and (3) are obtained by making appropriate assumptions consistent with the available data (interaction with Subtask 3).

In Subtask 3, the sources of appropriate data to estimate the parameters of the models as specified here are established and the data are collected.

In Subtask 4, the estimation techniques are applied and the parameters to be derived from the collected data are estimated together with their uncertainties.

Depending on the availability of plant specific ‘raw data’, two principally different situations with regard to Subtasks 3 and 4 are encountered:

— If raw data, for example the number of failures and the total exposure times for components, are available from the plant under consideration or from similar plants, these data are compiled in Subtask 3 and evaluated in Subtask 4 using appropriate models and estimation techniques. By this procedure, plant specific parameters are obtained.
— Previously compiled lists of parameters can be used when no raw data are available. Since these catalogues of parameters are often based on data from different plants, they are also called generic. In this case, Subtasks 3 and 4 consist of acquiring the generic ‘database’ and understanding the definitions, assumptions and methods used in generating it. Point values and associated uncertainties are also obtained from the generic database (see subsection 5.3.5).

5.2. TASK 24: ASSESSMENT OF THE FREQUENCY OF INITIATING EVENTS

5.2.1. Definition of initiating events

The task of quantifying initiating events starts with the outputs of Tasks 13 and 17, listing and grouping the initiating events. Typically, grouping of the individual
transients is based on the expected plant response. Each group includes a number of transients with similar event sequence responses. To complete this step successfully, it is very important that the rationale for a particular grouping of transients is clearly stated. Understanding of the grouping principles is especially important for the correct classification of transients that are found in plant records with a description differing from the original listing of initiating events. For example, in a plant that has instrumentation which trips the main feedwater pumps in the event of a high water level in any steam generator, such events may be listed as reactor trips due to high steam generator level. These trips are important, however, for the quantification of the loss of feedwater transient, since they result in such a condition. A strong liaison with the group that developed the initiating event grouping is therefore required during this task.

5.2.2. Model and parameter selection

Most PSAs performed to date have assumed that the frequency of initiating events is constant with time, i.e. that the events occur randomly in time, and that the distribution of times between occurrences is exponential. The parameter to be estimated therefore is the intensity $\lambda$ of this process.

Although this model was used in the vast majority of PSAs performed, there are two situations for which the assumption of constant frequency might not be valid:

1. For a relatively new plant, 'teething troubles' may influence the rate of occurrence of a particular initiating event. Usually this type of failure is eliminated during the first one or two years of plant operation, which results in a decreasing rate of occurrence during this period. A similar trend occurs for incidents initiated by plant personnel. This phenomenon is caused by the learning process undergone by personnel during the first years of plant operation. This situation is further complicated by the fact that mitigating systems might also have higher unavailabilities in early plant life.

2. Where the initiating event occurs as the result of failures of redundant equipment, it can be shown that the frequency of occurrence of the initiating event is time dependent. For this type of initiating event, the related frequency is not estimated on the basis of the occurrence of the event itself, but is viewed as that of a composite event. The frequency of this composite event is calculated from the frequencies of the simpler events that compose it. Even if the frequency of occurrence of the simpler event is constant with time, the frequency of the composite event is usually not. The loss of condensate is an example of such an event, since condensate systems are usually equipped with redundant condensate pumps.

A possible approach to dealing with time dependent situations is to calculate the probability of occurrence of the initiating event within an appropriate time frame.
and then to estimate the constant frequency (rate) that yields the same probability of occurrence. Although this approach is not exact, it constitutes a practical alternative to a time dependent analysis or to an approach in which the first two or three years of plant operation are considered separately.

As an alternative way of defining and quantifying initiating events, logic models such as fault trees or Markov models are sometimes used. Fault trees with the initiating event as the top event are useful for the identification of possible dependencies among the initiating events and mitigating systems. In this case, these fault trees can also be used for the calculation of the frequency of occurrence of the top (initiating) event.

5.2.3. Data source identification and data gathering

The data required for quantification of the models that yield the frequencies of initiating events are the numbers of occurrences of the events and the total periods over which these events have been observed. Sources of such data are the plant log books, in which ‘significant occurrences’ are recorded, and licensee event records.

If a plant specific assessment is not attempted, then the frequencies are taken from appropriate ‘generic’ lists or ‘databases’ (see for example Ref. [32]).

5.2.4. Estimation techniques and application

Maximum likelihood estimations or Bayesian techniques can be applied. Appendix H of Ref. [3] provides details of a composite Bayesian technique that allows for population variability. This technique is based on a more complicated model that estimates constant frequencies of occurrence by combining data from several plants, while taking into account the differences between the plants.

5.3. TASK 25a: ASSESSMENT OF COMPONENT RELIABILITY

5.3.1. Definition of basic events

Component data analysis has as its objective the modelling of component failure, component repair, and component testing and maintenance. The definition of what constitutes a component failure requires the specification of some attributes of components. This specification delineates the component boundary assumed (e.g. command faults are not included) and defines the mode of failure. The mode of failure is given as an undesirable state of component performance (e.g. a closed motor valve does not open when required owing to a mechanical failure of the valve prior to the demand).
Component repair and component testing and maintenance are analysed for how often and for how long they render a component inoperable for the plant operating state under investigation (see Section 2 concerning plant operating states). The investigations concern which component or components are affected and whether the action occurs on-line or off-line. On-line repair, testing and maintenance are of primary concern in calculating probabilities of accidents that can occur during power plant operation. However, leaving equipment in a failed or unavailable state following off-line testing or maintenance also has to be accounted for. The off-line activities can be important if failure probabilities are to be estimated for other modes of operation.

5.3.2. Model and parameter selection

The models of interest in this subtask are those describing the stochastic failure behaviour of components of the various systems. In general these models estimate the probability that a component will not perform its intended function and they depend on the mode of operation of the system to which the components belong. One set of such models is described in the following.

5.3.2.1. Standby systems

The major reliability measure of interest for standby systems is their unavailability on demand. It is presently assumed that the unavailability of a standby system can be reasonably approximated by the use of fault trees (or some other logic model) in which the component time averaged unavailabilities are used as the probabilities of the basic events.

The component time averaged unavailabilities are derived on the assumption that the failure of a component is a time dependent phenomenon and that the time to failure during the standby period is a random variable distributed according to a certain distribution (usually exponential). The unavailability of these components is a function of the standby time. If the component is tested periodically, the unavailability becomes a periodic function of time. To reduce the burden of calculation, the time dependent unavailabilities of the components may be substituted in some logic models by their average values over the period of the analysis. This assumption allows the component unavailabilities to be considered as 'constant' in the models.

If the component is periodically tested, then the average unavailability during the period of analysis is the average unavailability during the period between tests. Obviously, the value of this average ('constant') unavailability depends on, among other things, the period of testing.

An alternative model that has been proposed for components during the standby period is that of constant unavailability or constant failure probability per demand. This model assumes that the failure of the component is only caused by
immediate influences related to the demand. The unavailability does not change with
time nor is it affected by tests or actual demands. In fact, tests should be avoided
if this model holds.

The failure mechanism of most components includes elements of a time depen-
dent process and elements of a demand related process. The fractional influence of
each is, however, difficult to assess. Moreover, if this dual aspect is introduced in
the modelling, very specific data are needed. Studies have not supported such
analyses. It is therefore recommended that a time dependent model be used which
can include, where quantified on the basis of real data, both time dependent
influences and indirectly demand related features. The time dependent feature allows
for the inclusion in the model of the influence of the frequency of periodic testing.

A word of caution is warranted here regarding the use of ‘generic’ databases
or published plant specific databases that quote constant unavailabilities as ‘failures
per demand’. Often these values are the average unavailabilities calculated on the
basis of a particular test frequency and with a time dependent failure model. If these
values are to be utilized as failure probabilities in an application, care should be taken
to ascertain that the frequency of testing of the components in the new application
is comparable with that implicitly or explicitly assumed for the components that
provided the value in the database. Otherwise, significant overestimations or
underestimations of the component unavailability might result.

Depending on how a component is tested, we can distinguish three types of
components of standby systems:

(1) **Periodically tested standby components.** These components are usually in
standby mode and are tested periodically. If they are found to have failed in
a test, they are repaired. In addition, the components may be subject to
periodic scheduled maintenance. For these components there are five kinds of
contributions to the component unavailability: hardware failure; unavailability
due to testing; unavailability due to unscheduled repair; unavailability due to
scheduled and unscheduled maintenance; and unavailability due to interfacing
maintenance. The expressions for these unavailabilities are given in Table XI.
The parameters that must be estimated from data are the standby failure
rate, the mean time to repair (unscheduled repairs), and the mean time of
on-line maintenance actions. The estimation techniques are described in
subsection 5.3.4.

(2) **Untested standby components.** If a standby component is not tested, then the
averaged unavailability is given by the formula presented in Table XI. In this
formula, the fault exposure time $T_p$ (the time during which a failure can occur
and the state of the component are unknown) is set equal to the life of the plant
(40 years). However, it often happens that the component is indirectly tested
or renewed. For example, if the system to which the component belongs is
called upon to operate, the state of the untested component might be detectable
<table>
<thead>
<tr>
<th>Component type/ unavailability mode</th>
<th>Time averaged unavailability expression</th>
<th>Parameter definition</th>
<th>Data requirements for parameter estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Tested stand-by components</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1. Hardware failure</td>
<td>$1 - \frac{1 - e^{-\lambda_s T}}{\lambda_s T}$</td>
<td>$\lambda_s$: Stand-by failure rate</td>
<td>Number of observed failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$T$: Component test period</td>
<td></td>
</tr>
<tr>
<td>1.2. Test outage</td>
<td>$\frac{\tau}{T} q_0$</td>
<td>$\tau$: Average test duration</td>
<td>Total component stand-by time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$q_0$: Override unavailability (if applicable) obtained from system analysis</td>
<td>Observed test durations</td>
</tr>
<tr>
<td>1.3. Repair outage</td>
<td>$\lambda_s T_R$</td>
<td>$T_R$: Mean time to repair</td>
<td>$T_R$, $T_m$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$f_m$: Scheduled maintenance frequency (includes interface maintenance)</td>
<td>Observed individual times for repair and maintenance, respectively, including detection and waiting time</td>
</tr>
<tr>
<td>1.4. Scheduled maintenance</td>
<td>$f_m T_m$</td>
<td>$T_m$: Mean time of scheduled maintenance action</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>$\lambda_s$: Stand-by failure rate</td>
<td>$T_p$</td>
</tr>
<tr>
<td>2. Untested standby component</td>
<td>$1 - \frac{1 - e^{-\lambda_s T_p}}{\lambda_s T_p}$</td>
<td>$T_p$: Fault exposure time</td>
<td>Inferred from replacement times of component due to other failures or if not replaced, then assume</td>
</tr>
<tr>
<td>3. Monitored standby component</td>
<td>$\frac{\lambda_s T_R}{1 + \lambda_s T_R}$</td>
<td>$T_R$: Mean waiting time plus repair time</td>
<td>$T_p = 40$ years</td>
</tr>
</tbody>
</table>

*From Table 5.5 of Ref. [3].
(operating or failed) when the system is demanded. In this case the mean fault exposure time for the untested component is the mean time to challenge the system to which it belongs. In other cases the component might be replaced every time some other tested component is replaced. In this case the mean fault exposure time is approximately equal to the mean time to failure of the tested component. Additional information on this subject is given in subsection 5.3.1.1 of Ref. [5].

(3) **Continuously monitored components.** Some components, although they belong to standby systems, are continuously monitored. This is equivalent to assuming that a failure is detectable as soon as it occurs. The formula for the averaged unavailability for such components is given in Table XI.

### 5.3.2.2. Operating systems

For operating systems, the reliability characteristic of interest is generally the probability that the system will fail to operate successfully for a given period of time $T_M$ (the mission time). It is assumed that the failure probability of an operating system can be approximated by the use of fault trees or some other appropriate logic model with which the component failure probabilities up to the time $T_M$ are used for the basic events. The failures of operating components are assumed again to follow an exponential distribution with an operating failure rate $\lambda_o$ instead of a standby rate. Operating systems contain two general types of components: non-repairable components and repairable components.

(a) **Non-repairable components.** The parameter $\lambda_o$ (operating failure rate) is estimated in a completely analogous way to that for the other failure rates mentioned earlier (Table XII).

(b) **Repairable components.** Care must be exercised when calculating the unavailability formula quoted for repairable components. The word ‘repairable’ in this context means ‘repairable without taking the total system out of service’. Thus unless there is a redundant component, and unless the failed component is accessible for repair with the system operational, the component should be treated as non-repairable. Failure to observe these conditions results in significant underestimation of system failure probabilities (Table XII).

### 5.3.2.3. Standby systems in operating mode after startup

Standby systems are usually required to operate for a required mission time after successful startup. For this operating phase, the systems can be handled analogously to operating systems as described in subsection 5.3.2.2. In principle, the systems can be regarded as repairable, provided that the conditions on repairability of operating systems mentioned earlier are fulfilled. However, as a usually accepted
TABLE XII. COMPONENT UNAVAILABILITY EXPRESSIONS FOR ON-LINE SYSTEMS

<table>
<thead>
<tr>
<th>Component type/unavailability mode</th>
<th>Time averaged unavailability expression</th>
<th>Parameter definition</th>
<th>Data requirements for parameter estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Non-repairable component</td>
<td>$1 - e^{-\lambda_o T_M}$</td>
<td>$\lambda_o$: Operating failure rate</td>
<td>$\lambda_o$: Number of observed failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$T_M$: Mission time (obtained from success requirement)</td>
<td>$T_M$: Total time to failure</td>
</tr>
<tr>
<td>2. On-line repairable component</td>
<td>$\frac{\lambda_o T_R}{1 + \lambda_o T_R}$</td>
<td>$T_R$: Mean time to repair</td>
<td>$T_R$: Observed individual times for repair</td>
</tr>
</tbody>
</table>

*From Table 5.6 of Ref. [3].
conservative simplification, the systems are considered in many cases to be non-repairable for the following reasons:

— the repair times for the given accident situation are comparable with the mission time;
— the unavailability contribution from the operating phase is small compared with the contributions due to failures during the standby phase.

### TABLE XIII. PLANT SPECIFIC DATA SOURCES

<table>
<thead>
<tr>
<th>General record type</th>
<th>Specific names</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Design drawings</td>
<td>P&amp;IDs, Process drawings, electrical drawings, fire zone drawings</td>
<td>Type, population, identification, location, and functional as well as physical interfaces of equipment in the plant</td>
</tr>
<tr>
<td>2. Operating records</td>
<td>Operator (control room) logs, monthly status reports, licensee event reports</td>
<td>Chronological reporting of events occurring during operation in various levels of detail and various reporting scopes</td>
</tr>
<tr>
<td>3. Plant systems specification</td>
<td>System identification list, system operability matrix</td>
<td>Identification of system names, functions and boundaries, and identification of which systems are operable during which plant modes</td>
</tr>
<tr>
<td>4. Equipment records</td>
<td>Equipment lists, parts lists</td>
<td>Type, population, functional name, and system assignment of each component</td>
</tr>
<tr>
<td>5. Maintenance records</td>
<td>Maintenance logs, maintenance work requests, maintenance requests, job orders</td>
<td>Date, name, type and identification of component and system requiring maintenance action, problem observed, and action taken</td>
</tr>
<tr>
<td>6. Test records</td>
<td>Periodic test reports, plant test procedures, plant test schedule, (master surveillance schedule)</td>
<td>Procedures, schedule, reporting of tests and identification of components requiring testing</td>
</tr>
<tr>
<td>7. Calibration records</td>
<td>Calibration reports, calibration cards, calibration procedures</td>
<td>Procedures, schedule, reporting of tests and identification of components requiring testing</td>
</tr>
</tbody>
</table>

* Table 5.3 of Ref. [3].
5.3.3. Plant specific data sources and data gathering

Although many nuclear power plants have established rather extensive collection systems for operating and maintenance data, and although some of these systems have been computerized since the plants began to operate, very few stations have data systems designed specifically for providing plant specific data for use in a PSA. The PSAs previously performed had to depend on a combination of sources of plant specific information for the construction of a plant specific database to support a PSA. These sources included plant design, operating and maintenance records and procedures that should be made available to the PSA data analysts. The names used to refer to these records differ from plant to plant, but a representative listing of record types and their contents is given in Table XIII.

The basic data to be collected from these records are summarized in Table XIV. Further descriptions of data collection activities and the data that can be extracted from plant records are given in Section 5 of Ref. [5].

5.3.4. Methods for estimation of plant specific parameters

The following subsections describe approaches for estimating component failure rates, failure probability on demand, mean times to repair, test frequencies, average test times, maintenance frequencies and average maintenance times from the plant specific data gathered in the previous subtask. Techniques are also given for estimating the parameters of a repair distribution for those applications for which the probability of failure to complete the repair in a given time period is required.
5.3.4.1. Component failure rate estimation

The parameter to be estimated is either the standby failure rate $\lambda_s$ or the operating failure rate $\lambda_o$ of the exponential distribution. The steps for estimating both these parameters are as follows:

1. Identify the component population whose failure history is to be used to estimate the assumed common component failure rate (i.e. components assumed to have the same failure rates).
2. Identify the time period during which the component failures are to be counted.
3. In the component population, count the total number of failures $N$ and the total component standby time $T$ (or total operating time for operating components) for the time period. Care should be taken to avoid counting preventive maintenance actions as catastrophic failures. This distinction is not always made in plant records.
4. Estimate the plant specific mean failure rate $\lambda$ as $\lambda = N/T$. From the Bayesian point of view this estimate is the mean of the posterior distribution of $\theta$ if a non-informative prior distribution is assumed. This estimate is also the maximum likelihood estimator of the parameter $\lambda$ of an exponential distribution.
5. For an assessment of the uncertainties, a Bayesian approach can be used in which an appropriate prior distribution is updated using the 'sufficient' information of Step 3 to provide a posterior distribution.

5.3.4.2. Repair time estimation

The average repair time $T_R$ is estimated as the sum of the observed repair times divided by the number of repair actions. The repair times should include detection plus waiting times. For reliable estimates, the number of observed repair times should be more than ten (see Ref. [3]). If there are fewer than ten samples, available generic values should be used.

If a repair time distribution is required, then as a crude model an exponential distribution for the time of repair can be used with the estimated mean repair time $T_R$ as the mean of the distribution. It is important to identify any delay time during which repair is unlikely to be performed because of the time required for detection and repair initiation. This delay time can have large effects and can compensate for the crudeness of the exponential model. The exponential density $f(t)$ for the repair time accounting for a delay time $t_0$ is

$$f(t) = \frac{1}{T_R} \exp[-(t-t_0)/T_R]$$

When $t_0$ is incorporated, then any wait or detection times do not need to be included in the estimation of $T_R$ used in the density $f(t)$. 

72
5.3.4.3. Test frequency estimation

The estimation of actual test frequency, or equivalently the actual average time between surveillance tests, can be made if testing is more frequent than specified in the technical specifications and it is desired that credit be taken for the extra testing. Some of the tests do not contribute to the component (system) unavailability, because during tests the component is in a safe state (e.g. operational). This has to be assessed on a case by case basis. Tests that occur during a reactor state for which the system is not required to operate should not be taken into account in assessing the unavailability due to testing.

5.3.4.4. Estimation of the average test duration

The test duration time needs to be estimated when the test causes the component to be unavailable. The average test duration time $\tau$ is estimated as the sum of the total test duration in a certain time period divided by the number of test operations. For reliable estimates the number of observed test durations should be more than ten; otherwise, generic data should be used. The test duration time is the time period from the moment the component was taken out of service to the moment it was returned to service. This information is usually available in plant log books.

5.3.4.5. Estimation of maintenance parameters

The estimations of maintenance frequency and maintenance duration are similar to those for test frequency and test duration. Depending on the type of maintenance (preventive or corrective) and the in-plant sources of information, it is important to stress that total component unavailability has to be taken into account only when the reactor is in a state that requires the system to be available.

5.3.5. Generic databases

Whenever plant specific data do not exist for estimating the parameters of the plant models, existing compiled lists of such parameters can be used. These lists are usually referred to as generic databases and could range from published plant specific lists of parameters to lists that were based on information from more than one plant and are called ‘generic’.

This subsection discusses the major characteristics, possible pitfalls and procedures for using these databases.
The amount of information included in the various databases varies and might contain some or all of the following:

1. component description;
2. failure mode;
3. failure rate (per hour) or failure per demand, expressed as mean or median values;
4. upper and lower bounds (if a distribution is being used), high and low values, maximum and minimum or other parameters defining a possible range of failure rates;
5. the error factor associated with the failure rate;
6. repair time (seldom found).

The first three are usually found in the data tables; the others very much depend on the source and on the method of acquiring data.

Existing databases can be divided into three broad categories:

1. Databases generated by expert opinion (single or aggregate). This expert opinion is based partly on actual operational data, but mainly on general or detailed knowledge of design, manufacturing, modes and environment of operation for the component. Typical examples of this category are the databases provided in Refs [3] and [15]. Databases of this type combine knowledge from several plants. Non-nuclear industry sources are also classified in this category.

2. Databases generated by aggregating the operating experience of a group of plants, usually done by extracting information about component failures from established plant event reporting systems. Data in databases of this type represent actual operating experience.

3. Databases generated from plant specific operating experience. Some of the plants for which PSA studies have been performed have a considerable operating experience, and a substantial amount of data on component failures has been collected.

