IAEA-TECDOC-1267

Procedures for conducting probabilistic safety assessment for non-reactor nuclear facilities

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

January 2002

The originating Section of this publication in the IAEA was:

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

PROCEDURES FOR CONDUCTING
PROBABILISTIC SAFETY ASSESSMENT FOR NON-REACTOR NUCLEAR FACILITIES
IAEA, VIENNA, 2002
IAEA-TECDOC-1267
ISSN 1011–4289

Printed by the IAEA in Austria
January 2002

FOREWORD

A well performed and adequately documented safety assessment of a nuclear facility will serve as a basis to determine whether the facility complies with the safety objectives, principles and criteria as stipulated by the national regulatory body of the country where the facility is in operation. International experience shows that the practices and methodologies used to perform safety assessments and periodic safety re-assessment for non-reactor nuclear facilities differ significantly from county to country. Most developing countries do not have methods and guidance for safety assessment that are prescribed by the regulatory body. Typically the safety evaluation for the facility is based on a case by case assessment. Whilst conservative deterministic analyses are predominantly used as a licensing basis in many countries, recently probabilistic safety assessment (PSA) techniques have been applied as a useful complementary tool to support safety decision making. The main benefit of PSA is to provide insights into the safety aspects of facility design and operation. PSA points up the potential environmental impacts of postulated accidents, including the dominant risk contributors, and enables safety analysts to compare options for reducing risk. In order to advise on how to apply PSA methodology for the safety assessment of non-reactor nuclear facilities, the IAEA organized several consultants meetings, which led to the preparation of this TECDOC.

This TECDOC is intended as guidance for the conduct of PSA in non-nuclear facilities. The main emphasis here is on the general procedural steps of a PSA that is specific for a non-reactor nuclear facility, rather than the details of the specific methods. The report is directed at technical staff managing or performing such probabilistic assessments and to promote a standardized framework, terminology and form of documentation for these PSAs. It is understood that the level of detail implied in the tasks presented in this publication is not necessary for all types of facility or PSA applications. In fact, it is anticipated that for many facilities, a ‘streamlined’ or ‘simplified’ interpretation of the information presented in this TECDOC will be acceptable. The appropriate level and form of streamlining is dependent upon the specific objectives of the analysis and the magnitude of the hazard that the facility represents. Facility hazard can drive the depth of analysis, as it may well be appropriate to analyse a lower hazard facility to less depth than higher hazard facilities (i.e., the depth of analysis is commensurate with the risk). Thus, the concept of hazard-graded depth of probabilistic safety analysis is considered as appropriate for non-reactor nuclear facilities.

This report was reviewed during a Technical Committee Meeting on Current Practices in PSA for Non-reactor Nuclear Facilities held in Vienna, in November 2000. The IAEA appreciates the work performed by all the participating experts and wishes to thank them for their valuable contribution to the preparation of this report. The IAEA officer responsible for this publication was V. Ranguelova of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

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

CONTENTS

1. INTRODUCTION

1.1. Background

The PSA approach provides a formal structured procedure for defining the functional logic of complex systems, assessing the consequences of failure and deriving numerical estimates of risk[1] from the operation of a plant.

In addition, PSA allows, through the calculation of risk measures, an explicit demonstration of safety that is comparable across different types of systems and different industries. Calculated risks can also be compared against explicitly defined risk criteria. Such criteria are generally derived from publicly defined norms of what constitutes acceptable levels of safety and promulgated through regulatory controls covering the industry. The risk measures themselves are also more easily understood by the public than complex engineering justifications of safety.

PSA can also support enhancement of plant safety. For example, it can provide plant designers with an unbiased benchmark against which to rank the safety significance of alternative design options, and enable them more easily to decide on the best option. Also, PSA is being increasingly used to develop more rational (from a safety standpoint) maintenance regimes.

These additional benefits of PSA can be applied to simpler and less hazardous nuclear facilities or systems and are judged to be particularly beneficial to non-reactor nuclear facilities (NRNFs). The underlying theme of this report is that these benefits can be obtained while employing a simplified or graded version of the full PSA method that is matched to the complexity and level of hazard[2] presented by each facility. The types of NRNFs where PSA can be of benefit include, for example:

- enrichment facilities of the diffusion or centrifugal type;
- fuel fabrication facilities for a range of different types of fuel;
- fuel reprocessing facilities;
- waste treatment and waste conditioning facilities;
- short and intermediate term storage facilities for irradiated fuel and other materials, e.g., fuel storage ponds;
- short and intermediate term storage facilities for storage of other solid radioactive wastes and liquid wastes, e.g., storage tank facilities;
- irradiation facilities;
- hot cell facilities;
- radiation emitting devices, e.g., accelerators.

The first comprehensive application of methods and techniques of PSA to a nuclear power plant (NPP) dates back to 1975 for the United States Nuclear Regulatory Commission's Reactor Safety Study (WASH-1400) [1]. Since that study, there has been substantial methodological

[1] A multiattribute quantity expressing hazard, danger or change of harmful or injurious consequences associated with actual or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences.