If these data are used for a plant having close similarity, for example, a plant of a similar size, type, manufacturer and operating environment, this may be the best available database if no plant specific data are available.

To use any of the existing databases, either directly or as a basis to form a prior distribution for a Bayesian update using plant specific data, special attention should be given to component boundary and failure mode definitions.

There is no unique way of defining the component boundary in any one of the categories described. Most of the sources in the first category do not provide a precise definition of the component boundary. In some cases components are defined as ‘off the shelf’ items, having boundaries as when ordered from the manufacturer. Sometimes there is no definition at all, and, for example, it is not even known whether or not a valve includes control and actuation.
The second category is generally better defined than the first one, since it can be related to the actual component that experienced failure. If the reporting system itself does not have strict rules on defining components, however, misinterpretations may occur.

The third category generally has a clear definition of the component boundary, if an adequate data collection system exists at the plant. However, if the data have been extracted from log books or maintenance reports, misinterpretations are possible and inconsistent boundary definitions may be found.

Although it is not strictly related to component boundary definition, there is a potential problem in the attempt to use an existing database to assess reliability parameters for components of totally new design, or which significantly differ from the components described in the database. Examples are the totally new designs of pressure operated relief valves (PORVs), for which no data exist and all generic data seem not to be applicable. There is often a similar concern for pumps; there may be a wide range of pump sizes, but in generic databases there is often no distinction in the parameters for different pump sizes.

The situation is even more complex for failure mode definition. There is no widely accepted system for defining failure modes, although similarities exist. Existing databases sometimes provide definitions of failure modes, but usually no detailed information is available. Data sources for which the failure mode is not strictly defined should be used cautiously.

Most of the databases do not distinguish between operating failure rate and standby failure rate, which may lead to misinterpretation.

There is an important problem area in the usage of existing databases in attempting to combine different databases. If the component (including its boundaries and failure mode) is well defined, such a combination is possible. In most cases, however, there is little similarity in component definition, so the combination of data could lead to unacceptable results and generally is not recommended.

Furthermore, before combining several existing databases, it is important to assess their interdependence. Sometimes the same data source is used, or data have only been upgraded, which could result in highly interdependent databases. Treating the sources as independent could result in an overestimation of the existing uncertainty.

Typically, existing data sources include a wide range of mechanical, electrical and instrumentation and control equipment most frequently accounted for in PSA studies. The usual number of component types and failure modes found in data sources is in the range of 30–80. Most of the mechanical data are on pumps and valves. Electrical data cover transformers, switches, relays, instrumentation, equipment, transmitters and sensors. Diesel generators are sometimes treated as a separate group and are often included in the generic database.

The IAEA has completed a computerized compilation of generic reliability data [33].
5.4. TASK 25b: ASSESSMENT OF COMMON CAUSE FAILURE PROBABILITIES

This report proposes the performance of common cause failure (CCF) analysis for those groups of components that may be subject to such failures. An example of a more detailed CCF analysis is briefly described in Appendix IV; detailed procedures are given in Ref. [27]. Furthermore, Refs [26, 28 and 29] give results of comparative CCF calculations and important insights on the various models and the availability and use of data.

Common cause events are a subset of the more general class of dependent events whose causes are not normally explicitly modelled as basic events in the system logic models. In principle, the logic models can be developed further to include a larger number of basic events that correspond to common cause events. Each common cause basic event in such a logic model would be indicated as resulting in failure of two or more specific systems/components. One of the important tasks in a common cause event analysis is to define, unambiguously, the appropriate combination of explicit and implicit modelling techniques and the appropriate analysis of the data in support of those techniques to ensure adequate completeness. A clear understanding of the mechanisms by which dependent events occur is essential to performing this task. It is also necessary to categorize and interpret operational data to identify occurrences of the defined set of common cause events and to use the data to estimate the probability of common cause events for use in reliability and safety evaluations.

The tasks of CCF analyses that are relevant to this major procedural step are those of definition of the common cause basic events, the selection of probability models for these events, the data classification and screening and the estimation of the parameters. Ref. [27] further discusses these tasks.

5.5. TASK 26: ASSESSMENT OF HUMAN ERROR PROBABILITIES

The general approach described in Section 5.1 is in principle applicable in the assessment of human error probabilities.

The first two steps of event definition and model and parameter selection (see Section 5.1) are actually performed in conjunction with Task 20 (see subsection 4.3.2) after the screening of Task 28 has been completed. These models would require an estimation of success (or failure) probabilities for various tasks or actions. Ideally, data for estimating these probabilities (the third step in Section 5.1) would come from a large number of people performing the tasks. The estimation technique (the fourth step in Section 5.1) could then vary from a classical estimator, equal to the ratio of number of errors to the number of attempts, to a Bayesian approach that included uncertainty assessment.

76
As of 1992, however, there is a paucity of actual data on human performance. Human error probability assessments must therefore be based on extrapolation from other sources of information combined with expert judgement, or on expert judgement alone.

Potential sources of data pertinent to the task of assessing human error probabilities are given in Section 5 of Ref. [22] and in the IAEA publication Procedure for Conducting Human Reliability Analysis in Probabilistic Safety Assessment [23].

There are, however, some generic databases for human error probabilities that can be used in the absence of other more pertinent and plant specific data. These, according to the types of human actions considered in the models of a PSA (see subsection 4.3.1), are as follows:

Type 1: Ref. [34] provides techniques for quantifying errors of this type.

Type 2: The frequency of the initiators that can be caused by this type of error include the contribution of human errors and hence special quantification is not required.

Type 3: For a planned response to an initiating event, time dependent response curves such as those proposed in Refs [23], [24] and [35].

Type 4: Expert judgement is the only available source at the present time.

Type 5: A generic procedure for quantifying recovery actions is given in subsection 6.3.1.

6. ACCIDENT SEQUENCE QUANTIFICATION

The fifth major procedural step includes all the tasks associated with the quantification of the accident sequences. The plant model built during the third major step is quantified using the parameters estimated in the fourth step. The tasks to be performed include the determination of the accident sequences to be quantified and the manipulation of the accident sequences. The manipulation uses the laws of Boolean algebra to put the sequences into a form suitable for quantification. The tasks also involve actual quantification of the sequences using point values and associated uncertainties. The relative importances of various contributors to the core damage frequency are determined and sensitivity studies are performed to evaluate the effects of modelling assumptions.

The discussion of this procedural step, particularly the quantification of accident sequences, is confined exclusively to the event tree/fault tree technique for
modelling event sequences and systems, respectively. If other techniques are used (i.e. Markov models for system modelling), other procedures should be used for basically the same fundamental issues. Given the relative paucity of applications of other models in complete PSAs, however, these models are not considered in the quantification step.

There are five tasks in this procedural step, shown in Fig. 5.

6.1. TASK 27: DETERMINATION OF ACCIDENT SEQUENCE BOOLEAN EQUATIONS

The determination of the Boolean equations for accident sequences requires the selection of the accident sequences to be quantified and the manipulation of the sequences to place them in a form suitable for quantification. The system models are also placed in a form that allows their quantification. The selection of accident sequences also requires screening out of sequences at the system level because of their low contributions in comparison with those of other sequences. This screening takes place at the system level within the same plant damage category. For example, assume accident sequence IABC has been quantified and IABDE is to be quantified. If it is known positively that DE has no dependences with IAB and has a much lower probability (e.g. two orders of magnitude) than C, then IABDE might not need to be quantified. Care must be taken in determining that no dependence exists.

In manipulating the event trees in the small event tree approach, the fault trees are combined with the event trees to produce accident sequence minimal cut sets. The accident sequence minimal cut sets contain the initiating event and primary events that result in the accident sequence. Dependences among initiating events, component failures and human errors need to be considered in this evaluation process.

The large event tree method essentially requires that the dependences among systems be treated and displayed on the event tree as part of the event tree construction process. The large fault tree linking method requires that the dependences be treated as part of a Boolean reduction process to obtain Boolean reduced equations for each event tree sequence.

In all cases, reduced Boolean equations are required for the sequence quantification process, and these equations must correctly reflect the various types of dependences between systems. The manipulation of the event trees and fault trees to obtain the minimal cut sets and the reduced Boolean equations is discussed in Ref. [5]. The difficulties associated with selecting the event trees and obtaining reduced Boolean expressions are generally associated with the proper treatment of dependences; the remainder of Section 6 deals with this important area.

When the large event tree method is used, it is important that no dependences are overlooked and that all are treated explicitly in the event tree. If there is a component common to two systems and this is not noted, then incorrect quantification will
result. It is not absolutely necessary that all dependences be explicitly displayed on the event tree. If two systems have a common component not displayed on the event tree, then fault tree linking can be used for these two systems. This is the approach used in the small event tree method.

There are several types of dependences that need to be explicitly considered. These dependences include:

1. Common cause initiating events which also cause failures in front line systems or support systems.
2. Single component faults that contribute to the failure of more than one system (shared individual faults).
3. Dependences caused by shared support system trains.
4. Dependences caused by support systems embedded in other support and front line systems.
5. Looping caused by mutual dependence of support systems on each other (dependence loops).
6. Dependences caused by the requirement to distinguish between early and late system failures.

These types of dependences can be treated by either the large event tree method or the large fault tree method. The treatment of dependences of Types 1, 2, 3, 4 and 5 is discussed in Ref. [5]. Subsection 6.1.1 discusses additional considerations in the treatment of Type 6 dependences.

6.1.1. Early versus late system failure

Sometimes accident consequences depend on whether a particular front line system fails early in the progress of an accident or later, after the accident has been partially mitigated. For these cases, it is necessary to differentiate between early and late failures of the systems. In some cases, the early failure of a system precludes any situation for which the system will be called upon later. This specific type of dependence is expressed on the event tree by not branching on late failure for those branches that include early failure of the same system. Support systems can also fail early or late, resulting in event tree sequence cut sets that can include both early and late failures of support systems. The early and late failures of support systems should be excluded from sequences where both early and late front line system failure is not possible. An accepted method of accomplishing this is to express the late failure of a support system as the Boolean product, ‘system fails late’ and ‘system succeeds early’. The reductions will then correctly account for combinations of early and late failure in this case. References [5] and [15] further discuss dependence and operational considerations in constructing event trees.
6.1.2. Treatment of system success in an accident sequence

In certain instances when the success of a system is included in the sequence of events that define an accident sequence, it is important to consider explicitly the success of this system in the Boolean reduction of the accident sequence to avoid an overestimation of its frequency. Such a situation arises, for example, when the system models for front line systems include the support systems (e.g. small event trees/large fault trees). In such a situation the success of a front line system implies the success of its support systems, which cannot be then considered as contributing to the failure of a different front line system in the same accident sequence. Similar situations arise in accident sequences that result in core damage because of containment failure. Such sequences assume that core damage has not occurred prior to the failure of containment and this in turn requires the success of a number of front line and support systems. The failure of the systems that induce the containment failure should therefore be conditional on the success of all the systems that can cause core damage directly.

Exact treatment of this problem requires the use of success models that correspond to the models that define the failure of the system. If fault trees are used, such an approach can result in very large (accident sequence) trees that, in addition, are non-coherent. Handling of large, non-coherent fault trees is a formidable task, however, and is generally beyond the capability of even the more advanced computer codes for fault trees. One way around this problem is the cut set matching technique, where two lists of cut sets are generated: (a) the accident sequence cut sets that correspond to the linked fault trees of the failed systems and (b) the cut sets of the fault trees of each and every system whose success is part of the accident sequence. These two lists are then compared and the cut sets of the first list (accident sequence cut sets) that contain a cut set that appears in the second list are eliminated. This is an approximation to the linking of fault and success trees but the error in most cases is insignificant.

6.1.3. Requirements for modularization

The complexity of the Boolean reduction process of the event trees increases geometrically with the number of terms (cut sets) in the individual fault trees making up the sequences. A process by which the complexity can be reduced is to define independent subtrees, or modules, which contain multiple primary faults. The Boolean equation for the fault tree is then written in terms of the individual subtrees rather than in terms of the primary events. Since each independent subtree in general consists of more than one primary event, the resulting Boolean equation in terms of subtrees will contain considerably fewer terms than the Boolean equation written in terms of primary events. Thus, modularization of fault trees using independent subtrees can significantly reduce the complexity of the Boolean reduction process.
The objective in the modularization process is to combine as many primary faults as possible into independent subtrees. This process must be performed with caution, however. Each subtree must be entirely independent of every other subtree in the same accident sequence. If a primary fault appears as a fault in more than one system, it is itself defined as an independent subtree. Collections of faults that appear in more than one system as independent subtrees must be given the same name in each system in which they appear. References [5, 10 and 15] further discuss modularization considerations.

6.1.4. Requirements for a Boolean reduction code

The process of Boolean reduction of all event tree sequences requires a significant effort. The Boolean reduction process is also a mechanical one which lends itself to a computerized solution. Several computer programs exist that are capable of accomplishing the Boolean reduction of fault trees and event tree sequences. A computer code is required for this process for the following reasons:

— Boolean reduction of fault trees and event tree sequences by hand requires inordinate amounts of time and resources.
— Boolean reduction by hand would generally increase considerably the chance of obtaining incorrect or incomplete cut sets.

It is emphasized that the requirement for defining independent subtrees remains and may be necessary even though a code will be used for the mechanics of the Boolean reduction process. All of the codes are limited by the number of terms that they can accept. The characteristics and availability of computer codes are detailed in Ref. [20]. A PSA code package (PSAPACK) developed by the IAEA for use with personal computers is described in Ref. [36].

6.1.5. Treatments of frequency of initiating events

The quantification of accident sequences requires incorporation of the frequency of the initiating event. For the small event tree/large fault tree method, the initiating event is a simple multiplier to each sequence on the event tree and no special manipulations need be done on the accident sequences. For the large event tree/small fault tree method, the accident sequences should be coalesced into those that would be used in the small event tree/large fault tree method for discussion and display purposes. It is important that the accident sequences be displayed in terms of the initiating event and combinations of front line system failures and successes, as well as in terms of the sequences which appear directly on the large event tree. The reader is referred to Refs [5] and [15] for further discussion.

In the event that fault tree analysis has been performed to obtain a frequency estimate for the initiating event, the fault tree for the initiating event can be incorpo-
rated into the analysis by linking it with all the other fault trees in the sequence paths. The Boolean manipulation to obtain the minimal cut sets is the same as for any other linked fault trees. The numerical quantification is different, however. The contributions to the minimal cut sets from the initiating event must be explicitly identified. These elements provide a frequency contribution to the quantification of each cut set. The frequency contribution must be quantified using the correct frequency equations. Many computer codes are not capable of calculating the frequency of occurrence of such cut sets, however, and care should be taken to use a suitable code.

6.2. TASK 28: INITIAL QUANTIFICATION OF THE ACCIDENT SEQUENCES

This task involves the initial quantification of the accident sequences. Screening values are used for the human errors identified in the event trees and fault trees. Human errors which contribute significantly to core damage frequency (‘important errors’) are then studied further as part of the human performance task; errors which do not contribute significantly are not considered to warrant further study. This procedure assumes, of course, an iterative execution of Tasks 28, 29 and 31. The list of errors considered and the output list of important errors should be documented together with a detailed statement of the criteria used for determining the important errors.

The primary events and the frequencies of the initiating events are initially quantified by using as point values the mean values of the distributions that quantify the associated uncertainties (see also Section 6.4). Where detailed data are not available, conservative values can be used for the primary event data or the initiating event frequencies. If the conservative values result in significant contributors, then they can be more precisely evaluated.

Preliminary point estimates of the frequencies of the accident sequences are calculated by multiplying the point value unavailability estimate of each event tree sequence by the point value frequency estimate for the corresponding initiator. The unavailability of the event tree sequence is estimated by summing the point value unavailabilities of the component level minimal cut sets for the sequence. Post-accident recovery, such as recovery of actuation faults or of pre-accident mis-positioning faults, is not credited at this stage.

In some applications, it may be convenient to perform this quantification concurrently with the sequence Boolean reduction. This is true particularly when the large fault tree method is used and a computer code is used to perform both the sequence Boolean reduction and sequence quantification.

An important subject is the review of cut sets generated by the Boolean reduction process, both at the system level and at the sequence level. The top level cut sets should be individually reviewed for engineering significance with respect to the plant system design in order to detect modelling errors.
6.2.1. Truncation

In order to make the sequence quantification practical, it is generally necessary to truncate the analysis; that is, to consider only those cut sets whose probability is above some cutoff, which is termed the truncation value. Truncation can be used both in the screening and in the final quantification.

Practice has shown that it is generally adequate to consider a truncation value that is smaller by a factor of 1000 than a dominant value that is obtained or a criterion value that is considered. Thus if a criterion value of $10^{-5}$ is to be demonstrated, a truncation value of $10^{-8}$ is generally adequate. As another example, if a cut set of $10^{-4}$ has been obtained then a truncation value of $10^{-7}$ is generally adequate. Reference [15] suggests a truncation value of $10^{-9}$ for sequence cut sets but it allows for greater values provided that sequences (cut sets) of the order of $10^{-6}$ per year are not neglected.

The factor of 1000 is not a guaranteed value and for special situations or special applications it may be necessary to use other truncation criteria. For example, for status monitoring applications where the PSA is used to evaluate the implications for the core damage frequency of one or more components given to be down, then lower truncation criteria will generally be needed.

It should be noted that if a truncation value has been adopted while using screening values for certain events (e.g. human error probabilities), a reassessment of the truncation value should be made in the final calculation when more exact values are used.

Care must also be taken if truncation is performed in a Level 2 or higher PSA study (or in a Level 1 PSA study that is to be expanded). In this case, a truncation value such as that given here will need to be separately applied to each of the different plant damage states.

6.3. TASK 29: FINAL QUANTIFICATION OF THE ACCIDENT SEQUENCES

This task consists of the requantification of accident sequences chosen in the previous stage, now using more accurate human error probabilities and data values. Unless particular accident sequences are negligible, or recovery is out of the question, it will also be necessary to consider recovery. Thus, after intermediate results have been obtained using more accurate human error probabilities, the final results are obtained by applying an appropriate multiplicative factor to each cut set probability. This multiplicative factor, which is the non-recovery probability, accounts for the possibility that operator action will eliminate one of the faults in the cut set and thereby prevent core damage. Preliminary guidance for recovery analysis is provided in Ref. [15]. The following discussion presents additional considerations regarding the recovery analysis.
6.3.1. Recovery analysis

Each accident sequence minimal cut set represents one possible way the sequence may occur. The information available to the operator and the recovery action to be taken generally depend on the combination of events that have occurred and hence on the particular minimal cut set. Therefore recovery actions are generally considered at the minimal cut set level rather than at the accident sequence level. Since there may be a large number of minimal cut sets for an accident sequence, it may be necessary to consider recovery for only the most significant minimal cut sets. A probability of non-recovery is estimated for each minimal cut set which is recoverable by some operator recovery action. The frequency of the minimal cut set is then multiplied by its probability of non-recovery to estimate the final minimal cut set frequency with recovery. The final estimated frequency for an accident sequence is computed using these minimal cut set frequencies with recovery.

The primary events of a particular accident sequence minimal cut set may or may not be recoverable by routine recovery actions. Extraordinary recovery actions are not considered, but routine recovery actions are. For example, the overhaul of a pump is not considered, but the manual realignment of a valve, whether by a hand switch in the control room or local turning, is. If a primary event can be recovered by a routine recovery action, the location of the recovery action is determined. In general, recovery actions can be separated into those which can be accomplished from the control room and those which can only be performed locally. If recovery can only be performed locally and the local site is inaccessible (for example, inside the containment), the primary event is considered non-recoverable.

Once a primary event is deemed recoverable and the location of the recovery action is determined, a critical time for the recovery action is estimated. Two types of critical times are considered when determining the critical time for a recovery action.

The primary event itself can have a critical recovery period which is independent of the accident sequence or of the state of the core or containment in an accident sequence. An example of this type of primary event critical time is that associated with the lubricating oil cooling for a pump. If the primary event is the loss of such cooling, there is a definite time interval during which the pump can operate without the cooling, and this time interval defines the critical time for the recovery of the primary event.

For the second case, the time in which a mitigatory action can be carried out is considered. In general, the accident sequences can be combined into groups with each group having its own set of critical times. For example, sequences initiated by large LOCAs have different time constraints for recovery than do sequences initiated by small LOCAs. In this second type of critical time examination, the questions asked in determining the critical time for recovery are phenomenological in nature. For example, if none of the containment spray pumps receives an actuation signal,
### TABLE XV. PROBABILITIES OF RECOVERY AND NON-RECOVERY USED IN REF. [26]a

<table>
<thead>
<tr>
<th>$P(R)$</th>
<th>$P(NR)$</th>
<th>Critical time for recovery action</th>
<th>Critical time for recovery action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>In control room (min)</td>
<td>Locally (min)</td>
</tr>
<tr>
<td>0.00</td>
<td>1.00</td>
<td>&lt;5</td>
<td>&lt;15</td>
</tr>
<tr>
<td>0.75</td>
<td>0.25</td>
<td>5–10</td>
<td>15–20</td>
</tr>
<tr>
<td>0.90</td>
<td>0.10</td>
<td>10–20</td>
<td>20–30</td>
</tr>
<tr>
<td>0.95</td>
<td>0.05</td>
<td>20–30</td>
<td>30–40</td>
</tr>
<tr>
<td>0.97</td>
<td>0.03</td>
<td>30–60</td>
<td>40–70</td>
</tr>
<tr>
<td>0.99</td>
<td>0.01</td>
<td>&gt;60</td>
<td>&gt;70</td>
</tr>
</tbody>
</table>

a $P(R) = 0.0$ and $P(NR) = 1.00$ for faults that are non-recoverable or whose location is inaccessible.

The critical time during which they can be manually actuated is determined by how long it takes for the containment to be pressurized to the point of failure. When both types of critical times are applicable for a particular recovery action, the shortest critical time is used.

After the critical times and locations of the possible recovery actions are established, the probability of recovery is estimated for each recovery action. The probability of non-recovery is one minus the probability of recovery. If a primary event is not recoverable, its probability of recovery is zero and its probability of non-recovery is one.

Table XV is an example of a generic recovery model, for which the probability of recovery is a function of the critical time and location of the recovery action. From the table, if a primary event has a critical time of 18 minutes and can be recovered by a recovery action in the control room, the probability of non-recovery is 0.1. If this primary event can also be recovered locally, the associated probability of non-recovery is 0.25. In such a case, the probability of non-recovery used in the analysis should be the smallest one, 0.1 in this example.

Table XV was developed from a simplified human reliability model [37] that accounted for two important factors in estimating recovery and non-recovery probabilities: (1) the time available to perform a recovery action and (2) the location in
which the recovery action takes place. More recent models of human actions include other factors; for example, the human cognitive reliability (HCR) correlation includes as variables the available time to perform the task, the type of cognitive processing (skill, rule or knowledge), the stress level and the man–machine interface. These aspects are discussed further in Sections 4.3 and 5.5.

For most minimal cut sets, recovery of a single primary event of the minimal cut set will restore the sequence to a success (no core damage). For these minimal cut sets, the frequency of the minimal cut set is multiplied by the probability of non-recovery to estimate the final frequency of the minimal cut set with recovery.

When accident sequences are categorized into plant damage states, then in a small number of minimal cut sets (for the Arkansas Nuclear One Interim Reliability Evaluation Programme (IREP) analysis [37], less than 1% of the minimal cut sets) more than one basic event in the minimal cut set requires recovery to restore the sequence to a success state. Recovery of just one primary event in these minimal cut sets alters the minimal cut set so that it becomes a minimal cut set of another sequence, still leading to core melt but belonging to another plant damage state. The probability of non-recovery for a minimal cut set which requires the recovery of more than one of its primary events is given by:

\[
P(NR) = 1 - \sum_{i=1}^{n} (1 - P(NR)_i)
\]

where \( n \) is the number of primary events requiring recovery and \( P(NR)_i \), for \( 1 \leq i \leq n \), is the individual probability of non-recovery for each of the \( n \) primary events to be recovered from.

Finally, minimal cut sets may contain events that represent independent subtrees. One approach to applying recovery to the independent subtrees is to replace the developed events that represent independent subtrees by the minimal cut sets of the independent subtrees that were determined earlier in the analysis. Recovery can then be applied as previously described.

6.4. TASK 30: UNCERTAINTY ANALYSIS

The objective of Task 30 is to provide qualitative discussions and quantitative measures of the uncertainties in the results of the PSA, namely the frequency of core damage, the frequency of accident sequence categories and the dominant accident sequences. Uncertainty analysis is an important task of a PSA. It should be emphasized that the uncertainties associated with the ways in which core damage might occur pertain regardless of whether or not a PSA is performed for the plant. It is one of the main advantages of a PSA that it can identify a number of sources of this uncertainty and quantify and describe a substantial part of it.
Since the PSA model attempts to simulate reality, it is inevitable that there will be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations will generate uncertainties. We can distinguish three major categories of sources of uncertainties in these models.

(1) **Completeness.** The main thrust of the PSA model is to assess the possible scenarios (sequences of events) that can lead to undesirable consequences — core damage for a Level 1 PSA. However, there is no guarantee that this process can ever be complete and that all possible scenarios have been identified and properly assessed. This lack of completeness introduces an uncertainty in the results and conclusions of the analysis that is difficult to assess or quantify.

(2) **Modelling adequacy.** Even for those scenarios that have been identified, the event sequence and system logic models do not precisely represent reality. There are uncertainties introduced by the relative inadequacy of the conceptual models, the mathematical models, the numerical approximations, the coding errors and the computational limits. These uncertainties are discussed as part of the uncertainty analysis in the PSA, and sensitivity studies are usually performed to assess their relative importance. It is also possible to quantify a part of this uncertainty through formal uncertainty analyses [38].

(3) **Input parameter uncertainties.** The parameters of the various models used in the PSA are not exactly known because of scarcity or lack of data, variability within the populations of plants and/or components, and assumptions made by experts. Input parameter uncertainties are the uncertainties that are at present most readily quantifiable.

In the following subsections, specific points in the uncertainty analyses are discussed.

### 6.4.1. Propagation of uncertainties

The quantification of the third category of uncertainties, input parameter uncertainties, is usually done by considering a PSA result (e.g. frequency of core damage) as the output of a model which has as inputs parameters that are characterized as random variables. The probability distribution function assumed for each parameter then quantifies the uncertainty that is due either to lack of knowledge about the exact value of this parameter or to actual variations in the value of the parameter among the members of a certain population. Although there are conceptual differences between these two types of uncertainty, the operational methods for propagating these uncertainties through the model are the same.

The most widely used technique for propagating uncertainties is Monte Carlo simulation. In general, a Monte Carlo simulation consists of generating a random sample of the inputs of the model and determining the PSA output from each set of
inputs in the sample. This process results in a random sample of the PSA output. Quantitative measures of the uncertainty associated with the output are then derived from this random sample. The various Monte Carlo techniques can be distinguished on the basis of the random sampling method as follows:

1. **Simple random sampling (SRS).** Simple random sampling is the simplest of the sampling methods. In this method, every value of the sample is randomly sampled from its distributions. The advantages of simple random sampling are simplicity of generation, availability of well known methods of estimation and statistical analysis, robustness and aggregation. With regard to aggregation, simple random samples obtained using the same models and parameter distributions can be combined to make larger samples. There is one main disadvantage of simple random sampling: it may require many simulations which for complex time consuming models (such as those in PSAs) might impose excessive computer time requirements.

2. **Latin hypercube sampling (LHS).** Latin hypercube sampling is one method of sampling a large number of input variables that yields estimators of model response more efficiently than SRS. The name of the sampling method derives from its similarity to certain fractional factorial sampling plans. LHS partitions a parameter range into discrete intervals. A parameter value within each interval is sampled using SRS. This approach reduces the sample size (relative to SRS) required to obtain estimates of a specified precision. The beneficial characteristics of LHS include its unbiased and efficient estimators. The efficiency of LHS versus the SRS has been demonstrated for cases in which the output is a monotonic function of the input variables, as is the case for PSA models when the rare event approximation is used. (In the rare event approximation, the frequency of core damage is expressed as a closed, monotonic function of the various input parameters, i.e. sums of products). If, however, non-events (e.g. successes) are included in the model, then the model ceases to be monotonic and there is no theoretical basis for assuming that LHS performs better than SRS. Furthermore, subsamples of LHS do not constitute a Latin hypercube sample and hence the LHS does not exhibit the advantage of aggregation. LHS looks promising for reducing the ‘cost’ of uncertainty analysis, but its advantage over SRS for non-coherent PSA models remains to be demonstrated.

Another approach that has been used for uncertainty propagation is that of discretization. According to this technique, all input variables and parameters are discretized; that is, their range is divided into a finite number of regions. A single value, such as the midpoint, represents the whole region and the value is assigned the probability corresponding to that region. All combinations of the discrete values of the input variables are then taken, with each combination having the probability of occurrence specified by the joint probability of the discrete input variables. Thus,
discretization can be viewed as another way of generating a random sample of the input variables. The advantage of this method is its simplicity. The main disadvantage is the exponential increase in the number of ‘sampling’ points as the number of input variables and/or the number of discrete values of each variable increase. A related problem lies in the possibility of using too coarse a mesh for discretization and in so doing missing a whole region of the input variables that can be very important for the output.

6.4.2. Specific issues in propagating uncertainties

All the cautions taken in the previous steps of quantification to obtain point values must be repeated here. Thus the function that provides the core damage should be the Boolean reduced form, i.e. the minimal cut sets at the resolution level established in Tasks 27 and 29.

Points in propagating uncertainties which require special attention are:

1. **Treatment of similar components.** If two or more primary events have the same parameter (e.g. failure rate λ and failure mode), then in the uncertainty analysis these parameters should be totally correlated. Thus in the random sample they should be represented by the same random variable (see Ref. [39]).

2. **Inclusion of non-events.** The uncertainty propagation is usually based on the rare event approximation, as in the case when the point calculations are carried out. However, for certain events, particularly human errors modelled at the event tree level, it might be important to include non-events to avoid an overestimation of the final result. Events with mean values of around 0.10 or greater can take values close to unity during the generation of the random sample. If this is the case, accident sequences that assume the success of these events should be multiplied by the complementary probabilities.

3. **Probability density functions for input variables.** Probability density functions (PDFs) are used to characterize the uncertainties and hence the random variable distributors. The inputs to be characterized by appropriate PDFs include the frequencies of the initiating events, the component failure rates and the human error probabilities. If a plant specific assessment of these parameters is performed (see Section 5), then the plant specific posterior PDFs are to be used. If a generic database is used, then the appropriate PDFs defined in the database should be used.

4. **Results.** The results should include the mean and the median values, together with sufficient information about the distribution to allow the user to estimate the probability associated with any interval. Further guidance on reporting the results, along with the inputs used, is given in Section 7.

Reference [20] presents computer codes that are available for uncertainty analysis.
6.5. TASK 31: IMPORTANCE AND SENSITIVITY ANALYSIS

Importance analysis requires the determination of the importance of contributors to core damage frequency, accident sequence frequencies and system unavailability. Sensitivity analysis requires the determination of the sensitivity of the PSA results to input assumptions, models and data. In analysing both importance and sensitivity, particularly for primary events, it should be recognized that the two are related. Events which have a high calculated importance initially will also display a high sensitivity. The following sections discuss specific points regarding these analyses.

6.5.1. Importance analysis

Reference [40] provides extensive discussions on the evaluation and utilization of risk importance. This section highlights important aspects of these discussions.

The purpose of the importance evaluation is to identify the important accident sequences, system failures, component failures and human errors with regard to core damage frequency (CDF). The importances which are determinable from a PSA can be grouped into two classes:

1. qualitative importances;
2. quantitative importances.

Qualitative importances are importances to CDF that are derived from the logic structure of the PSA models. The logic structure of the PSA includes the fault tree and event tree models and the failure combinations causing undesired events (the minimal cut sets). The qualitative information in a PSA provides valuable criteria by which to evaluate the importances of risk contributors and changes.

The quantitative importances are the importances of CDF contributors and changes that are derived from the quantitative results of the PSA. The quantitative importances utilize the estimated system failure probabilities, accident sequence frequencies or CDF. Although quantitative importances can provide more detailed information than the qualitative importances, they are also subject to the greater uncertainty associated with the quantification.

These two types of importances are discussed in the following subsections.

6.5.1.1. Qualitative importances: critical groups of components susceptible to common cause failures

The minimum cut sets are the key quantities used in quantifying the PSA models. However, the minimum cut sets also provide qualitative, structural information which can be used to identify important component failures and important situa-
tions that can lead to undesirable consequences. Single component minimum cut sets for a system, for example, are single component failures that result in system failure.

On the basis of reliability considerations, it is known that components that have a common failure susceptibility are subject to failure from one common cause which can fail all the components (see also Section 4.4 and Appendix VI on common cause failure analysis). These common susceptibilities are significant only if the susceptible components are in the same minimum cut set. The minimum cut set information from PSAs can thus be evaluated to identify the minimum cut sets in which all the components have a common susceptibility.

The common susceptibilities in a minimum cut set that can be specifically focused upon include:

1. all components of the same generic type (such as all pumps) in a minimum cut set (critical group) indicative of potentially common, critical vulnerabilities;
2. all components in a minimum cut set in the same location;
3. all components in a minimum cut set under the same maintenance or testing procedure;
4. all human errors in a minimum cut set that implies that human errors alone can fail critical subsystems, systems or functions;
5. all components in a minimum cut set that can be exposed to a common harsh or degrading environment;
6. all components in a minimum cut set not testable in routine surveillance testing, thereby giving a critical undetectable failure mode;
7. all components in a minimum cut set tested under a common pre-operational or start procedure: if the procedure is inadequate, a critical failure mode can be untested or undetected.

These common cause failure susceptibilities can be further evaluated quantitatively using the approaches discussed in Appendix VI and in subsection 6.5.2.

6.5.1.2. Quantitative measures of importance

There are two basic measures of importance generally calculated in a PSA: the Birnbaum importance and the Fussell-Vesely importance.

(1) The Birnbaum importance

The Birnbaum measure of importance of an event X is defined as the rate of change of the frequency of core damage (derivative) with respect to a change in the probability of occurrence of the event X:

\[ I_B(X) = \frac{d \text{(CDF)}}{dX} \]
which because of the nature of the PSA equations can also be expressed as:

\[ I_B(X) = \text{CDF}(1) - \text{CDF}(0) \]

where \( \text{CDF}(1) \) is the CDF if the event is assumed to have occurred and \( \text{CDF}(0) \) is the CDF if the event is assumed not to have occurred. Thus, the Birnbaum measure of importance is the difference between the frequency of core damage given that event \( X \) has occurred and the frequency of core damage given that event \( X \) has not occurred.

2. The Fussell-Vesely importance

The Fussell-Vesely measure of importance of an event \( X \) is defined as the fractional contribution to the frequency of core damage (or accident sequence frequency) from the event.

The Fussell-Vesely importance can be expressed as

\[ I_{FV}(X) = \frac{\text{Sum of cut set contributions to CDF containing the event } X}{\text{CDF}} \]

Reference [40] provides additional qualitative and quantitative measures of importance, as well as potential uses.

6.5.2. Sensitivity analysis

The purpose of sensitivity analysis is twofold: (1) to determine the sensitivity of the core damage frequency to possible dependences among component failures and among human errors; (2) to address those modelling assumptions suspected of having a potentially significant impact on the results. These assumptions are generally in areas where information is lacking and heavy reliance must be placed on the analyst’s judgement. Sensitivity analysis can then be performed by substituting alternative assumptions and evaluating their individual impacts on the results. Sensitivity analyses of possible dependences among component failures and among human errors are further discussed in the following subsections.

6.5.2.1. Component failure dependence analyses

The sensitivity prescribed here is intended to explore, among other things, whether a detailed common cause failure analysis is warranted for a particular group of components.
As a first step, a search is conducted for areas that are sensitive to coupling between hardware failures. Searches for sensitivity to dependence can be carried out on a system basis or on an accident sequence basis.

The following assessment can be performed to further quantify common cause and dependence potentials.

(1) The minimal cut sets can be searched for dependence suspect minimal cut sets (DSMCSs). DSMCSs are minimal cut sets containing failures of components, of which two or more have a common property that renders them susceptible to dependent failures. These susceptibilities, together with the way of determining DSMCS, were described in subsection 6.5.1.1. (Note that for more refined analyses not all components in the cut set have to have the common property, but only two or more.)

(2) Each DSMCS can be requantified as follows:
   (a) identify the highest failure probability among the potentially coupled events having a common cause failure susceptibility;
   (b) set the product of the remaining coupled failure probabilities equal to 0.1.

(3) For each type of coupling, the pertinent DSMCSs can be presented, together with their respective new and old quantifications; the ratio change in system unavailability (referred to that assessed in (1)) can also be presented.

(4) Whenever the effect of a given coupling on a given system is substantial (e.g. greater than a factor of two in system unavailability), the corresponding change in the frequencies of the affected core damage sequences can be presented, together with a discussion of precautions, actions or conditions existing in the subject plant that serve to reduce the potential dependence.

Single failures in any of the systems can also be tabulated and discussed separately. The discussion can give the defences or conditions that reduce the contributions of these events to system unavailability.

6.5.2.2. Human error dependence analyses

The human error dependence sensitivity analyses should be performed similarly to the component dependence sensitivity analyses. The DSMCSs that can be identified are those containing multiple human errors of any type. The minimal cut set can also contain component failures; it is the fact that it contains multiple human errors that renders it suspect. Rather than being requantified, these DSMCSs can be analysed and a description given of the precautions, management control or conditions that serve to eliminate significant dependences among the human errors in the cut sets. These discussions can be prepared in a tabular format, with the DSMCSs ordered according to the number of human errors involved.

93
7. DOCUMENTATION OF THE ANALYSIS: 
DISPLAY AND INTERPRETATION OF RESULTS

The sixth major procedural step includes all the aspects of documentation of the PSA. 'Documentation' here is understood in its broad sense; that is, related subjects, which influence directly or indirectly the form and handling of documentation, are also considered. Section 7 is mainly directed towards giving specific guidance concerning the suitable forms for external documentation; for example, presentation of results to different users of PSAs in consideration of different types of applications. The format of the suggested documentation is generally based on that provided in Refs [3] and [41].

Three tasks can be distinguished in this procedural step. A schematic representation of these tasks is shown in Fig. 6.

7.1. TASK 32: OBJECTIVES AND PRINCIPLES OF DOCUMENTATION

This task identifies PSA users, applications and principles to be followed in the documentation effort.

The primary objective of the PSA documentation should be to fulfil the requirements of its users and be suitable for the applications in question.

The potential users are:

— utilities (management, operating personnel);
— designers/vendors;
— regulatory authorities, including other potential reviewers;
— other government bodies;
— the public.

The main applications/uses of a PSA are identified in Section 2.1 in conjunction with the definition of the PSA objectives.

The documentation of PSA should be well structured, clear and easy to follow, to review and to update. In addition, means should be provided for possible extensions of the analysis, including integration of new topics, use of improved models, broadening of the scope of the PSA in question, and use for alternate applications. Explicit presentation of the assumptions, exclusions and limitations of extending and interpreting the PSA is also of critical importance to the users. Thus, a qualification of the results should be given.

Finally, it is recommended that:

— conclusions be distinct, and reflect not only the main, overall results, but the contributing analyses;
7.2. TASK 33: ORGANIZATION OF DOCUMENTATION

In this task the detailed organization of the documentation is established. The first step in organizing the documentation of the study consists in determining the nature and the amount of information that is going to form the external

---

emphasis be given to the analysis of uncertainties in the data and to sensitivity analysis where the effects of assumptions, limitations and conservatisms in methods and modelling are clearly demonstrated.

---

FIG. 6. Tasks for the documentation of the analysis.
documentation, i.e. what is going to be published, and the information that is going to form the internal documentation.

The documentation should provide within the report or by reference to available material all the necessary information to reconstruct the results of the study. All intermediate subanalyses, calculations, assumptions, etc., which will not be published in any external reports should be retained as notes, working papers or computer outputs. This is very important for reconstructing and updating each detail of the analysis in the future. It is recommended to use well organized computer and word processor files as much as possible for storing this type of information.

The organization of the PSA documentation should be governed by two general principles:

— traceability: for review and updating of the analysis it should be possible to trace any information with minimum effort.
— sequentiality: the order of appearance of the analysis in the final documentation should follow as far as possible that of its actual performance; that is:

  • initiating events;
  • event tree analysis;
  • systems analysis and related topics;
  • accident sequence quantification;
  • uncertainty and sensitivity analysis.

It is recommended that the external documentation of the PSA study be divided into three major parts:

• summary report;
• main report;
• appendices to the main report.

The summary report should provide an overview of the PSA project’s motivations, assumptions, objectives, scope, results and conclusions at a level which is useful to a wide audience of reactor safety specialists and which is adequate for high level review.

The summary report is designed to:

— support high level review of the PSA;
— communicate key aspects of the study to a wider audience of interested parties;
— provide a clear framework and guide for the reader or user prior to consulting the main report.

The summary report of a PSA should include a subsection on report organization which should present concise descriptions of the contents of the sections of the main report and of the individual appendices. The relation between various sections and parts of the PSA should also be included in this section.
TABLE XVI. SAMPLE CONTENTS OF EXTERNAL DOCUMENTATION OF PSA STUDY

I. SUMMARY REPORT

S.1. Introduction
S.2. Results of the analysis
S.3. Results of importance and sensitivity analyses
S.4. Interpretation of results, conclusions and recommendations
S.5. Overview of methods
S.6. Organization of the main report

II. MAIN REPORT

M.1. Overview of the study
   M.1.1. Background and objectives of the study
   M.1.2. Scope of the study
   M.1.3. Project organization and management
   M.1.4. Project implementation
   M.1.5. Overview of procedures and methods
   M.1.6. Report organization

M.2. Plant and site description
   M.2.1. Overall plant characteristics
   M.2.2. Plant systems
   M.2.3. Plant site

M.3. Identification of radioactive sources, accident initiators and plant response
   M.3.1. Sources and conditions of radioactive releases
   M.3.2. Selection of initiating events
   M.3.3. Plant functions and system relations
   M.3.4. Plant system requirements
   M.3.5. Grouping of initiating events

M.4. Accident sequence modelling
   M.4.1. Event sequence modelling
   M.4.2. System modelling
   M.4.3. Human performance analysis
   M.4.4. Qualitative dependence analysis
   M.4.5. Impact of physical processes in the progression of accident sequences
   M.4.6. Classification of accident sequences into plant damage states

M.5. Data assessment and parameter estimation
   M.5.1. Initiating event data and frequencies
   M.5.2. Component data and parameters
   M.5.3. Human performance data and parameters
TABLE XVI. (cont.)