[2] For NRNF PSAs, 'hazard' is defined as an inherent physical or chemical characteristic that has the potential for causing harm to people, property or the environment.

development, and PSA techniques have become a standard tool in the safety evaluation of NPPs. The application of PSA to NRNFs started in the 1980s but this application was challenged to some degree by major differences between the design and operation of NPPs and NRNFs.

Fuel cycle facilities differ from reactors in several important aspects. First, they employ a greater diversity of technologies and processes. Second, fissile material and wastes are handled, processed, treated, and stored throughout the nuclear installations. These treatment processes use large quantities of hazardous chemicals which can be toxic, corrosive or combustible. Consequently, the materials of interest to nuclear safety are more distributed throughout the nuclear installations, in contrast to reactors, where the bulk of the nuclear material is located in the reactor core or fuel storage areas. For example, the nuclear materials in fuel cycle facilities are often present in solutions that are transferred between vessels used for different parts of the different processes, whereas in reactors the nuclear material is generally concentrated in the solid fuel.

Third, the facilities are often characterized by more frequent changes in operations, equipment and processes, which are necessitated by treatment or production campaigns, new product development, research and development, and continuous improvement. Fourth, for fuel cycle facilities there is generally a significantly greater reliance placed on the operator, not only to run the facility during its normal operation, but also to respond to fault[3] and accident conditions. Fifth, the range of hazards in some NRNFs can include inadvertent criticality events, and these events can occur in different locations, and in association with different operations. Finally, major steps in the NRNFs consist of chemical processing of fissile materials, and if not properly managed, this chemical processing may lead to inadvertent release of hazardous chemical or radioactive substances.

Further details on the differences between NPPs and NRNFs, together with a comparison with chemical process plants are given in Appendix I.

In principle, the methodology applied to a PSA study for an NPP is the same as that for an NRNF. However, the differences listed above have led to there being some features specific to an NRNF PSA. In general, the following features distinguish a PSA study for an NRNF from one performed for an NPP:

- For many NRNF PSAs, there is no differentiation between Level 1, 2 or 3 as used in the study of NPPs. Depending upon the objectives of the safety analysis, the PSA modelling process can encompass all aspects, from identification of initiating events[4], through the frequency estimation of the potential accident sequences[5], and calculation of the consequences in terms of the doses received by the workers and public which

[3] For NRNF PSAs, 'fault' is defined as any unplanned departure from the specified mode of operation of a system or component due to a malfunction or defect within the system or component, or due to external influences or personnel error.

[4] For NRNF PSAs, 'initiating event' or 'initator' is defined as an identified event that upsets the normal operations of the facility and may require a response by the facility operators and systems to avoid an undesirable outcome.

[5] For NRNF PSAs, 'accident sequence' and 'event sequence' and 'fault sequence' are defined as the combination of events, starting with an initiating event, that places a demand on a given set of safety measures. The accident/event/fault sequence represents a combination of success and failure of these safety measures and which then ends in a given set of consequences. They can also be defined as a scenario ending in a definable end state. The end state or set of consequences can, depending on the sequence, be either desirable/acceptable or undesirable.

could result from the sequences (though it may be appropriate for some studies to calculate the magnitude of off-site release, or to determine the magnitude and frequency of radioactive material being introduced to a specific environmental receptor, without calculating resultant dose).

- The initiating events tend to be much simpler; they are also more varied in their nature, leading to fewer opportunities for grouping and bounding of initiating events than for an NPP PSA study.
- There is reduced benefit in the consideration of generic lists of initiating events, due to the wide variety of NRNFs.
- The dominant hazard source at NPPs (the reactor core) is very centralized, whereas the dominant hazard source(s) at NRNFs can be widespread in location. In some cases, this leads to the need for assessing similar initiating events distinguished mainly by the event location.
- There are a considerably greater variety of accident sequences and end states, although they tend to be less complex than for NPP; in particular there is no need for models of the same degree of complexity as those used to address the phenomena of core damage and subsequent activity release. Accordingly, models representing details of the accident progression, such as fault trees, are in most cases much simpler than those used when modelling NPP accident progressions.
- With the greater reliance on operator actions at NRNFs to remain within the safe operating envelope, there can be a requirement to model a greater number of operator actions, both as initiating events, and in response to fault conditions.

This publication presents guidance on conducting a PSA study for an NRNF. The guidance is based in principle on that presented in Refs [2–4], which are specific to PSA studies for NPPs. Where these documents contain information applicable to a PSA for an NRNF, they have been appropriately referenced, and the details not reproduced here. Guidance for performing safety analysis on research reactors is available in IAEA Safety Series No. 35-G1 [5]. Several US Department of Energy publications [6–8] also include guidance on NRNF safety analysis techniques. Reference is also made to two American Institute of Chemical Engineers publications [9, 10], which discuss methodologies for hazard evaluation and quantitative risk analysis for chemical plants.