M.6. Accident sequence quantification
   M.6.1. General concept of the quantification process
   M.6.2. Analysis of system models
   M.6.3. Quantification of accident sequences
   M.6.4. Uncertainty analysis
   M.6.5. Importance and sensitivity analysis
   M.6.6. Computer codes used in the analysis

M.7. Display and interpretation of results
   M.7.1. Dominant sequences contributing to core damage frequency
   M.7.2. Results of uncertainty analysis
   M.7.3. Results of importance and sensitivity analyses
   M.7.4. Interpretation of results and engineering insights
   M.7.5. Credibility and qualification of results
   M.7.6. Conclusions, recommendations and potential applications

III. APPENDICES TO THE MAIN REPORT

A. Appendices to systems analysis
   A.1. General items on systems analysis
      A.1.1. Contents and organization of appendices
      A.1.2. General modelling assumptions
      A.1.3. Methodological issues
      A.1.4. Nomenclature and format used in system description and analysis
   A.2. System /.../ (for each system)
      A.2.1. Description of system
         A.2.1.1. Sources of information
         A.2.1.2. System function
         A.2.1.3. Design basis
         A.2.1.4. Interfaces
         A.2.1.5. Operation
         A.2.1.6. Test and maintenance
         A.2.1.7. Technical specifications
      A.2.2. Event tree interface
      A.2.3. Fault tree (or other system model)
      A.2.4. Quantification of basic events

B. Data assessment and parameter estimation
   B.1. Methods and assumptions
   B.2. Initiating events
   B.3. Components
   B.4. Human errors

C. Human performance analysis

D. Dependence analysis

E. Quantification of accident sequences
It should be noted that although presented at the front, the summary report is the last part of the documentation to be prepared.

The main report should give a clear and traceable presentation of the complete PSA study, including plant description, study objectives, methods used, initiating events considered, plant modelling results and conclusions. Perhaps the most significant feature of the main report (and its appendices) is that it should contain sufficient information presented in such a way as to allow the efficient quantitative reconstruction of the dominant accident sequences.

The main report together with its appendices is designed:

— to support technical review of the PSA;
— to communicate key detailed information to interested users;
— to permit the efficient and varied application of the PSA models and results;
— to facilitate the updating of models, data and results to support a continuing safety management programme.

The physical size of the main report will depend on the objectives and scope of the specific project.

The appendices should contain detailed data, records of engineering computations, detailed models, etc. While it is impossible to specify what detailed information should generally be provided in the appendices, the functional requirements of the main report should provide the necessary guidelines. A good rule of thumb is to put information in the appendices if most users will not need it or will not need to consult it regularly. The appendices should be constructed to correspond directly to the sections and subsections of the main report, as far as possible.

The recommended organization of the external documentation is given in Table XVI and further discussed in Appendix VIII.

7.3. TASK 34: PREPARATION OF DOCUMENTATION

In Task 34 the study documentation is generated on the basis of the objectives and principles defined in Task 32 and in accordance with the detailed organization of the documentation established in Task 33.
Appendix I

EXAMPLE OF A TYPICAL SCHEDULE FOR A LEVEL 1 PSA

Table XVII shows a simplified schedule for a Level 1 PSA based on the tasks defined in this report. The durations shown are indicative (e.g. the data assessment task assumes the use of generic databases) and the iterative nature of almost all tasks is not shown. The tasks should be split into more than one phase so that some of them can be repeated when the results of other tasks are available.
### TABLE XVII. PROJECT: EXAMPLE OF SCHEDULE OF LEVEL 1 PSA

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management and organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Definition of objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Definition of scope</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Project management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Selection of methods and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>establishment of procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Team organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Team training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Funding and scheduling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Setting of technical quality assurance procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of radioactive sources and accident initiators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Plant familiarization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and information gathering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Identification of site release sources of concern</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Identification of plant operating states of concern</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Definition of core damage states or other consequences</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Initiating event selection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Safety functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. Function/system relations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. Plant system requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Grouping of initiating events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
</tbody>
</table>

**Accident sequence modelling**

18. Event sequence modelling
19. System modelling

**For System 1**

- Define top event(s)
- Develop fault tree logic
- Label fault tree
- Assign data
- Solve fault tree
- Plot fault tree
- Document fault tree analysis

**Fault tree analysis for other systems**

- Prepare analysis (as above)

20. Human performance analysis
21. Qualitative dependence analysis
22. Impact of physical processes on logic model development
23. Classification of accident sequences into plant damage states

**Data assessment and parameter estimation**

24. Assessment of frequency of initiating events
25a. Assessment of component reliability

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>25b. Assessment of common cause failure probabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26. Human error probabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accident sequence quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27. Determination of the accident sequences Boolean equations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28. Initial quantification of accident sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29. Final quantification of accident sequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30. Uncertainty analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31. Importance and sensitivity analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentation of PSA: display and interpretation of results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32. Objectives and principles of documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33. Organization of documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34. Preparation of documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix II

CONTENTS OF WORK SPECIFICATION

Where work specification is to be issued before commencement of work, it should include the following as a minimum:

(1) A summary of the work proposed.

(2) An introduction which should explain the background to the project and give a general description of the plant and the extent of the work, the purpose of the study and the nature of the work to be carried out.

(3) A detailed and clear description of the scope of the work (see Section 2.2).

(4) A description of the extent of the study, which should clearly specify what will be produced in the PSA and the work to be carried out by the organization responsible for the analysis. The methodological steps that should be included should also be specified. For example, the specification would include:
   — the proposed methods;
   — a list of initiating events to be considered and the justification and verification required;
   — the fault trees to be constructed for the plant by an approved method and their review if required;
   — the database to be developed if necessary, methods for covering newer plant specific components in a generic database, the justification of additions and/or modifications, and whenever applicable the extent of intended use of plant specific experience;
   — analytical work, including the studies to be carried out to determine the consequences of particular fault sequences, investigations to be carried out into detailed plant operation and requirements for the use of real time simulation for fault development.

The contents of written reports and the format to be adopted should be detailed. The form of the output may differ depending on the end use envisaged for the PSA (see Section 7 and Appendix VIII). Specifically, the form of a detailed numerical report relevant to the needs of a design or licensing organization is unlikely to meet the requirements of the operating staff.

It is necessary that regular reports be produced while the work is in progress. Where the contract calls for changes to existing computer software, this should be clearly specified.

(5) Input from the organization that commissioned the PSA should specify the documentation that it will provide. The commissioning organization should nominate a representative through whom all communications should be channelled and should require the body carrying out the analysis to nominate its representative. Arrangements for plant visits and inspection should be set out.
(6) The required time-scale for completion of the project should be specified or the body carrying out the analysis should be required to submit a programme for approval. The project programme should include milestones which mark completion of significant parts of the work.

(7) The form of contract, confidentiality and copyright are not covered in the report but should be taken into consideration if external resources are used.
Appendix III

QUALITY ASSURANCE PROCEDURES

Appendix III presents specific aspects of QA procedures for a PSA and it is based on Ref. [42]. The QA procedures provide for control of the constituent activities associated with a PSA, which can be distinguished in the following three areas: organization, technical work and documentation. For each of these areas there are a number of characteristics or attributes that characterize the technical quality of the PSA. The QA procedures aim at strengthening or ensuring the adequacy of each and every attribute. Table XVIII presents the three areas of PSA activities and the corresponding attributes.

The development of QA procedures for a PSA has two stages: (a) a matrix is established in which each procedural task of the PSA is associated with the relevant attributes that characterize its technical adequacy; (b) on the basis of this matrix a detailed QA activity is established with the aim of strengthening the attributes that characterize each step.

<table>
<thead>
<tr>
<th>Area of a PSA study</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Experience, Balance, Integration, Communication, Responsibility</td>
</tr>
<tr>
<td>Technical work</td>
<td>Completeness, Accuracy, Quantification, Verification, Consistency</td>
</tr>
<tr>
<td>Documentation</td>
<td>Clarity, Traceability</td>
</tr>
</tbody>
</table>

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
III.1. QUALITY ASSURANCE MATRIX

The quality assurance matrix provides an indication of which attributes apply within the PSA procedural structure. An example of such a matrix is presented in Table XIX, adapted from Ref. [42]. The vertical dimension of this matrix characterizes the general area (organization, technical work, documentation) in which a particular task belongs and the more relevant attributes. The horizontal axis covers all the procedural steps of the PSA. It should be noted that the horizontal axis does not correspond directly to the PSA tasks presented in this report. Thus, although the technical elements outlined in the PSA structure cover most of the tasks suggested in the report, they are mainly structured for QA use and as such are biased towards QA issues. The list of procedural tasks in Table XIX assumes that fault tree and event tree methods are used in the procedural step of accident sequence modelling. The approach, however, can be extended to alternative systems analysis methods.

The vertical axis of Table XIX does not contain the additional complementary attributes of communication and responsibility (integration of organization) or verification of quantification (accuracy of technical work) that are included in Table XVIII.

The matrix provides a framework for the development and evaluation of QA activities. A comprehensive set of QA procedures should include checks and controls on each of the attributes that characterize the technical adequacy of each of the procedural tasks.

III.2. QUALITY ASSURANCE PROCEDURES

This section presents QA procedures based on internal intradisciplinary review.

The term internal intradisciplinary review refers to the review of work within a task (or discipline) by other members working on the same task. For example, fault trees might be reviewed by other fault tree analysts on the study team. A major element in such a review process is the participation of plant and/or utility personnel who are on the study team. These people are the most knowledgeable with respect to the plant layout, systems and performance. If such people are not included on the study team, they should nevertheless be included in this type of internal review.

Also included in the internal intradisciplinary review are limited reviews by members from other tasks. These reviews are limited to the use of data or results generated in tasks other than the task being reviewed. For instance, someone responsible for data development might review the use of the data in the quantification of the fault trees.

The internal intradisciplinary review would not address such concerns as the balance of the study or the consistency or integration of tasks. However, this type
of review is a good way of ensuring validity in such areas as plant modelling, calculations, code application and application of methods.

A suggested QA procedure based on intradisciplinary review is outlined in the remainder of Section 3.2. It should be kept in mind that the effectiveness of such a review is highly dependent upon the mechanics of the specific QA procedure. The general procedure listed here is designed to maximize the effectiveness of the review. The programme covers all applicable areas of the matrix.

— A person should be designated from each task or subtask listed in Table XIX to be responsible for the administration of procedures within that discipline.
— Each person selected is to be responsible for ensuring that every attribute listed in the matrix under his or her task or discipline is considered.
— A leader should be chosen for this review team. This leader is responsible for the intradisciplinary review and should report directly to the person in charge of the PSA. (The review team leader and the PSA leader may be the same person, but such an arrangement might compromise the independence of the review. It is therefore suggested that if possible within the budgetary constraints of the PSA the review team leader and the PSA team leader be different.)
— Documentation concerning the review should be provided for every attribute associated with procedural tasks listed in the matrix.
— Documentation of the review should include: date of review, reviewer, methods of review, results of review (including the review team’s assessment of whether and how well each of the applicable standards has been met), and areas of the matrix covered by the particular review.
— Reviews should be conducted as soon as possible after each subtask is completed. To avoid the costly and ineffective repetition of the review of some subtasks that are normally iterated several times during a PSA, it may be agreed in advance that certain reviews will be conducted only upon completion of major phases of the PSA study or at the final iteration.
— Review of preparatory work, such as the selection of methods and assumptions, should be conducted before the actual analyses are performed.
— Reviews should be conducted by the most knowledgeable person within the task group.
— Reviews should be independent; a task member should preferably not review his own work.
— For repetitive subtasks such as the development of fault trees, one person should review all of the similar subtasks in order to ensure consistency of treatment.
— For subtasks requiring knowledge of plant layout, plant response and plant data, an extra review should be conducted by the most knowledgeable plant or utility person(s). This review should follow the same guidelines as for the review performed by the task member(s).
### TABLE XIX. QUALITY ASSURANCE MATRIX

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Technical work</th>
<th>Organization</th>
<th>Technical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>Clarity</td>
<td>Consistency</td>
<td>Accuracy</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Technical elements:

- Goal/PSA framework
- Goal/scope
- Scope/funding
- Schedule/study team
- Schedule/methodology
- Methodologies
- Responsibilities
- Interfaces (communication)
- Direction and control
- Quality assurance
- Review
- In-progress documentation

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
<table>
<thead>
<tr>
<th>Documentation</th>
<th>Technical work</th>
<th>Organization</th>
<th>Technical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>Clarity</td>
<td>Consistency</td>
<td>Accuracy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE XIX. (cont.)

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Technical work</th>
<th>Organization</th>
<th>Technical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>Clarity</td>
<td>Consistency</td>
<td>Accuracy</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
<table>
<thead>
<tr>
<th>Documentation</th>
<th>Technical work</th>
<th>Organization</th>
<th>Technical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>Clarity</td>
<td>Consistency</td>
<td>Accuracy</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
TABLE XIX. (cont.)

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Technical work</th>
<th>Organization</th>
<th>Technical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traceability</td>
<td>Clarity</td>
<td>Consistency</td>
<td>Accuracy</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
— For subtasks requiring the use of data or results from another subtask, the responsible person from the other subtask should review the use of these data or results in the subtask in question.

A second type of QA procedure is based on internal interdisciplinary review. Internal means that the reviewers are part of the study team, and interdisciplinary indicates that the review covers concerns that extend beyond individual task boundaries. The interdisciplinary review is viewed as a complementary effort to the intradisciplinary review.
IV.1. INTRODUCTION

The aim of establishing a standard nomenclature for accident sequences is to provide reviewers and users of PSA studies with a concise, clear, readily understandable and intercomparable representation of important accident sequences of different nuclear power plants. At the same time, this nomenclature must be applicable to accommodate important features of present and future PSAs without requiring substantial revision of their results or methods.

The nomenclature:

— should be adaptable to plant specific and PSA specific differences;
— should be able to include special factors deemed significant by the organization commissioning the study or by its intended users;
— should be able to deal with more detailed definitions elicited by improved methods and extended regulatory and safety needs;
— should take account, where appropriate, of physical, functional and operational plant conditions;
— should be able to handle existing results;
— should be usable in plant implementations.

The nomenclature proposed in Appendix J of Ref. [3] is adopted here for PSAs for LWRs. Nomenclature for other reactor types is not presently available.

IV.2. GENERAL FORMULATION

The proposed standard nomenclature is based on initiators $I_i$, front line systems $F_j$ and accident physical characteristics bins $Z_k$.

These are largely but not exclusively determined by containment and consequence phenomena. Inclusion of binning is important not only for the insight it provides about the accident sequences, but also for its utility in carrying the Level 1 PSAs further to Levels 2 and 3.

The proposed system is similar to some PSA nomenclature schemes in that it includes initiators and front line system failures, but is somewhat untypical in that it excludes support system failures (notably electric power failures) and certain other events that appear in the nomenclature of some PSAs. It is shown in the following that there is scope within the present system for adding certain details of interest to
the primary sequence identifier; however, it is felt that standardization is easiest and clarity is greatest if the primary sequence identifier is kept as simple as possible, and the suppression of support system failures contributes to these goals.

The general formulation of this nomenclature is set out here, together with some explanatory comments. Section IV.3 lists the suggested specific definitions for the $I_i$, $F_j$, $Z_k$. (Since the nomenclature is constructed to allow expansion and extension the lists are not to be considered exhaustive.) The notation $I_i$, $F_j$, $Z_k$ is used in this section for purposes of discussion only: the actual notation listed in Section IV.3 uses wherever possible the more familiar (and in a historical sense more indicative) letters associated with previous studies.

The *primary* accident sequence identification is simply

$$I_i F_j ... F_m Z_k$$

which represents an accident sequence initiated by the initiator $I_i$, involving the failure of the front line systems $F_j ... F_m$ and pertaining to the plant damage state $Z_k$.

The more detailed (optional) format for an accident sequence is as follows:

$$I_i .. F_j .. F_m .. Z_k$$

or:

$$I_i(..) F_j(..) .. F_m(..) Z_k$$

The additional indices or bracketed dots represent additional information which serves to qualify and elaborate the primary identifiers $I_i$, $F_j$, $Z_k$ on the basis of the specific plant PSA and the particular sequence. This information, when available, will always add useful detail to the classification, but may not be necessary for the ‘first reading’ of the PSA results except in certain plant specific cases or unusual circumstances.

Those front line system failures $F_n$ which are deterministically related to preceding failures $F_j$ or to the initiator $I_i$ need not be included in the primary identification. They may usefully be displayed, however, if the situation is not immediately obvious, in the more detailed general (indexed or bracketed) format.

IV.3. NOMENCLATURE

Section IV.3 presents a standardized nomenclature for LWR plants. Because of the objectives and requirements already discussed, the suggested nomenclature listed here is, at the first level, as general as possible, and relies as far as possible on functional and operational characteristics. This allows ready comparison between the analyses of plants whose specific initiators and front line systems might have
rather different quantitative engineering descriptions. These differences in detail could be included in the additional indices (or brackets) if desired and available.

**IV.3.1. Initiators I<sub>i</sub>**

LOCA initiators are qualitatively determined by the associated coolant inventory loss, but the particular definitions in terms of either geometric (break size) or mitigating function requirements tend to be plant specific, depending on both design and operational considerations. It is nevertheless convenient to divide them into three classes, and the index or bracket format described should be used to indicate the specific details.

A Large LOCA: for example, a breach of the reactor coolant system (RCS) resulting in a pressure drop calling for the activation of the low pressure (high flow rate) mitigating system by engineered safety features (ESFs). In many PSAs such initiators are defined by the breach area; for example, exceeding 1 ft<sup>2</sup> (1 ft<sup>2</sup> = 929 cm<sup>2</sup>). This, or other critical characteristics, should be identified as indicated.

S<sub>1</sub> Medium LOCA: for example, a breach of the RCS resulting in a (lower) pressure drop that calls for high pressure (low flow rate) ESF mitigation: often characterized by breach areas between 0.55 ft<sup>2</sup> and 1 ft<sup>2</sup>. Again, the geometric and functional characteristics should be identified.

S<sub>2</sub> Small LOCA: for example, a small breach of the RCS, with a flow rate low enough to be controlled by non-ESF systems such as charging pumps. The geometry and mitigation requirements should be identified.

A more detailed (or finer) subdivision could be used if desired.

This terminology is by way of example rather than definitive. It is essential that the geometric and functional details be provided to clarify the plant specific variations.

V Interfacing system LOCA: this a a LOCA leading to bypassing of the containment.

T<sub>1</sub> Loss of off-site power transient.

T<sub>i</sub> Other transients with i = 1.

The primary index i may be used to identify particular transients such as turbine trips, loss of main feedwater and others that may apply. In a number of cases, transient initiators, followed by one or other front line system failures, result in LOCA conditions, which in turn lead to exactly the same further behaviour (sequences) as those described by the corresponding A or S<sub>i</sub>. From the point of view of the quantitative contribution to the core damage frequency (CDF), it is adequate and convenient to lump these with the corresponding S sequences. However,
in view of some aspects of plant intercomparability and operational and functional insight, it is important to note the genesis of such contributions. This may be done by applying the indexing (or bracketing) method described earlier to the S sequence, e.g. $S_1(T,F_2)$, denoting that the medium LOCA $S_1$ was generated by the transient induced sequence $T,F_2$. In particular, such identification should always be given in the case of transient induced LOCAs and in the case of a loss of off-site power initiated by in-plant phenomena.

IV.3.2. Front line system failures

For historical and engineering reasons it is desirable to distinguish between the proposed nomenclature for PWR plants and that for boiling water reactor (BWR) plants. (It would, however, be possible to develop a common system if required.)

(a) Pressurized water reactors

C: failure of the containment spray system.

For those systems with different success criteria for which operation of the injection and recirculation can be appropriately distinguished, the index $i$ should be used to denote the corresponding failures:

$C_i$: failure of containment spray injection system;
$C_r$: failure of containment spray recirculation system.

The same type of notational distinction should be adopted for those other systems listed in the following for which it is appropriate.

G: failure of the containment heat removal system;
D: failure of the low pressure emergency core cooling system;
K: failure of the reactor protection system;
L: failure of the auxiliary feedwater system;
M: failure of the power conversion system;
N: failure of the secondary system steam relief valves;
Q: failure of the pressure operated relief valves (PORVs) to reclose after opening;
R: massive rupture of the reactor vessel;
U: failure of high pressure core cooling system;
Y: failure of reactor building cooling system.

This classification is slightly more expanded and somewhat more rationalized than the familiar version from Ref. [1]. For example, the old designation TMLB' (from Ref. [1]) now might appear as $T_1(\ )\ ML$, where the symbol ( ) represents
failure to recover electrical power within a (defined) specific time. Other extended
or bracketed information could include:

— functional and operational particularities;
— the system success criteria including associated support system success
criteria;
— specific failure mode information.

(b) Boiling water reactors

K: failure of the reactor protection system.

The following indices should be used to identify the particular distinct failure
modes:

m: mechanical operation;
e: electrical activation;
a: alternate rod insertion;
s: standby liquid control system;
t: timely scram.

L: failure to limit reactor vessel high water level;
M: failure of overpressure protection system;
P: failure of relief valves to reclose after opening.

The primary index n may be used to indicate the number of solenoid operated
relief valves (SORVs) involved.

Q: failure of the feedwater system to provide core make-up water;
R: failure of recirculation pump trip;
R:\: failure of recirculation pump trip and feedwater runback;
V: failure of low pressure.

Indices may be used to identify distinct aspects of such failure. However, the
indices i and r should be reserved to denote the injection and recirculation phases.

U: failure of high pressure core cooling system (again with appropriate
(defined) indices);
W: failure of containment heat removal system;
X: failure to depressurize system;
X:\: failure to inhibit depressurization.

Remarks similar to those made for PWRs apply to additional indexed (or
bracketed) information.
IV.3.3. Classification of accident sequences into plant damage states

A plant damage state is defined by important common characteristics of the accident sequence, with special reference to the effects on containment integrity and leakage and ultimate release. This information is usually implicit (and sometimes even explicit) in the partial sequence, especially if the indexed (or bracketed) information is complete.

\[ I_i \ldots F_j \ldots - F_m \ldots \]

Even in this case, it will be desirable to display the most significant features of the plant damage state; in general, the detailed (indexed or bracketed) information may not appear in the accident sequence listing in complete form, and it then becomes important to include at least the more critical aspects of the plant damage state in the sequence definitions. At a minimum, each sequence should include the following, as appropriate:

- \( Z_e \): early core damage relative to the time of reactor scram;
- \( Z_a \): late core damage relative to the time of reactor scram;
- \( Z_p \): containment failure (of whatever kind) before core damage;
- \( Z_s \): containment failure (of whatever kind) after core damage.

The following additional features (as well as others not listed here), which to a degree recapitulate information implicit in the partial accident sequences, are also candidates for inclusion in the plant damage state information:

- containment bypass (those sequences of interfacing system LOCA type);
- LOCA with or without pressure suppression (BWRs);
- pool is subcooled or saturated when core damage occurs (BWRs);
- vessel pressure when core slump occurs;
- availability of containment heat removal;
- availability of AC power and recovery times;
- condition of reactor cavity at vessel failure (water flooded or dry).

IV.4. SUMMARY

The scheme outlined has the following properties:

- it displays the accident sequences in a relatively familiar form;
- it embraces both more comprehensive and/or more detailed formulations, without requiring extensive translation or entailing loss of clarity;
- it allows the embodiment of more specific equipment, functional and operational data as permitted or required by available data;
- it can be used and reviewed at a variety of levels depending on the needs of the reader.
Appendix V

FAILURE MODES AND EFFECTS ANALYSIS

V.1. INTRODUCTION

Failure modes and effects analysis (FMEA) is a standard evaluation procedure for systematically identifying potential failures in an equipment/system design and analysing the resulting effects on the performance of the equipment/system. The FMEA is useful in identifying the critical problem areas of a design and design improvements or operational modifications necessary in order to achieve the required equipment/system performance throughout the plant’s life cycle, and it is also a very useful preliminary step to system model development (e.g. fault trees).

Failure modes and effects analysis is an inductive method of reliability analysis and is based on the question ‘What happens if...?’ It considers one (single) failure within the equipment/system at a time. As such, it provides a better appreciation of the functioning of the equipment/system and its potential failure modes.

Failure modes and effects analysis has the disadvantage of being a relatively laborious method. However, it is a systematic method for analysing and clarifying the effects of component failures on the system functions.

V.2. DEFINITION OF TERMS

Failure mode: The manner in which the function of a component can fail (e.g. for an isolation valve one failure mode is ‘fail to close on command’).

Effect: The consequences of failure on a subsystem, a system or the plant as a whole.

Component: The specific subdivision of the plant or system under consideration in the analysis. Unless defined by contractual or regulatory requirements, the definition of components is at the discretion of the analyst for any given analysis.

Function: The specified working requirements of a component within a system (e.g. the functions of an isolating valve may be to open and close a particular flow path upon command and to maintain the pressure boundary of that path intact).
V.3. PURPOSE OF FMEA

The primary purpose in performing an FMEA in the context of a PSA is to provide qualitative information on the various ways and modes in which a system can fail, and hence it constitutes an input to system modelling. Additional uses of FMEA include:

— comparison of various design alternatives and configurations;
— confirmation of the ability of the system to meet its design reliability criteria;
— identification of problem areas such as:
  • single failure modes that can cause system failure;
  • cross links between systems;
  • areas requiring additional redundancy;
— input data for establishing priorities or corrective actions and trade-off studies;
— providing an objective evaluation of the design requirements related to redundancy, failure detection and annunciation systems, fail safe characteristics, and automatic and manual override features.

In addition, FMEA provides historical documentation for future reference to aid in the analysis of field failures, the evaluation of design changes and the comparison of in-service performance with predicted performance.

V.4. PREREQUISITES FOR PERFORMING AN FMEA

Before performing an FMEA, the analyst must define what constitutes the system under analysis and the extent or level of resolution of the analysis. The definition will include:

— the functional performance requirements of the system;
— the environmental and operational conditions under which the system is to perform;
— a clear statement of the physical bounds and interfaces;
— a definition of system failure;
— the level of resolution (subsystems or components) at which the analysis starts;
— the level of resolution (major system or overall plant) at which the analysis stops.

In addition to the foregoing, the objectives of the analysis and the assumptions must be clearly stated. The objectives of the analysis will dictate the level of resolution. Further, it is recommended that a review of relevant operational experience should be conducted to help identify all the applicable failure modes of the components of the system.
<table>
<thead>
<tr>
<th>Component identifier</th>
<th>Generic type</th>
<th>Location</th>
<th>Description</th>
<th>Status</th>
<th>Failure mode</th>
<th>Failure cause</th>
<th>Effects on</th>
<th>FT ident</th>
<th>Method of detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>HV</td>
<td>Actuated valve</td>
<td>×</td>
<td>Motor operated Solenoid actuated</td>
<td>Active</td>
<td>Spurious opening</td>
<td>Design fault, Defective maintenance, Abnormal environment</td>
<td>HVTSD1 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>I</td>
<td>Indicator</td>
<td>×</td>
<td>Any indicator</td>
<td>Passive</td>
<td>No output</td>
<td>Electrical fault, No signal from...</td>
<td>IFSA1 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(outside specification) (indicates high)</td>
<td></td>
<td></td>
<td>Electrical fault, Defective maintenance, High signal from...</td>
<td>IFSF1 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(outside specification) (indicates low)</td>
<td></td>
<td></td>
<td>Electrical fault, Defective maintenance, Low signal from...</td>
<td>IFSF2 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>M</td>
<td>Electric motor</td>
<td>×</td>
<td>Electric motor</td>
<td>Active</td>
<td>Excess output</td>
<td>Excessive mains frequency, Bearings seized, Internal electrical fault, Defective maintenance, Power supply failure, Control failure, Overheating, Lubrication failure</td>
<td>HFSJ1 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(in operation)</td>
<td></td>
<td></td>
<td></td>
<td>HFSH1 (× ×)</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
V.5. FORMAT OF THE ANALYSIS

A tabular worksheet format is recommended. Table XX depicts a typical format. The detailed design of the worksheet is at the discretion of the analyst or may be dictated by company procedures. However, it should allow the analyst to present the following information as a minimum:

1. A description of the component under consideration (component name, part number, function and the system in which it is used), specified by a unified subject index number;
2. A statement of the failure mode, e.g. for a valve, ‘failed open’;
3. A list of probable causes of failure;
4. A complete description of the effect of the failure mode at the subsystem level and, where relevant, at the system and overall plant level. If different effects occur in different environmental conditions, then a separate description must be written for each set of conditions, with a clear statement of the different effects;
5. A complete description of the failure symptoms, alarms and indications that would alert an operator to the failure;
6. A list of other failure modes which display the same symptoms;
7. A list of diagnostic actions to determine the actual failure mode;
8. A list of corrective actions by which the effects of the failure may be alleviated;
9. If the failure displays no symptoms, alarms or indications, i.e. it is dormant, a list of failures which in-combination with the dormancy would produce a noticeable effect;
10. Administrative data such as power plant, operating utility, report number, revision, date of issue, name of analyst.

Further additions are permissible as required by company policies, analytical details, etc., but no omissions from this list should be considered. Items (6), (7), (8) and (9) are iterative in nature; that is, as an analysis progresses, more failure modes with similar indications may be found and lists may need to be revised.

V.6. METHOD OF ANALYSIS

The analysis proceeds in a series of logical steps, as follows:

1. Gather all relevant design information for the system under consideration: design manuals, flowsheets, instrument loop diagrams, elementary electrical diagrams;
2. Determine the level at which the component breakdown is to be made for the initial iteration and list the system components;
(3) Using the worksheet format, identify the possible functional failure modes for each component, with their probable causes;

(4) Trace the effects of each failure to determine its effect at the relevant sub-system level; in the process, identify other failures with the same or very similar effects and indications;

(5) Check the diagnostic actions necessary to isolate the effects to a particular failure mode;

(6) Determine the corrective actions necessary;

(7) Repeat steps (4), (5) and (6) for each set of operating conditions that modify the effects of a failure mode;

(8) When the process is complete at the subsystem level, trace the effects of the failure through the system level and the overall plant level, as dictated by the requirements of the analysis.
Appendix VI

PROCEDURAL FRAMEWORK FOR THE ANALYSIS
OF COMMON CAUSE EVENTS

Appendix VI describes the procedural steps for a CCF analysis. Section VI.1 discusses in general terms the mechanisms that induce dependent events and how an understanding of these mechanisms can lead to the definition of CCF events. Section VI.2 briefly describes the procedural steps for CCF analysis. A detailed discussion of CCF analysis is given in Ref. [27] and additional critical comments and insights are given in Refs [26-28].

VI.1. FUNDAMENTALS OF CCF MECHANISMS

To understand and model dependent events, it is necessary to answer such questions as: Why do components fail or why are they unavailable? What is it that can lead to multiple failures? Is there anything at a particular facility that could prevent such multiple failures from occurring?

To answer these questions requires the consideration of three concepts. The first is the root cause of failure or unavailability. A root cause is the mechanism for a transition of state from available to the state of failure or functional unavailability. The degree of detail in specifying the root cause is dictated by how specific the analysis needs to be, but it is clear that a thorough understanding of dependent events and how they can be prevented can only come from a very detailed analysis of root causes.

Figure 7 shows a root cause classification system for dependent failures. This classification system includes different causes of dependence and CCFs. An important observation from Fig. 7 is that the causes of dependent (and common cause) failures are also the causes of single independent failures of plant equipment; the vast majority of equipment failures can be attributed to one or more causes of failures listed in Fig. 7. This factor is important in the analysis of root causes of CCFs because it implies that such an analysis cannot be fully separated from the more general root cause analysis of equipment failure.

This observation about the nature of the root causes of CCFs and single independent failures being the same leads to the second important concept in CCF analysis, the linking or coupling mechanism that leads to multiple equipment failure. The coupling mechanism explains why a particular cause affects several components. Obviously, each component fails because of its susceptibility to the conditions created by the root cause and the effect of the coupling mechanism in making those conditions common to several components.
Common cause failure causes

Engineering (E)
- Design (ED)
  - Functional deficiencies
    - Hazard undetectable
    - Inadequate instrumentation
    - Inadequate control
  - Realization faults
    - Channel dependence among operation and protection components
    - Operational deficiencies
    - Inadequate components
    - Design errors
    - Design limitations
- Construction (EC)
  - Manufacture
    - Inadequate quality control
    - Inadequate standards
    - Inadequate inspection
    - Inadequate testing
- Realization faults
  - Inadequate components
  - Design errors
  - Design limitations
- Operational deficiencies
  - Inadequate quality control
  - Inadequate standards
  - Inadequate inspection
  - Inadequate testing
- Inadequate testing and commissioning
- Inadequate quality control
- Inadequate standards
- Inadequate inspection
- Inadequate testing
- Inadequate testing and commissioning
- Inadequate components
- Design errors
- Design limitations
- Realization faults
  - Inadequate components
  - Design errors
  - Design limitations
- Operational deficiencies
  - Inadequate quality control
  - Inadequate standards
  - Inadequate inspection
  - Inadequate testing
- Inadequate quality control
- Inadequate standards
- Inadequate inspection
- Inadequate testing
- Inadequate testing and commissioning

Operations (O)
- Procedural (OP)
  - Maintenance and testing
    - Imperfect repair
    - Imperfect testing
    - Imperfect calibration
    - Imperfect procedures
    - Imperfect supervision
- Operation
  - Operator errors
    - Inadequate procedures
    - Inadequate supervision
    - Communication errors
- Operation
  - Operator errors
    - Inadequate procedures
    - Inadequate supervision
    - Communication errors
- Maintenance and testing
  - Imperfect repair
  - Imperfect testing
  - Imperfect calibration
  - Imperfect procedures
  - Imperfect supervision
- Imperfect repair
- Imperfect testing
- Imperfect calibration
- Imperfect procedures
- Imperfect supervision

Environmental (OE)
- Normal extremes
  - Temperature
  - Pressure
  - Humidity
  - Vibration
  - Acceleration
  - Stress
  - Corrosion
  - Contamination
  - Interference
  - Radiation
  - Static charge
- Energetic events
  - Fire
  - Flood
  - Weather
  - Earthquakes
  - Explosions
  - Missiles
  - Electric power
  - Radiation
  - Chemical sources

FIG. 7. Edwards's and Watson's classification system for common cause failures [43].
For example, suppose that two components located in the same room are both susceptible to high humidity. A common cause failure could occur as a result of an event at the plant that results in high humidity in this room. High humidity is the root cause of failure of both components. One immediately recognizable coupling mechanism is the fact that both components are located in the same room.

Another example of a dependent event that actually occurred at a nuclear power plant is the case of a redundant safety injection system that failed to actuate because of a design error in which the motor operated valves in the redundant pump trains were undersized and unable to open against the differential pressure created by the operation of the pumps. In this example, the root cause of failure of each valve is the inadequacy of the motor due to an error in the design process. The use of identical valves, the common demand conditions and the failure of the surveillance tests to reveal this deficiency prior to the actual demand form the coupling mechanism.

Dependent failures, and more specifically CCFs, can therefore be thought of as resulting from the concurrence of two factors, one that provides a susceptibility for components to fail or to be unavailable from a particular root cause of failure and a coupling mechanism that creates the conditions for multiple components to be affected by the same cause. This may be illustrated as:

Root cause → coupling mechanism → Component A
                        ↓ 
                        ↓ 
Component B  ↓  Component N

Root causes can be conveniently grouped into three major types according to the nature of the coupling mechanism:

Type 1. *Root causes that affect similar equipment.* Similar components are usually affected by the same installation, maintenance and testing procedures and by common design and manufacturing processes. These commonalities allow for multiple failures due to systematically repeated human errors. Therefore, for these causes of CCFs, the coupling mechanism is the equipment similarity and the component groups of interest are groups of similar

\footnote{Depending on how far back the identification of failure causes goes, high humidity could be considered as the immediate cause, being caused itself by some other causes; e.g. pump leakage. Hence, the term 'root cause' can imply different levels of deductive reasoning in establishing the cause.}
components. The CCFs resulting from root causes of this type are dependent events that can be either Type 2 (physical) or Type 3 (human) according to the classification of Section 4.4.

Type 2. **Root causes that affect equipment in the same location.** Common cause failures can also be attributable to adverse environmental conditions caused by fire, flood, moisture, etc. Most causes of harsh environmental conditions generate adverse conditions only within a limited area. The spread of the conditions is hindered or prevented by barriers to the environment (such as walls and fire doors) within the plant. Therefore, for environmental causes of CCFs, the coupling mechanism of interest is the susceptibility to a specific harsh environment and the location with respect to the origin of the harsh environment; that is, not separated from the cause of the harsh environment by barriers. This type of root causes generates CCFs that are subsets of Type 2 (physical dependences) dependent events as discussed in Section 4.4.

Type 3. **Root causes that affect equipment operated according to the same procedures.** Components that are all affected by the same emergency or normal operating procedures are also coupled because these components could all fail owing to a common operator error. Unlike the Type 1 root causes, common emergency or normal operating procedures may involve dissimilar components. Consequently, this type of root cause can affect dissimilar components generating dependent events of Type 3 in the classification scheme of Section 4.4. Very often the analyst will find that Type 3 root causes are also more likely to affect similar equipment; thus, a part of this type of root cause may be considered a subset of the Type 1 root causes that affect similar equipment. It is convenient, however, to consider these procedure related root causes as a separate type for analytical purposes. The advantage of considering this type separately is that a detailed analysis of emergency and normal operating procedures permits a closer scrutiny of the utility's testing, maintenance and operational activities. This in turn allows closer examination of the procedure related root causes of failure.

There is a third factor that enters into the determination of the potential for dependent failures, including common cause failures, and it is arguably the key determinant. This factor is the presence or absence of engineered or operational defences against unanticipated equipment failures. Typical tactics adopted in a defensive scheme include design control, segregation of equipment, well designed test and inspection procedures, maintenance procedures, review of procedures, training of personnel, and quality control in manufacturing and construction and in installation and commissioning. The different tactics may be particularly effective for mitigating specific types of dependent or common cause failures. As an example, physical sepa-
ration of redundant equipment reduces the chance of simultaneous failure of the equipment due to certain environmental effects. In this case, the defence acts to remove the coupling mechanism. Other tactics may be effective at reducing the likelihood of independent failures as well as dependent failures by reducing the susceptibility of components to certain types of root causes. Thus a complete treatment of CCFs should not be performed independently of an analysis of the independent failures; rather, the treatment of all failures should be integrated. Indeed, the procedural framework described in Section VI.2 places emphasis on the proper integration of the treatment of dependent and independent events.

Although the preceding discussion applies to all types of dependent failures, the thrust of common cause failure analysis is the treatment of those dependent events for which the dependence is not explicitly included in the logic model. From a probabilistic point of view, a dependence among two or more events means that the joint probability of their occurrence is not equal to the product of their individual probabilities of occurrence. Since we are interested in adverse dependences, the joint probability is higher than the product of the independent probabilities. Operationally, if two events A and B exhibit a dependence, then:

\[ P(A \text{ and } B) > P(A) \cdot P(B) \]

Common cause failure analysis considers those events for which the joint probability \( P(A \text{ and } B) \) is supplied directly (as an input) to the logic model. The procedural steps consist in identifying the events subject to CCFs, establishing the particular model that provides the joint probability of failure, determining and analysing the data on which the estimation of the parameter(s) of the model will be based, estimating the parameter(s) and quantifying the model. These steps are further discussed in Section VI.2.

VI.2. THE PROCEDURAL STEPS FOR COMMON CAUSE FAILURE ANALYSIS

This section is a brief description of the procedural framework that was developed in Ref. [27] for performing a CCF analysis. There are four major stages, each of which has a number of steps. They are summarized in Table XXI and discussed in this section.

The steps summarized in Table XXI represent a complete set of procedural steps to perform a CCF stand-alone analysis. A substantial portion of the CCF analysis is performed in connection with the development of the accident sequence modelling and in particular with Tasks 19 (system modelling) and 21 (qualitative dependence analysis), as well as the quantification of accident sequences in Tasks 27 to 31. The discussion that follows identifies those steps of CCF analysis
TABLE XXI. PROCEDURAL STEPS FOR A COMMON CAUSE FAILURE ANALYSIS

State 1: Steps in the development of the system logic model

1.1. System familiarization
1.2. Problem definition
1.3. Logic model development

State 2: Steps in the identification of common cause component groups

2.1. Qualitative screening
2.2. Quantitative screening

State 3: Steps in common cause modelling and data analysis

3.1. Definition of common cause basic events
3.2. Selection of probability models for common cause basic events
3.3. Data classification and screening
3.4. Parameter estimation

State 4: Steps in system quantification and interpretation of results

4.1. Quantification
4.2. Result evaluation and sensitivity analysis
4.3. Reporting

that overlap with the other tasks of the PSA and elaborates on those parts of the procedures that are more specific to the CCF analysis.

Stage 1: Development of the system logic model

Step 1.1. System familiarization

This is an essential element of any systems analysis. To be able to model a system, the analyst must understand the intended function of the system, its components and what procedures govern its operation, testing and maintenance. This is done in Task 16 (plant system requirements).

With regard to common cause failure, particular attention needs to be paid to identifying those elements of design, operation and maintenance and test procedures that could influence the possibility of multiple component failures. The information collected in this step is essential in the identification of potential sources of dependence and the grouping of components in the screening phases of the analysis (Steps 2.1 and 2.2).
Step 1.2. Problem definition

In this step, the analysis boundary conditions, such as the physical and functional system boundaries of the system, functional dependences on other systems (support systems), functional interfaces with other systems, and system success criteria need to be defined. This is done in Tasks 16, 18, 19 and 21 of the PSA. For CCF analysis, those root causes of dependence that are to be explicitly modelled should be identified. For example, certain categories of human errors, such as calibration errors and errors in returning equipment and systems to their original configuration after testing and maintenance, are typically modelled explicitly. Hence many important classes of common cause events are, or may be, modelled explicitly in the system logic models, depending on the application. This process then defines the scope of the residual common cause failure analysis in terms of the root causes that should be considered as a group in the common cause events rather than individually; the analyst must define a sharp boundary between the residual common cause events and those common cause and other events to be modelled explicitly.

Step 1.3. Development of the logic model

In this step, the system logic model is developed; for example, a system fault tree. This is Task 19 of the PSA procedures.

Stage 2. Screening of common cause component groups

The objectives of the screening stage include:
- identifying the groups of system components to be included in or eliminated from the CCF analysis;
- prioritizing the groups of system components identified for further analysis so that time and resources can be best allocated during the CCF analysis;
- providing engineering arguments to aid in the data analysis step (Step 3.3);
- providing engineering arguments to formulate defence alternatives and stipulate recommendations in Stage 4 (Interpretation of results).

These objectives are accomplished through the qualitative and quantitative screening steps. These two steps are presented separately, but they can be, and often are, performed interactively.

Step 2.1. Qualitative screening

In this step, a search is made for common attributes of components and mechanisms of failure that can lead to common cause events. Past experience and engineering intuition are used to identify obvious signs of dependence among redun-
tant components. Also, experience and intuition are used to assess the effectiveness of defences there may be to preclude (or reduce the likelihood of) the occurrence of certain CCF events. For example, an analyst may assume that dissimilar components are unlikely to experience a CCF. This assumption is supported by operational experience (Refs [44, 45] present hundreds of CCF events that affected identical components but few, if any, that affected diverse, redundant components). This research identifies initial groups of system components to be included in the analysis.

This step is very important and should be conducted in conjunction with Tasks 19 and 21 of the PSA procedures. The identification of the common attributes of components and mechanisms of failure that can lead to common cause events at this stage will influence the development of the system models (Task 19). These aspects are included or can be easily added in the system models to facilitate the identification of accident sequences that contain events subject to common failures (Tasks 27 and 31).

Next, a formal analysis of the root causes of equipment failure is performed to substantiate (or improve) the initial search. For increased efficiency, the root cause analysis can be performed following the quantitative screening (Step 2.2). (In this way, the analyst can focus on dominant CCF contributors to system unavailability in performing Step 2.1.) The analysis of root causes of failures focuses on the three root cause types previously defined: (1) root causes that affect similar equipment; (2) root causes that affect equipment in the same location; (3) root causes that affect equipment operated according to the same procedures.

**Step 2.2. Quantitative screening**

In this step, a generic value is assigned to the probability of each CCF event in the system fault tree. The system unavailability is evaluated using the generic data, and the dominant contributions to the system unavailability are identified. These dominant contributors will be emphasized in Stages 3 and 4.

The quantitative screening step is essential for performing an efficient CCF analysis at the plant (i.e. an accident sequence CCF analysis). This is due to the fact that an accident sequence CCF analysis covers a large number of CCF events and a large number of accident sequences; thus, prioritizing CCF events increases the efficiency of the analysis. In fact, this is the procedure adopted in this report. A complete CCF analysis will be performed for those failures that are assessed to make a substantial contribution to the probability of core damage in the sensitivity and importance analysis of Task 31.

Finally, several factors in the quantitative analysis of accident sequences will affect the contribution of CCFs to the frequency of accident sequences. Some of these factors tend to affect different CCF contributors in different ways. In particular, recovery considerations will affect the relative contribution of CCF scenarios not only to accident sequence frequencies but also to system unavailabilities. Thus,
recovery considerations (even if only of a preliminary nature) can play an important role in the quantitative screening step, since the purpose of this step is to permit concentration on dominant CCF scenarios as early in the analysis as possible.  

Stage 3. Common cause modelling and data analysis

Step 3.1. Definition of common cause basic events

To model common cause failures, it is convenient to define common cause basic events; that is, basic events that represent multiple failures of components from shared root causes. This step also leads to a redefinition of the single component basic events. Definition of new basic events leads (for some system modelling techniques) to a redefinition of the structure of the logic model to include the new events.

Step 3.2. Selection of probability models for common cause basic events

The objective of this step is to construct models that provide the necessary input to the logic model in Step 3.1 for quantification. This is done by associating a probability model, such as the constant failure rate model or the constant probability of failure on demand modes for each basic event (common cause or independent).

Each model has one or more parameters, estimation of which is based on analysis of the operational data and specific assumptions. Some of these models are presented in Ref. [27]; a critical review of corresponding applications together with insights is given in Refs [26, 28 and 29]. This step strongly interacts with Step 3.1 since the choice of model affects the definition of the basic events and vice versa.

Step 3.3. Data classification and screening

The purpose of this step is to evaluate and classify event reports to provide input to parameter estimation (e.g. beta factors). It is necessary to take care to distinguish between events whose causes are explicitly modelled and those that are to be included in the residual common cause event models. The sources of data available to the analyst are event reports on both single and multiple equipment failures. Since plant specific data on multiple equipment failures are usually rare, it is necessary to extend the search to other plants. However, since other plants may be designed or operated differently, events that have occurred at one plant may possibly not occur at another. Thus, the data should be carefully reviewed for applicability. This review concentrates on root causes, coupling mechanisms and defensive strategies at the plant of interest. Since the event reports are generally not as detailed as an analyst

---

5 This statement is made on the assumption that recovery considerations are to be included in the PSA.
would like, their analysis requires much judgement, and a systematic approach to this screening is essential for examinability and reproducibility of the analysis. The root cause analysis performed in Step 2.1 provides useful insights for this step.

**Step 3.4. Parameter estimation**

The purpose of this step is to use the information obtained in Step 3.3 on the numbers of applicable events of single and multiple failures to obtain numerical estimates of the parameters of a common cause probability model. There are several sources of uncertainty, including the interpretation of the data to elicit causal mechanisms, the assessment of their impact at the plant being modelled, and uncertainty about how the data were obtained. Consequently, it is desired not only to provide a point estimate but also to characterize this uncertainty numerically. Reference [27] provides specific estimation procedures for the various CCF models.

**Stage 4. Interpretation of results**

**Step 4.1. Quantification**

The event probabilities obtained for the common cause events in Stage 3 of the analysis are incorporated into the solution for the unavailabilities of the systems or into event sequence frequencies in the usual way cut sets are quantified. This is done in Tasks 27 and 31 of the PSA.

**Step 4.2. Uncertainty and sensitivity analysis**

The detailed CCF analyses are to be performed for those groups of components identified in the sensitivity analysis outlined in Task 31 of the PSA procedures as having the potential substantially to affect the final results. For those groups of components a detailed CCF analysis will be performed but, as has been pointed out, there is considerable uncertainty in the selection of the right CCF model and in the estimation of the corresponding parameters. An uncertainty analysis is therefore recommended to integrate the effect of these CCFs into the general uncertainty in the probability of core damage. In addition, further sensitivity (with respect to the model and the parameters) would help to illustrate the direct relation between the assumptions, the input values and the general results.

**Step 4.3. Reporting**

The final step is the reporting of the analysis. It is particularly important to be clear in specifying what assumptions have been made and to identify the consequences of using these and other assumptions. Further guidance on reporting requirements is given in Section 7.

136

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
Appendix VII

INTERFACE WITH LEVEL 2 AND LEVEL 3 PSA ANALYSES

Appendix VII briefly reviews the general characteristics of Level 2 and Level 3 PSAs in order to identify the constraints or demands that an extension of the study to these levels can impose on the Level 1 PSA.

VII.1. LEVEL 2 ANALYSIS

A Level 2 analysis is a probabilistic treatment of events in the primary circuit and the containment from the onset of core degradation to the release of radioactive material from the containment. Containment event sequences are mostly represented in event trees with branch points that correspond to those events that can ultimately influence the probability of containment failure. More specifically, the branch points and their quantification concern the following issues:

- phenomena related to degraded core behaviour;
- phenomena in the containment;
- containment pressure capability and failure mode;
- timing issues;
- performance of containment engineered systems;
- dependences.

These issues are influenced by the conditions in which the degradation of the core has taken place, including the availability of containment safeguards. In general, the branch point probabilities will depend on these conditions. Extension of a Level 1 PSA to Level 2 and Level 3 therefore requires that the end states of the Level 1 event trees be categorized (plant damage states) in terms of the conditions that have a significant influence on the structure and quantification of the containment event trees. Some indication of the conditions that are likely to define plant damage states with respect to the foregoing issues are given in the following.

(a) The behaviour of the degraded core at the time of vessel breach will depend on whether the vessel is pressurized or not. This in turn may depend on whether a transient or LOCA has occurred. If the vessel is pressurized, molten fuel could be dispersed into the containment and could heat the containment atmosphere. The dynamics and heat transfer processes will be different if instead the molten fuel were to drop under gravity from an unpressurized vessel. Hence the containment pressure and other subsequent phenomena in the containment could also differ (for example, debris behaviour, fuel/coolant
interactions, hydrogen generation, fission product release). These in turn will influence the probability and/or time-scale of containment failure.

(b) The timing of core degradation will also influence the pressures generated and the subsequent behaviour of molten fuel or debris in the reactor pressure vessel. These in turn can influence the mode of vessel failure (if it occurs) and the processes occurring within the containment after failure of the vessel. The timing of core degradation will depend on the causes (for example, which safety system has failed).

(c) Another condition would be whether the accident is accompanied by containment isolation failure or bypass of the containment (such as an interfacing LOCA or a steam generator tube rupture).

(d) The availability of containment safeguards (such as sprays and/or coolers) will influence, for example, pressures in containment and fission product behaviour. The availability (or survivability) of these safeguards may depend on the other conditions (such as those described) that define the plant damage states.

The functional dependences between safety systems required to prevent degradation of the core and the containment should also be represented in the Level 1 PSA. Two examples of these are:

(i) The availability of containment safeguards could be influenced by various supporting systems (for example, electrical power) that have also contributed to the core damage event. There would be a need to distinguish between these different circumstances in the Level 1 PSA in order to quantify the containment trees correctly.

(ii) A further link that should be allowed for in the Level 1 PSA is that arising from dependence between the containment state and the systems required to prevent core damage (for example, the source of water for pumped recirculation to the core depends on successful containment isolation).

Some detailed consideration of such dependences between the Level 2 and the Level 1 PSAs should be given in the actual selection of methods for the Level 1 PSA. The plant damage states could be represented as top events in large fault trees or as end points of event trees. The discrimination required for containment analysis as described would be required in both methods. Optimization of the method would consider this with regard to the plant under analysis and the analytical tools available.

It should be stressed that the foregoing are merely examples to illustrate the issues that need to be addressed in the Level 1 PSA if it is to be extended to Level 2, even if this is not to be done until a later stage.
VII.2. LEVEL 3 ANALYSIS

A Level 3 analysis covers the treatment of releases from the containment, the dispersion of radioactive materials and the evaluation of risk in terms of frequency of consequences to people and the environment (such as health effects, land contamination or economic effects). These consequences will depend on a number of factors related to the magnitude, timing and various other characteristics of the release. These characteristics may be influenced either directly by issues that are part of the Level 1 analysis or indirectly via the Level 2 analysis. Examples of aspects that may be influenced by these issues and may themselves in turn influence the Level 3 analyses are:

— early or late containment failure (or bypass);
— the chemical and physical forms of released radionuclides;
— the magnitude and energy of radioactive releases.

VII.3. FURTHER GUIDELINES FOR LEVEL 2 AND LEVEL 3 ANALYSIS

Appendix VII considers only the interface between the Level 1 and the Levels 2 and 3 PSAs. Future IAEA reports will present detailed guidelines for Levels 2 and 3 PSAs. The guidance given in Appendix VII will then be reviewed and possibly expanded to provide a more detailed definition of the interface between Level 1 and Levels 2 and 3 PSAs.
Appendix VIII

STRUCTURE OF THE PSA REPORT

Appendix VIII provides details on the contents of the PSA report, namely the summary report, the main report and the appendices.

VIII.1. SUMMARY REPORT

The purpose of the summary report is to communicate the project's 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.

The summary report could consist of the following six sections:

1. Introduction
2. Results of the analysis
3. Results of the importance and sensitivity analyses
4. Interpretation of results, conclusions and recommendations
5. Overview of methods
6. Organization of the report

The contents of each section are discussed in the following subsections.

VIII.1.1. Introduction

Section 1 of the summary report provides information on the background, motivation, objectives and scope of the study. It also provides a brief description of the project organization and management, the major tasks of the study and the organization of the summary report. Section 1 of the summary report is a condensed version of Section 1 of the main report.

VIII.1.2. Results of the analysis

Section 2 of the summary report summarizes the most important results of the study, which include the following:

(a) Point and uncertainty estimations of the core damage frequency together with relative contributions from the various initiators and the categories of plant damage states.

(b) A list of dominant accident sequences (contributing at least 10% to any of the plant damage states) together with point and uncertainty estimations of the corresponding frequencies.
— A description of each of the dominant accident sequences should be provided. This description should briefly discuss the nature of the initiating event and of the additional system failures in the sequence (and their impact on the maintenance of the plant's critical safety functions). The major contributing failures associated with each system failure should be presented. Any significant dependences between the events in the sequence should be discussed.

— The tabulations of dominant accident sequences must allow a determination of the source of the sequences and the constituent elements of the sequences. This will entail sequence descriptions which refer to sections in the main report relating to the source event tree, relevant fault trees and failure rates associated with contributing events.

For example, a tabulation of an accident sequence might be:

<table>
<thead>
<tr>
<th>Point value</th>
<th>5%</th>
<th>50%</th>
<th>Mean</th>
<th>95%</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0(-7)</td>
<td>1(-7)</td>
<td>5(-7)</td>
<td>1.2(-6)</td>
<td>5(-6)</td>
</tr>
</tbody>
</table>

Sequence: A B C (Frequency = \(1 \times 10^{-6}/a\))

Initiating event A entails a small steam line break outside the containment. A more detailed description of Initiating event A is found in Section X of the main report. The event tree developed for A is presented and discussed in Section Y of the main report.

System B is designed to /.../. A more detailed description of System B can be found in Section W of the main report and additional information related to its response to A is presented in Section Z. An important dependence between the occurrence of A and the performance of System B was identified to be /.../. A more detailed discussion of this interaction is presented in Section X.

The fault tree for System B is presented in Section X. The major contributing cut sets (conditional upon A) are:

\[
(C_1, C_2) = (1.0 \times 10^{-2}) (5.0 \times 10^{-2}) = 5 \times 10^{-4}
\]

\[
(C_1, C_3) = (1.0 \times 10^{-2}) (1.0 \times 10^{-2}) = 1 \times 10^{-4}
\]

\[
6 \times 10^{-4}
\]

\(C_1\) is the failure of Valve xyz to open on demand. \(C_2\) is the failure of the operator to notice this failure and manually open the valve. \(C_3\) is the failure of the switch which allows manual opening of the valve. These failure events are discussed in more detail in Section X of the main report and Appendix Y. The failure probabilities for \(C_1\), \(C_2\) and \(C_3\) are discussed in Section Y (Fault trees) and Section Z (Failure data) of the main report.
— A ‘road map’ from the dominant accident sequences to the relevant sections of the main report should be provided in tabular form. See, for example (this is only an example; actual headings will differ), Table XXII.

c) Modularized logic trees depicting major contributors to system failures. These can be a valuable aid to the high level peer reviewer in conjunction with the discussion format recommended earlier for dominant accident sequences. It is recommended, therefore, that such trees be provided for the most important systems. This is not a substitute for the presentation of the actual trees used in the study but simply a pictorial method of presenting the conclusions.

d) A qualitative discussion of the uncertainty in the results, in addition to the quantitative statements of uncertainty provided for the frequency of core damage and the various accident sequences. The discussion should cover the sources of uncertainty, the methods of treatment in the study and the effects on the results.

e) A list of the identified dependences and a brief description of their nature.

VIII.1.3. Results of the importance and sensitivity analyses

Section 3 of the summary report documents the results of the importance and sensitivity analyses, which can include lists of:

(a) the relative importances of initiating events with respect to core damage frequency;
(b) the relative importances of individual sequences to the core damage frequency;
(c) the relative importances of various systems with respect to the core damage frequency;
(d) the relative importances of various human errors with respect to the core damage frequency;
(e) the relative importances of test and maintenance unavailabilities;

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Initiating event</th>
<th>Event tree</th>
<th>System descriptions</th>
<th>System interactions</th>
<th>Fault trees</th>
<th>Failure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>2.2.1</td>
<td>5.3</td>
<td>4.1 (A)</td>
<td>13.3.1</td>
<td>4.1 (A)</td>
<td>7.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.2 (B)</td>
<td></td>
<td>4.2 (B)</td>
<td>7.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.3 (C)</td>
<td></td>
<td>4.3 (C)</td>
<td></td>
</tr>
</tbody>
</table>
(f) the relative importances of specific hardware failures or classes of hardware failures;
(g) various assumptions and issues that have been included in sensitivity studies on core damage frequency.

VIII.1.4. Interpretation of results, conclusions and recommendations

Section 4 of the summary report provides an interpretation of the substantial amount of information presented so far, draws certain conclusions and presents the recommendations of the study.

The major contributors to the frequency of core damage in terms of accident sequences, initiators, systems, human actions and components are discussed. The identified dependences are also discussed and evaluated. Engineering insights and plant features important to safety should be presented in the light (and in terms) of the results of the study.

The dominant accident sequences and the results of uncertainty and importance analyses of the subject plant should be compared with those of similar plants that have been studied, highlighting differences in assumptions between studies and, where appropriate, qualitatively characterizing the effect of credible changes in modelling assumptions.

The results should also be examined and commented upon in the light of existing plant specific regulatory issues. It would also be useful to discuss existing or pending regulatory requirements in the light of the results being presented in the study and to show how they have influenced the conduct of the PSA.

Recommendations on possible design or procedural changes and possible uses of the PSA models and results, as well as on further analyses, should be proposed and discussed in this section.

Finally, any limitations and constraints associated with methods and input data together with their impact on the PSA results should be proposed and discussed in this section.

VIII.1.5. Overview of methods

Section 5 of the summary report presents a general overview of the procedures and methods adopted in the conduct of the PSA. The reasons for selecting the particular methods and a brief overview of their key elements should be presented in such a way as to permit a high level reviewer to assess the adequacy of the methods for the purposes of the given PSA study.

Advances in techniques should be described. If special techniques were used in performing the study, these should be briefly discussed, and dealt with in detail in a separate section of the main report or in its appendices.
Section 5 should also report on activities undertaken to ensure the completeness and adequacy of the models, particularly of the initiating events, the identification of failure modes associated with each event tree heading and the identification of dependent failures and human interactions. Any other issue or key factor in the ultimate credibility and qualification of the results should also be presented in this section.

Finally, a special subsection should describe the activities undertaken to ensure the technical quality of the study.

VIII.1.6. Organization of the report

Section 6 of the summary report provides an overview of the organization of the external (published) documentation of the study (summary report, main report, appendices to main report) and guides the reader to the parts of the documentation that deal with specific items. It would be desirable to include in this section an index ("road map") relating sections of the summary report to sections of the main report and the appendices, as in Table XXIII.

TABLE XXIII. RELATION BETWEEN SUMMARY REPORT AND MAIN REPORT

<table>
<thead>
<tr>
<th>Summary report section</th>
<th>Corresponding main report section(s)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.3. Fault tree analysis</td>
<td>M.4.1. Fault tree methods</td>
<td>Appendix A.9 contains complete fault trees and fault summaries and the database</td>
</tr>
<tr>
<td></td>
<td>M.4.2. System fault trees</td>
<td></td>
</tr>
<tr>
<td></td>
<td>M.9.2. Linking of fault trees</td>
<td></td>
</tr>
</tbody>
</table>

VIII.2. MAIN REPORT

The main report should describe in depth all tasks of the PSA including the tasks related to organization and management. In addition, the main report should provide the necessary links between different parts of the report and the appendices to help the reader to locate any additional information on specific issues of interest.
VIII.2.1. General structure of the report

The general structure of the main report could parallel the major procedural steps described in the present report, and thus could comprise the following sections:

(1) Overview of the study
(2) Plant and site description
(3) Identification of radioactive sources, accident initiators and plant initiators
(4) Accident sequence modelling
(5) Data assessment and parameter estimation
(6) Accident sequence quantification
(7) Display and interpretation of results.

VIII.2.2. General guidelines for reporting the PSA tasks

Regardless of the specific characteristics of each PSA task, the report should deal with the following:

— assumptions and inputs for each task;
— methods for each task;
— products of each task.

Assumptions and inputs for each task

The requirements of each task should be summarized. The source of each input should be defined (that is, which inputs come directly from other tasks in the study, which are generated through interactive loops with other tasks, which originate outside the study).

Inputs generated outside the study should be given either in the main report with specific sources cited or in the appendices. Inputs generated within the study as outputs of other tasks are to be given in any event.

The limitations and qualifications of the available information and databases should be discussed. The applicability of the sources to the general requirements of the task should be evaluated with respect to their effect on the quality of the task output.

Methods for each task

This report admits of considerable latitude in the choice of methods for several of the tasks. In several areas, advances in techniques are expected. The following treatments of the methods should therefore be provided so that the reports are self-contained.
— an outline of the general methodology;
— definition and discussion of inherent limitations of the methods or practical constraints encountered during implementation;
— discussion of the impact of these limitations and/or constraints on the quality of the output of the task;
— benchmarking or referencing of the methods if new or significantly different from past applications;
— if computer codes are used, references to users' manuals and a brief discussion of the code consistent with the aforementioned items. Any new validation and verification process should be referenced. Input decks for computer runs should be provided, both in printed form and in machine readable forms (e.g. magnetic tape, diskettes), as part of either the appendices or the internal documentation;
— the uncertainties and sensitivities associated with the parameters and the models/methods should be quantified to the extent necessary to support the decision making goals of the PSA.

Products of each task

The view adopted in this report is that the products of each task are 'results' of the PSA which compare in importance with the final core damage frequencies. Nominally, each task is a stepping stone on the path to the final answer; but for future users of the model, the intermediate results of the various tasks are as important as the contents of the results section. Moreover, clear presentation of intermediate steps is a prerequisite to a successful detailed technical review and decision making process.

Certain of the required outputs cannot usefully be printed as part of the report (or can be printed only by particular computer codes in particular formats). An example of this is the task output 'Boolean equations for each accident sequence of each event tree'. With all events developed down to basic component failures, such an expression is so large as to be useless. In such a case, it is appropriate to provide an abbreviated version in print (for example, a few leading terms) and a machine readable version. The goal is to permit users of the study to make use of products that have been generated in the PSA.

VIII.2.3. Contents of the individual sections

Detailed contents of individual sections of the main report are discussed in the remainder of this subsection. Subsections VIII.2.3.1–VIII.2.3.7. correspond to Sections 1 to 7 of the main report.
VIII.2.3.1. Overview of the study

Section 1 of the main report provides a brief overview of the project. It is recommended that this section be organized as follows:

1.1. Background and objectives of the study
1.2. Scope of the study
1.3. Project organization and management
1.4. Project implementation
1.5. Overview of procedures and methods
1.6. Report organization.

Section 1.1 presents the background of the project and the specific objectives defined by the organization commissioning the study.

Section 1.2 is devoted to the presentation of the scope of the study. It should be specified in terms of parameters characterizing the scope of a PSA as discussed in this report (see Section 2.2).

Section 1.3 describes the project team organization and the project management, including organizations participating in the project, type and extent of participation, lines of communication and the flow of information. Section 1.4 discusses further aspects of project implementation including the structure and scheduling of major tasks. Section 1.5 is devoted to a brief presentation of the PSA process, considering all PSA steps and focusing on points unique to, or of particular interest in, the study. A brief overview of the methods used in different tasks should also be provided.

Section 1.6 should provide guidance enabling the interested reader to find more information on a specific topic in the main report and the appendices. Contents of individual sections should be briefly described. Appropriate cross-references between the sections of the main report and the appendices should be given.

VIII.2.3.2. Plant and site description

Section 2 of the main report provides a brief description of the plant and its size. The information is oriented to provide bases for more detailed presentation of the PSA tasks in subsequent sections of the main report. It is recommended that this section should have the following structure:

2.1. General plant characteristics
2.2. Plant systems
2.3. Plant site.

Section 2.1 includes a general description of the plant. The main design characteristics of the plant are provided.
Section 2.2 provides a brief description of all plant systems that are included in the study.

Section 2.3 presents general characteristics of the plant site, including topographic, meteorological and demographic data. For a Level 1 PSA some of these data (e.g. demographic data) are not used as inputs and need not be very detailed.

Plant/system related information included in this section is limited to general design information and functional descriptions. More detailed and specialized information on systems design should be contained in the appendices.

VIII.2.3.3. Identification of radioactive sources, accident initiators and plant response

Section 3 of the main report provides the necessary inputs and products of the tasks that form the basis of the plant model (Tasks 9–17).

The general structure of this section parallels the corresponding procedural steps as follows:

3.1. Sources and conditions of radioactive releases
3.2. Selection of initiating events
3.3. Plant functions and systems relations
3.4. Plant system requirements
3.5. Grouping of initiating events

Section 3.1 addresses:

— the possible sources of radioactive releases from the plant;
— the operational states of the plant selected for detailed consideration;
— the definition of core damage states or other consequences of concern (if considered).

The product should be consistent with the objectives and scope of the analysis as specified in Section 1 of the main report. If the scope of the study is limited to a particular selection of sources and conditions of release, the reasons should be explained.

Section 3.2 describes the general approach to the selection of the initiating events (such as reference to existing list, engineering evaluation, deductive analysis of the plant or operational experience) and provides lists of initiating events on the basis of a preliminary categorization as follows:

— list of LOCA break sizes;
— list of interfacing system LOCAs;
— list of LOCAs that affect mitigating systems;
— list of transients applicable to the subject plant, including both generic and plant specific transients;
— list of transients initiated by support system faults that affect mitigating systems.

Section 3.3 presents and discusses the following:
— the functions incorporated into the design of the plant for preventing or mitigating the consequences of core damage (or other consequences) following an initiating event;
— relations between safety functions and plant systems; this section also contains the following specific outputs:
  • a list of safety functions that were generally applied in constructing the plant model together with a discussion of how the functions were selected;
  • a table relating plant systems to the function they perform and a discussion of the sources of information used;
  • a list of front line systems;
  • a list of support systems;
  • tables or diagrams of dependences among front line systems and support systems;
  • tables or diagrams of dependences among support systems.

Detailed descriptions of the systems should be provided in appropriate sections of the appendices and referred to in the relevant subsections.

Section 3.4 discusses the required performance of front line systems (minimum success criteria) associated with each initiating event. The development of minimum success criteria should be briefly described and reported in the form of:
— a table giving for each LOCA category the mitigating systems, their success criteria and reference to supporting documentation;
— a table giving for each transient category the mitigating systems, etc.

Detailed information on the selection of the success criteria, particularly if less conservative than in the final safety analysis report, should be supplied in the appendices. Reference to the corresponding section should also be provided.

Section 3.5 is devoted to further refinement of the initial list and covers the process of final categorization and grouping of initiating events. The information provided in this section should include:
— a description of approaches adopted (such as detailed analysis of plant response, screening based on approximate frequencies, identification of events, comparison with operational experience);
— a table of all the initiators analysed together with appropriate explanation and final categorization;
— a list of the final groups of accident initiators, including the designator abbreviation, a short title to be used throughout the report, a brief description and the mean values of the frequencies. Appropriate subsections of Section 5 of the main report where the derivation of the frequencies are discussed should be referenced.

VIII.2.3.4. Accident sequence modelling

Section 4 of the main report contains the necessary input, methods and products of the tasks that develop the model of the plant (Tasks 18-23). The general structure of this section follows that of the major procedural step of plant model development and consists of six subsections:

4.1. Event sequence modelling
4.2. System modelling
4.3. Human performance analysis
4.4. Qualitative dependence analysis
4.5. Impact of physical processes in the progression of accident sequences
4.6. Classification of accident sequences into plant damage states.

Section 4.1 provides the qualitative description of the modelling of the plant response to every group of initiators (Task 18). The models/methods used in the modelling of the event sequences that lead to a successful plant state or to a damage state following an accident initiator should be described and explained, including:

— a phenomenological description of disturbances caused by the initiating events;
— a discussion of mitigating functions and systems;
— a description of the plant parameters responsible for actuation of protective systems (manual or automatic);
— a statement of the simplifying assumptions concerning plant design, operating or response.

Any event sequence diagrams that have been developed in support of the plant response modelling should be presented and clearly explained. If the method chosen for accident sequence modelling is that of event trees, all types of event trees developed (functional event trees, system event trees, time phased event trees) should be presented together with the following information:

— the headings of the event trees and a brief description of the corresponding event;
— a discussion of the ordering of event headings;
— the functional, phenomenological and hardware dependences between the event headings for each event sequence;
— a brief description of each event sequence in the tree together with explanations of branch points for which a success/failure choice has been omitted;
— a description of timings and sequencing of failures in the event sequence;
— a reference to any detailed final safety analysis report or other analysis used in the determination of sequence progression;
— a mnemonic designator depicting each individual sequence in terms of the event successes or failures;
— identification of the system models that provide input to each event tree heading and reference to the appropriate section of the main report and/or the appendices;
— a core damage designator characterizing each individual sequence in the context of the parameters important to physical processes associated with the damage to the core.

Section 4.2 contains the qualitative description of the system models developed in support of the accident sequence modelling effort (Task 19). Only the most important information on the system models are presented in the main report; the bulk of it is included in the appendices. Section 4.2 should contain:

— a list of the systems analysed, with appropriate reference to the appendices;
— information sources used in the analysis;
— a discussion of top events (for fault trees, success criteria and boundary conditions imposed by sequence logic);
— general modelling assumptions, including maintenance and testing unavailabilities, human error contribution, common cause failures, recovery;
— brief comments on the level of resolution of the basic events of the models;
— a discussion of system model modularization;
— a list of the most important basic event combinations (cut sets) that cause system failure.

Section 4.3 documents the results of human performance analysis (Task 20) and contains a list of the human errors considered in the analysis and the screening probabilities for each:

— a list of human errors modelled at the accident sequence level;
— a list of human errors eventually included in the system models;
— a description of the quantification model/procedure for each human error together with the source of data for the quantification;
— a list of recovery actions with the associated component sequences considered in the models.

Section 4.4 summarizes the results of qualitative dependence analysis (Task 21). This task is an integral part of event tree/fault tree development for any other combination of plant/system modelling approaches); however, the topic should be discussed separately because of its importance.
The following information should be provided:

— A brief explanation of the exact scope and treatment of the important types of dependences, including:
  • hardware coupling;
  • functional and process coupling;
  • multiple dependent failures due to commonalities in location or environment;
  • multiple dependent failures identified by reviewing operating experience;
  • initiator and location dependent effects caused by external events;
  • the effects of initiating events on the responding system;
  • human interactions.
— An identification of methods used in searching for and handling the dependences with appropriate references, and a brief description of methods that have not been published.
— The specific sources of information (other than those discussed in event tree and fault tree analysis tasks) used to identify the functional and phenomenological dependences.
— An enumeration and short description of specific dependences that were identified, including:
  • the specific human actions that couple components or system failure;
  • the individual events that were searched for susceptibilities to potential coupling mechanisms
  • the failures that appeared in more than one fault tree corresponding to the system function.

Section 4.5 provides a discussion of any effects of physical processes on systems included in the analysis.
Section 4.6 discusses the classification of accident sequences into categories according to the degree of severity of the resulting core damage. All assumptions and simplifications should be listed and elaborated upon.

VIII.2.3.5. Data assessment and parameter estimation

Section 5 of the main report provides the inputs, methods and products of the development of the database (Tasks 24 and 26), for the frequency of initiating events and component failure rates, for maintenance and repair parameters, and for human error probabilities.
This section could be divided into three subsections:

5.1. Initiating event data and frequencies
5.2. Component data and parameters
5.3. Human performance data and parameters.
Each of these subsections should provide general information on inputs, methods and results. The following issues should be discussed:

- event definitions and models (with their parameters);
- data source identification and data gathering, including generic and plant specific data sources;
- the methods for processing raw data;
- the methods for combining generic data with plant specific data (such as plant specific Bayesian);
- assumptions and preconditions with the impact of modelling assumptions on the results;
- the nature of uncertainty associated with the data, including:
  - incompatibilities or uncertainties between the data source and the plant analysis requirements;
  - variabilities in the data;
  - lack of experimental data;
  - quality of raw data collection (for example, limited documentation of success).

In addition to the foregoing information, final data tables should be provided. They should contain upper and lower bounds (percentiles) and mean values for each event required by the plant model. Any special points should be noted and discussed in the accompanying text.

Corresponding sections should address the specific types of data.

Section 5.1 should discuss the initiating event frequencies, including transients, losses of reactor coolant system integrity and external events. Treatment of rare event initiators is a specific issue that should be included.

Section 5.2 discusses the quantification of the component related basic events in the system models. Independent failures, common cause failures, testing, maintenance and repair parameters should be presented. The methods adopted and the sources of raw data used for estimating the various parameters are discussed.

Section 5.3 should include information on the quantification of the parameters of the human performance models.

More detailed information concerning data assessment should be provided in the corresponding appendix. Appropriate references should be given in this section.

VIII.2.3.6. Accident sequence quantification

Section 6 of the main report describes the inputs, methods and products of the tasks associated with the quantification of the accident sequences (Tasks 27-31). It is recommended that this section should have the following organizational structure:

6.1. General concept of the quantification process
6.2. Analysis of system models
6.3. Accident sequence quantification
6.4. Uncertainty analysis
6.5. Importance and sensitivity analysis
6.6. Description of computer codes used in the analysis.

Section 6.1 provides a brief overview of the steps in an accident sequence analysis. The description of each step should be presented together with the inputs and products of each step. The iterative character of the process should be pointed out. All elements of the quantification analysis discussed in the remainder of Section 6 should be briefly discussed in this section, including:

- initial solution of system models;
- initial solution of accident sequences;
- review of results and iteration;
- final quantification of accident sequences;
- uncertainty analysis;
- importance and sensitivity analysis.

References to appropriate sections of Section 6 should be given in this section.

Section 6.2 describes the first step of the quantification process, that is, the quantification of system models. In the remainder of this description of Section 6 of the main report, it will be assumed that fault trees have been selected for system modelling and the large fault tree/small event tree approach has been followed in the quantification of the accident sequences. The underlying principles, however, are applicable to all kinds of system models and approaches to accident sequence quantification.

The following issues should be addressed in this section:

- merging the front line system fault trees with their support systems;
- development of independent subtrees (modularization);
- system fault tree solution and quantification including truncation;
- reviewing the systems analysis and refinement of the fault tree logic and data.

A brief description of these tasks should be provided. Methods and assumptions used in the analysis (such as truncation criteria) and discussion of the product should be included, with references to where in the documentation the more detailed information may be found.

Section 6.3 should discuss the process of forming the accident sequence fault trees and their initial quantification. The following aspects of the analysis should be addressed in this section:

- integration of the event trees, fault trees and database as the input to the accident sequence analysis;
- accident sequence level modularization;
- determining the accident sequence minimal cut sets;
— truncation criteria for sequence level minimal cut sets;
— review of results and refinement of models and data.

A brief description of these tasks should be provided. Methods and assumptions, such as truncation values, should be described. Conclusions reached in this step of the analysis should be discussed and the modifications made to the model and data following initial quantification should also be documented.

Next, a description of the final quantification of the accident sequence cut sets should be given. The following aspects of the analysis should be discussed:

— determining the minimal cut sets and their truncation criteria;
— determining estimates for each accident sequence;
— reassessment of the human errors;
— treatment of recovery;
— selection of the dominant accident sequence in each category.

Brief descriptions of these tasks should be provided. Truncation values used in various stages of the analysis, the recovery model, and criteria for selecting dominant accident sequences together with their supporting rationale should be described. A description of each of the dominant accident sequences should be provided. Modifications made to the data following initial screening should also be documented, including the tables documenting recovery action.

Section 6.4 describes the uncertainty analysis. The following issues should be discussed in this section:

— The scope of the analysis, including:
  • selection of uncertainties propagated through the model;
  • selection of results that are evaluated for their uncertainties (e.g. total core damage frequency, group of sequences or individual sequence contributors, etc.) with assumptions and criteria used in obtaining the uncertainty results.

— The method of propagating the uncertainties, including:
  • the probability distributions for the primary events with reference to appropriate sources of information;
  • the methods of accounting for dependences and correlations between events, such as the existence of the same primary event in more than one cut set, different basic events whose failure probabilities were generated from the same failure rate data, etc.

— General insights from and observations on the results (detailed presentation of the results of the analysis should be provided in Section 7 of the main report).

Section 6.5 describes the processes of importance analysis and sensitivity analysis and the results obtained. A brief discussion of the scope and techniques should be included in this section, whereas the results of the analysis should be presented in Section 7 of the main report. The following elements of the analysis should be discussed in this section:
— identification of the importance measures chosen and their discussion;
— selection of issues with respect to which importance calculations are performed
  and an explanation supporting the choice;
— identification of the range of possible variations for selected sensitivity issues;
— assumptions made in the analyses;
— techniques used in the analyses;
— general insights and observations on the results.

Section 6.6 should describe the selection of computer codes and their use in
the quantification process. The following aspects of the analysis should be discussed:

— Selection of computer codes, their capabilities and the scope of application at
  various steps of the solution process.
— Technical aspects related to the solution process, including:
  • logic model preparation;
  • input preparation;
  • interfaces and linking facilities between different codes or computers (if
    appropriate);
  • transfer and storage of the intermediate results.
— Detailed information needed to trace back the outputs, which are not included
  in the documentation in printed form but are stored in the form of machine
  readable magnetic tapes or diskettes, including, for example:
  • computer representation of fault trees (both system and sequence level) with
    input data
  • truncated cut set expressions for system fault trees
  • detailed and truncated expressions for accident sequences.

VIII. 2.3.7. Display and interpretation of results

Section 7 of the main report concentrates on the detailed presentation of the
results of the PSA. The results obtained in each major step of the study, discussed
in preceding sections of the main report, are integrated and displayed in this section,
together with the important engineering insights gained in the analysis. Assessments
of the uncertainty, importance and sensitivity analysis of the results are also
presented. Finally, more general conclusions and recommendations are outlined. In
effect, Section 7 duplicates most of the information presented in the summary report.
The following organizational structure of this section is recommended:

7.1. Dominant sequences contributing to core damage frequency
7.2. Results of uncertainty analysis
7.3. Results of importance and sensitivity analysis
7.4. Interpretation of results, engineering insights
7.5. Credibility and qualification of the results
7.6. Conclusions, recommendations and potential applications.
Section 7.1 should provide the reader with detailed information on the dominant accident sequences. This information relies on the results of quantitative accident sequence analysis to be provided in Section 6.3 of the main report and should allow the identification of the fault contributors to the sequence and the calculated sequence frequency.

Documentation should include the following elements:

— a list of dominant accident sequences in order of their contribution to the core damage frequency;
— a narrative description of each of the dominant accident sequences, including:
  • the nature of the initiating events
  • the system failures involved in the sequence
  • the major contributing failures associated with each system failure
  • the significant dependences between the events
  • important operator actions
  • timing and sequencing considerations;
— a referencing of each sequence to the event tree, relevant fault trees and failure rates associated with the contributing events;
— estimation of the total frequency of core damage and relative contributions of each of the dominant sequences;
— dominant minimal cut sets of each of the dominant sequences and their probabilities (with and without recovery).

Section 7.2 should document the results obtained in the uncertainty analysis task discussed in Section 6.4 of the main report. In addition to these quantitative results, qualitative assessment of various uncertainties should also be provided. The following information should be included in this section:

— specification of uncertainties that are treated quantitatively and qualitatively;
— the results of the quantitative analysis, including:
  • tabulated uncertainty estimates for each dominant sequence (providing, for example, point estimates, mean, median and upper and lower bounds);
  • tabulated uncertainty estimates for core damage frequency (as before);
  • identification of the principal sources of uncertainty associated with each dominant accident sequence and with core damage estimates;
— the results of the qualitative assessment of uncertainty, including:
  • sources of uncertainty;
  • methods of treatment in the study;
  • effect on the results of the analysis;
  • qualitative evaluation of uncertainty.

Section 7.3 documents the results of importance and sensitivity analysis discussed in Section 6.5 of the main report. The following results should be presented:
— importance of the event with respect to core damage frequency;
— importance of the event class with respect to core damage frequency, including, for example:
  • human errors
  • test and maintenance unavailabilities
  • initiating events
  • classes of hardware faults, and so on;
— importance of the system with respect to core damage frequency;
— effects of various sensitivity issues on the dominant accident sequences and core damage frequency.

Section 7.4 summarizes the engineering insights gained in the analysis. The most important factors contributing significantly to the core melt frequency are discussed. The information provided in this section should include:

— procedural changes in design or operations as a result of the PSA;
— important plant features, events or classes of events;
— important assumptions in the analysis;
— comparison of results reported with those of previous PSAs (the reasons for any differences should be explained).

Section 7.5 brings together those aspects of input, methods and results that are key factors in the ultimate credibility and qualification of the results. The following issues should be addressed in this section:

— limitations and constraints associated with input data, assumptions and methodologies, and their influences on the results of the PSA;
— completeness of the analysis in respect of:
  • initiating events
  • system failure modes or causes
  • intersystem dependences
  • human interactions;
— evaluation of general uncertainties and their effects on the use of results;
— activities undertaken to ensure technical quality.

Section 7.6 presents some general conclusions and observations on the performance of the study and the usefulness of the results. The following points should be dealt with in this section:

— achievement of the objectives of the study;
— conclusions from results of the PSA;
— conclusions from the process of the PSA;
— recommendations related to:
  • plant safety assessment
  • plant design modification
• procedures
• training
• licensing safety issues.

VIII.3. APPENDICES TO THE MAIN REPORT

VIII.3.1. General guidelines

The appendices are for material whose bulk and level of detail are such that its inclusion in the main report is unwarranted. As has been pointed out earlier in this section, all information necessary to document the analysis should be included in the main report. The appendices would contain major parts of the descriptions of the plant and systems, important assumptions, detailed models, the system fault tree models, the complete database and a substantial part of the results (both final and intermediate). Not all the information in the appendices should necessarily be in printed form. Some of it could be more appropriately stored in magnetic records (computer tapes or diskettes, word processor files).

Five appendices are proposed with contents as described in subsections VIII.3.2 to VIII.3.6.

VIII.3.2. Systems analysis

Appendix A contains detailed information that supplements the material presented in Sections 3, 4 and 6 of the main report. It presents the results of the systems analyses performed to support the development and quantification of accident sequences. The material provided in this presentation includes detailed descriptions of plant systems, fault tree models and data needed for their quantification. All front line and support systems listed in Section 3.3 of the main report should be addressed.

Appendix A should consist of separate modules (sections), each dedicated to individual systems included in the analysis, with an introductory section including more general information common to all system model descriptions.

The introductory section (Section A1) should contain general information related to:

— contents and organizational structure of the system specific sections;
— general modelling assumptions;
— nomenclature and format used in systems and system model descriptions.

It is recommended that the organizational structure of every module dedicated to a specific system be the same, regardless of specific features of the system. Detailed guidelines concerning contents and organization of these modules are provided in the remainder of this section.
Certain modelling assumptions that are common to all systems or to specific groups of systems are specified in this section so as not to repeat them in each system description. An example of such an assumption may be excluding certain types of failures from the model (such as the diversion of flow through secondary lines of substantially smaller diameter or check valves failing in the reverse direction).

Detailed presentations of the nomenclature and format used in the system/system models description should be included in this section. Such a presentation may facilitate intermediate and final review of the results. A logical and consistent convention on nomenclature and format, if observed from the beginning, may help to prevent inconsistencies among different analysts. The following information concerning nomenclature and format should be provided:

- definition of components included in the system models;
- definition of failure modes considered in the analysis;
- format used in system drawings, including:
  - graphical component designators;
  - component descriptors and component coding;
- format used in fault tree representations, including:
  - a fault tree graphics convention (logic gates, transfers, types of events and so on)
  - an event naming scheme for graphical and computer representation.

For sections dedicated to specific systems (for example, A2) the following organizational structure is recommended:

A2.1. Description of system
A2.2. Event tree interface
A2.3. Description of the fault tree logic model
A2.4. Basic event quantification.

For a system description (Section A2.1), the following organization is recommended:

A2.1.1. Sources of information. The sources of system design data that were used in the analysis should be specified together with the discussion related to the actuality and sufficiency of the information.

A2.1.2. System function. A brief description of the purpose of the system is given. The principal function that the system helps to perform and the accident initiators to which it is expected to respond are specified.

A2.1.3. Design basis. A simple description of the piping/wiring configuration should be given, accompanied by a schematic diagram depicting the major components of the system. Piping/wiring segments should be noted on the diagram. This discussion should clarify system boundaries used in the
modelling. If certain flow paths have been ignored, these should be noted and reasons given. Technical data such as physical dimensions, locations, capacities will be included if important to the system's operation.

The minimal information needed about support systems should be provided and the requirement for these systems specified. Other auxiliaries such as instrumentation and control systems and their relation to system operation should also be discussed.

A2.1.4. Interfaces. Detailed lists of the interfaces with other systems or support systems, including all those necessary for operation, should be provided. The specific interfaces and impacts of supporting system failures should be described.

A2.1.5. Operation. Operation of the system in various operating modes of interest should be provided. The discussion should specify which equipment changes state to initiate the system, what signals cause the system to actuate, and any required operator actions. If the operator is to perform any backup actions, these should be discussed, together with the indications that the operator would have in the control room or locally to perform the action. Recovery actions available to the operator are discussed for major component or system failure modes. The portions of the emergency operating procedures relevant to this system are summarized.

A2.1.6. Testing and maintenance. General schedule for system test, the type of test procedure and the changes in system configuration during these tests is described. The maintenance schedule and procedures with respect to availability of system components are discussed. The system configuration during maintenance should be described.

A2.1.7. Technical specifications. A summary of the technical specification requirements and of other limiting conditions for operation is provided.

The system description discussed here will vary slightly depending on the system type. It is convenient to distinguish between process systems, electrical power supply systems and protective/control systems. Some additional topics that reflect specific features of a system in each of the aforementioned groups should be mentioned.

For most process systems, essential information should be provided concerning the instrumentation for monitoring the performance of the system. The control logic associated with any of the components of the system should also be provided. Detailed information should be provided concerning:

— system initiator: the parameters and setpoints used for automatic system actuation, the names of initiating signals with statements of the effects of these signals (such as open the valve, close the valve, check position of the valve), the names of start systems that are activated;
— component trips: the parameters and setpoints used to initiate component operation automatically, information that the operator receives (warning system), reasons for component trips;
— system isolation: the parameters and setpoints used to isolate the system.

For electrical power supply systems, a description should cover: the generator and house load system, the emergency power system, the allocation of consumers to busbars, feeders to power consuming equipment, short circuit protection, DC power supply, emergency diesels and switching on of emergency power diesels and consumers. A description should also consider protection against external events affecting the electrical power supplies.

For protection and safety actuation systems, a description of the system should include a list of the parameters that are monitored, the mitigatory actions initiated by the system and the components that are activated. Information should also be provided about the fail safe principle for major components and the failure warning system. The behaviour of the reactor protection system in external events should be discussed. The composition and organization of the instrumentation, including sensors and transmitters, signal processing channels, logic modules and load relay drivers, should be described. Separation and diversity of transmitters should be discussed. Manual override or actuation possibilities should also be discussed.

Section A2.2 discusses the performance requirements of the systems. These include:

— presentation of minimum requirements (success criteria) for mitigation systems;
— a description of interrelations and dependences among systems.

The information in the documentation of the minimum success criteria associated with each initiating event should include the following:

— Physical parameters, which express the minimum success criteria for front line systems — and if necessary for support systems — such as \( x \text{ L}\cdot\text{h}^{-1} \) in-feed against a pressure of \( y \text{ bar} \), with a feedwater temperature of \( Z \text{ K} \) within a time period of \( t \text{ h} \).
— Discussion of the origin of these physical parameters (e.g. conservative calculations from the licensing procedure or best estimate calculations) together with comments on how realistic they are believed to be.
— The minimum number of redundancies of the systems which would fulfil the physical system functions (e.g. one out of three emergency core cooling trains is sufficient to provide \( x \text{ L}\cdot\text{h}^{-1} \) at \( y \text{ bar} \) for \( Z \text{ K} \) within \( t \text{ h} \)) for front line systems.
— Special conditions imposed by different initiating events (such as extreme humidity or temperature) and special characteristics of the initiator.
Boundary conditions (such as different top events) imposed on the system model with different accident sequence logic should be discussed.

In Section A2.3, the principal output of the systems analysis, the system models (e.g. fault trees) and basic data, are presented in detail. The specific information used to develop the fault tree and the basic assumptions (specific to the system) are reviewed for each model developed. For example, the fault tree presentation should include:

- graphical representation and a description of the detailed fault tree model;
- additional qualitative and quantitative information related to logic elements used in the model (provided in tabular form), including:
  - description and data for all hardware failures (failure rate, mean time between demands or duration time, mean unavailability)
  - description and data for human errors (event type, failure probability)
  - description and data for maintenance events (mean frequency, mean duration, unavailability)
  - listing of all logic transfers to support systems
- definition of independent subtrees with module component specification and related data;
- graphical representation of modularized fault trees and their description;
- results of independent system evaluation (performed as an initial phase of the accident sequence quantification step).

Section A2.4 provides a list of the values used for quantification of the basic events in the corresponding fault tree. Cross-references to the information provided in Appendices A2 and A3 should also be made.

VIII.3.3. Data assessment and parameter estimation

Appendix B contains detailed information which complements the material presented in Section 5 of the main report. This documentation may include:

- detailed description of the methods for updating generic data with plant specific information;
- generic frequencies for initiating events;
- plant specific frequencies for initiating events, including:
  - method of estimation
  - tabulated events and source of information
- generic component failure rates in tabulated form, including:
  - component type identification
  - failure mode definition
  - distribution characteristics and mean (or joint estimate and interval estimates)
• source of information, providing reference to primary source, the way the
data were used and possible assumptions or data modifications with their
supporting rationale
  — plant specific failure data, including:
    • component identification
    • reported failure
    • date of failure
    • cause of failure
    • success data summary (operating hours or number of demands) with an
      explanation of how these data were developed
    • distribution characteristics and mean
  — generic component maintenance data in tabulated form, including:
    • component type identification
    • distribution and mean (or joint estimate and interval estimates)
    • source of information
  — plant specific maintenance data, including:
    • component identification
    • date of maintenance event
    • duration of maintenance
    • cause of maintenance
    • total shutdown time
    • total number of maintenance events.

VIII.3.4. Human performance analysis

Appendix C of the PSA documentation provides information on the human performance analysis and it supplements the material presented in Sections 4 and 5 (Sections 4.3 and 5.3) of the main report. The information provided in Appendix C is related to the inputs, methods and results of the analysis. It should include the following:

— a summary of the test and maintenance procedures with identification of potential restoration errors following test and maintenance;
— a summary of the emergency procedures relating the particular procedures to specific accident sequences and identifying human responses to accidents;
— a summary of administrative procedures outlining the administrative control systems at the plant;
— a list of potential significant human errors, including restoration errors following testing and maintenance (see also Appendix A) and human errors in accident response;
— identification of the model, quantification method and upper bound failure probability for each error included in the list;
— specification of errors assessed to be important for the analysis;
— a description of the task analysis performed on these human actions;
— a detailed description of models and methods used in the task analysis and the best estimate probabilities for relevant human errors;
— a list of recovery actions associated with recoverable events (component failures, etc.) not related to human error;
— a detailed description of models and methods used in the analysis of recovery probabilities, with relevant input information (critical time, location of recovery action, and so on).

The task analysis should be described in detail. Each human error event chosen for closer scrutiny should be discussed. For each, the action to be performed in the context of the applicable accident sequence should be described. This discussion should not only describe the event but also detail the information available to the operator, the appropriate performance shaping factors, the level of dependence and other information pertinent to the model. The following detailed information should be included:

— the definition of the event in the fault tree with fault tree identification;
— the goal of the human action;
— the time (relative to the initiating event or similar) at which the action is necessary or possible;
— the time that is needed to perform the action;
— identification of written procedures that describe the action;
— identification of possibilities for the operator to detect the necessity of the action (indications, announcements, reactor protection system signals or other);
— identification of potential links to other functional elements within the fault tree;
— the type of personnel intended to perform the action;
— the means and instruments to be used in performing the action;
— the identification of potential kinds of errors;
— the identification of potential ways to recover following these errors.

VIII.3.5. Qualitative dependence analysis

Appendix D contains detailed information related to the task of qualitative dependence analysis that is not contained in the main report. For example, information on location, elevation, fire barriers and so on that was used in the qualitative analysis of physical dependences should be presented here.
VIII.3.6. Quantification of accident sequences

Appendix E contains detailed information related to the accident sequence quantification task, which supplements the material presented in Section 6 of the main report and Section II of the summary report.

The detailed information that should be provided in Appendix E includes:

— computer input decks used in the accident sequence quantification;
— a complete list of accident sequences contributing to core damage and estimates of their frequencies;
— the dominant terms of the minimal cut set equation for each of the accident sequences together with probability estimates;
— the cut set expression for core damage used in the uncertainty analysis.

VIII.4. INTERNAL DOCUMENTATION

Internal documentation refers to all documentation of the PSA study that is not published. The organization and the content of the information that should be documented internally should comply with the requirements of technical quality assurance (see Appendix III of this report.)

Plant information used as input to the plant familiarization task and the fault tree development task constitutes part of the internal documentation. Material of this type summarizes and collates in one location significant information included in various items of plant documentation (such as design documentation and as built drawings, system descriptions, operating manuals, test and maintenance procedures, emergency procedures and technical specifications) and other documents that are not easily accessible to a reader or future user of the PSA models.

Additionally, substantial information is also gathered in the course of the assessment of plant specific reliability data, using various plant operational records (such as operator logs, monthly status reports, maintenance logs, test and calibration records and repair records).
REFERENCES


This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Alternating current</td>
</tr>
<tr>
<td>ATWS</td>
<td>Anticipated transient without SCRAM</td>
</tr>
<tr>
<td>BD</td>
<td>Block diagram</td>
</tr>
<tr>
<td>BWR</td>
<td>Boiling water reactor</td>
</tr>
<tr>
<td>CC</td>
<td>Core cooling</td>
</tr>
<tr>
<td>CCD</td>
<td>Cause consequence diagram</td>
</tr>
<tr>
<td>CCF</td>
<td>Common cause failure</td>
</tr>
<tr>
<td>CDF</td>
<td>Core damage frequency</td>
</tr>
<tr>
<td>CG</td>
<td>Co-ordination Group</td>
</tr>
<tr>
<td>DC</td>
<td>Direct current</td>
</tr>
<tr>
<td>DSMCS</td>
<td>Dependence suspect minimal cut set</td>
</tr>
<tr>
<td>ECCS</td>
<td>Emergency core cooling system</td>
</tr>
<tr>
<td>ESD</td>
<td>Event sequence diagram</td>
</tr>
<tr>
<td>ESF</td>
<td>Engineered safety features</td>
</tr>
<tr>
<td>ET</td>
<td>Event trees</td>
</tr>
<tr>
<td>FL-SS</td>
<td>Front line/support systems</td>
</tr>
<tr>
<td>FM</td>
<td>Fuel machine</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure modes and effects analysis</td>
</tr>
<tr>
<td>FSAR</td>
<td>Final safety analysis report</td>
</tr>
<tr>
<td>FT</td>
<td>Fault tree</td>
</tr>
<tr>
<td>GO</td>
<td>Go chart</td>
</tr>
<tr>
<td>HCR</td>
<td>Human cognitive reliability</td>
</tr>
<tr>
<td>HRA</td>
<td>Human reliability analysis</td>
</tr>
<tr>
<td>HT</td>
<td>Heat transport</td>
</tr>
<tr>
<td>IE</td>
<td>Initiating events</td>
</tr>
<tr>
<td>IORV</td>
<td>Inadvertently opened relief valve</td>
</tr>
<tr>
<td>IEPERS</td>
<td>International Peer Review Services</td>
</tr>
<tr>
<td>IREP</td>
<td>Interim reliability evaluation programme</td>
</tr>
<tr>
<td>LHS</td>
<td>Latin hypercube sampling</td>
</tr>
<tr>
<td>LOCA</td>
<td>Loss of coolant accident</td>
</tr>
<tr>
<td>LOOP</td>
<td>Loss of off-site power</td>
</tr>
<tr>
<td>LPSW</td>
<td>Low pressure service water</td>
</tr>
<tr>
<td>LWR</td>
<td>Light water reactor</td>
</tr>
<tr>
<td>MSIV</td>
<td>Main steam isolation valve</td>
</tr>
<tr>
<td>NPP</td>
<td>Nuclear power plant</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability density function</td>
</tr>
<tr>
<td>PHT</td>
<td>Primary heat transport</td>
</tr>
<tr>
<td>PORV</td>
<td>Pressure operated relief valve</td>
</tr>
<tr>
<td>PRA</td>
<td>Probabilistic risk assessment/analysis</td>
</tr>
<tr>
<td>PSA</td>
<td>Probabilistic safety assessment/analysis</td>
</tr>
<tr>
<td>PSAPACK</td>
<td>PSA code package for use with personal computers</td>
</tr>
<tr>
<td>PWR</td>
<td>Pressurized water reactor</td>
</tr>
</tbody>
</table>
QA: Quality assurance
RCS: Reactor coolant system
SC: Supervisory Committee
SG: Steam generator
SHARP: Systematic human action reliability procedure
SRS: Simple random sampling
SS-SS: Support systems/support systems
CONTRIBUTORS TO DRAFTING AND REVIEW

Note: Affiliations were correct at the times of the meetings.

Barrett, R. Nuclear Regulatory Commission, United States of America

Campbell, J.F. Nuclear Installations Inspectorate, United Kingdom

Carnino, A. Electricité de France, France

Chakraborty, S. Swiss Federal Nuclear Safety Inspectorate, Federal Energy Office, Switzerland

Cullingford, M. International Atomic Energy Agency

Debenham, A. (Observer) Atomic Energy Authority, United Kingdom

Fabian, H. Kraftwerk Union AG, Federal Republic of Germany

Feretic, D. Zagreb Electrotechnical Faculty, Yugoslavia

Gubler, R. International Atomic Energy Agency

Gumley, P. (Observer) Atomic Energy of Canada Ltd, Canada

Hirschberg, S. ASEA-ATOM, Sweden; Paul Scherrer Institute, Switzerland

Holloway, N.J. Atomic Energy Authority, United Kingdom

Horne, B.E. (Observer) Central Electricity Generating Board, United Kingdom

Kani, Y. Power Reactor and Nuclear Fuel Development Corporation, Japan

King, F. Ontario Hydro, Canada

Kröger, W. Institute for Nuclear Safety Research, Jülich Nuclear Research Centre, Federal Republic of Germany

Kulig, M. Atomic Energy Commission, Poland

This publication is no longer valid
Please see http://www-ns.iaea.org/standards/
Lanore, J.M. 
Institut de Protection et de Sûreté Nucléaire, 
Centre d'études nucléaires de Fontenay-aux-Roses, 
France

Lederman, L. 
deputy secretary
International Atomic Energy Agency

Markoczy, G. (Observer) 
Bernische Kraftwerke AG, Switzerland

McKeown, J. (Observer) 
South of Scotland Electricity Board, United Kingdom

Moroni, J.M. 
Electricité de France, France

Niehaus, F. 
International Atomic Energy Agency

Papazoglou, I.A. 
National Centre for Scientific Research Demokritos, 
Greece

Paula, H. 
Fiscal Management, United States of America

Poucet, A. 
Ispra Joint Research Centre of the 
Commission of the European Communities

Rasmussen, D. 
Nuclear Regulatory Commission, 
United States of America

Smith, J. 
Atomic Energy of Canada Ltd, Canada

Tingle, A. 
Brookhaven National Laboratory, 
United States of America

Tomic, B. 
International Atomic Energy Agency

Vesely, W.E. 
Science Applications International Corporation, 
United States of America

Villadoniga, J.I. 
Council for Nuclear Safety, Spain

Virolainen, R. 
Finnish Centre for Radiation and Nuclear Safety, 
Finland

Vöröss, L. 
Institute for Electric Power Research (VEIKI), 
Hungary

174
Advisory Group Meeting
Vienna, Austria: 1–5 December 1986

Advisory Group Meeting
Vienna, Austria: 1–23 October 1987

Consultants Meetings
Vienna, Austria
16–27 February 1987; 9–13 March 1987;
8–12 June 1987; 18–19 June 1987; 29 June – 3 July 1987;
18–22 January 1988; March – June 1988 (four weeks);
8–12 May 1989; 3–7 October 1989

Organizations
Gesellschaft für Reaktorsicherheit, Federal Republic of Germany
(First draft of Section 7, August 1987)
(Second draft of Section 7, April 1988)
HOW TO ORDER IAEA PUBLICATIONS

An exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, has been appointed for the following countries:

CANADA
UNITED STATES OF AMERICA

UNIPUB, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA

In the following countries IAEA publications may be purchased from the sales agents or booksellers listed or through major local booksellers. Payment can be made in local currency or with UNESCO coupons.

ARGENTINA
Comisión Nacional de Energía Atómica, Avenida del Libertador 8250, RA-1429 Buenos Aires

AUSTRALIA
Hunter Publications, 58 A Gipps Street, Collingwood, Victoria 3066

BELGIUM
Service Courrier UNESCO, 202, Avenue du Roi, B-1060 Brussels

CHILE
Comisión Chilena de Energía Nuclear, Venta de Publicaciones, Amunategui 91, Casilla 188-D, Santiago

CHINA
IAEA Publications in Chinese:
China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing
IAEA Publications other than in Chinese:
China National Publications Import & Export Corporation, Deutsche Abteilung, P.O. Box 88, Beijing

CZECHOSLOVAKIA
S.N.T.L., Mikulandska 4, CS-116 86 Prague 1

FRANCE
Office International de Documentation et Librairie, 48, rue Gay-Lussac, F-75240 Paris Cedex 05

HUNGARY
Kultura, Hungarian Foreign Trading Company, P.O. Box 149, H-1369 Budapest 62

INDIA
Oxford Book and Stationery Co., 17, Park Street, Calcutta-700 016
Oxford Book and Stationery Co., Scindia House, New Delhi-110 001

ISRAEL
YOZMOT (1989) Ltd, P.O. Box 56055, Tel Aviv 61560

ITALY
Libreria Scientifica, Dott. Lucio de Biasio “aeiou”, Via Meravigli 16, I-20123 Milan

JAPAN
Maruzen Company, Ltd, P.O. Box 5050, 100-31 Tokyo International

PAKISTAN
Mirza Book Agency, 65, Shahrah Quaid-e-Azam, P.O. Box 729, Lahore 3

POLAND
Ars Polona-Ruch, Centrala Handlu Zagranicznego, Krakowskie Przedmiescie 7, PL-00-058 Warsaw

ROMANIA
Ilexim, P.O. Box 136-137, Bucharest

RUSSIAN FEDERATION
Mezhdunarodnaya Kniga, Smolenskaya-Sennaya 32-34, Moscow G-200

SOUTH AFRICA
Van Schalk Bookstore (Pty) Ltd, P.O. Box 724, Pretoria 0001

SPAIN
Diaz de Santos, Lagasca 95, E-28006 Madrid
Diaz de Santos, Balmas 417, E-08022 Barcelona

SWEDEN
AB Fritzex Kungl. Hovbokhandel, Fredsgatan 2, P.O. Box 16356, S-103 27 Stockholm

UNITED KINGDOM
HMSO, Publications Centre, Agency Section, 51 Nine Elms Lane, London SW8 5DR

YUGOSLAVIA
Jugoslovenska Knjiga, Terazije 27, P.O. Box 36, YU-11001 Belgrade

Orders from countries where sales agents have not yet been appointed and requests for information should be addressed directly to:

Division of Publications
International Atomic Energy Agency
Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria
This publication is no longer valid
Please see http://www-ns.iaea.org/standards/