Some of the terms used in this publication are defined in footnotes throughout the present TECDOC. The definitions are those based on Refs [2–4], modified where appropriate to relate more specifically to NRNFs.

1.2. Objective and purpose of the report

This report provides guidance on conducting a PSA for NRNFs. The main emphasis is on the general procedural steps of the PSA specific for an NRNF rather than the details of the corresponding methods. The report is intended to assist technical experts managing or performing such 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.

It is very important to understand that the level of detail implied in the tasks presented in this report may not be necessary for all PSA applications for NRNFs. In fact, it is anticipated that for many NRNF applications, a “streamlined” interpretation of the guidelines presented here will

be appropriate. The appropriate level and form of streamlining is dependent upon the specific objectives of the analysis and the magnitude of hazard that the NRNF represents. Specific objectives may influence the range of analysis into excluding some of the procedural tasks outlined in this report. Facility hazard can influence the depth of analysis, since it may be appropriate to analyse lower hazard facilities to less depth than higher hazard facilities (i.e., the depth of analysis is commensurate to hazard). Similarly, facility complexity can influence the depth of analysis, since it may be appropriate to analyse simple facilities to less depth than more complex facilities.

Thus, the concept of hazard-graded depth of analysis is appropriate for NRNF PSAs. This report seeks to provide a comprehensive guidance for assessing the risk of a high hazard NRNF for regulatory purposes. Table I illustrates the concept of a graded approach and provides some guidance as to how to reasonably apply reduced depth of analysis for facilities of lower hazard.

The publication of this report 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.

The methodology presented in this TECDOC may be considered as support to the safety assessment guidance provided in the IAEA Safety Standards for nuclear fuel cycle facilities and waste predisposal management. Information on these standards can be found on the following Internet site: http://www.iaea.org/ns.

1.3. Scope of the report

The report provides guidance for conducting a PSA concerned with events that could lead to undesirable consequences. As discussed above, the guidance is specific to NRNFs of high hazard, but through the application of graded depth of analysis, the guidance is also applicable to NRNFs of lower hazard. The scope of this report is confined to:

- PSA techniques for NRNFs;
- identification of internal initiating events;
- scenario[6] development, evaluation of accident sequence frequency[7], and calculation of accident consequences;
- accidents that could give rise to radiological hazards.

No specific guidance is given for:

- the calculation of the health effects of an accident;
- the calculation of a monetary value for the detriment resulting from an accident.

[6] For NRNF PSAs, 'scenario' is defined as a combination of events starting with a fault (the initiating event) which places a demand on a given set of safety measures. The scenario represents a combination of success and failure of these safety measures and which then ends either in successful mitigation, or with undesirable consequences.

[7] For NRNF PSAs, the "sequence frequency" is determined by multiplying the frequency of the initiator (expressed as a frequency) with the conditional likelihood (unit-less measures) of success or failure of the safety measures relevant to the particular accident sequence.

TABLE I. FACILITY AND ANALYSIS RANKING

Hazard Rank	Low (low activity inventory)	Medium (medium activity inventory)	High (large activity inventory)
Examples of Facilities*	Radioisotope Lab	Fuel Fabrication Facility	Research Reactor
	Small Calibration Facility	Waste Treatment Facility	Large Reprocessing Plant
	Hot Cell Facility	Low-Level Waste Storage Facility	High-Level Waste Storage Facility

	Depth of Analysis		
	Simple	Intermediate	Detailed
PSA Tasks	(qualitative to semi-quantitative)	(semi-quantitative)	(quantitiative)
Familiarization (9)	Simple, minor effort	← →	Detailed diverse review
Hazard Identification (10), Initiating Events Selection (11)	Simple systematic or engineering evaluation	← →	Detailed systematic review (FMEA, HAZOP, etc.)
Undesirable End states (12)		← →	Detailed development
Safety Measures Identification (13)	Simple, minor effort	← →	Detailed identification
Safety Measures Information (14)		← →	Detailed information
Event Grouping (15)	Included in tasks 10 to 12 (simple grouping)	← →	Detailed development
Event Sequence Modelling (16)	Simple modelling or engineering evaluation	← →	Complex modelling (FTA, ETA, etc.)
Human Performance Analysis (17)	Simple (judgement)	← →	Detailed analysis (HRA, TA, etc.)
Consequence Analysis (18)	Simple analysis	← →	Detailed analysis
Parameter Estimating (19 to 24)	Few parameters, bounding case, qualitative frequencies	← →	Many parameters, best estimates
Sequence Quantification (25, 26)	Simple (dose, qualitative frequency)	← →	Complex (uncertainty analysis, sensitivity analysis, distributions)
Documentation (27)	Basic	← →	Detailed

***NOTE**: examples of facilities may rank differently depending upon the size of the facility (for example, a smaller reprocessing facility or plant involving a lower activity inventory may be ranked as a medium hazard).

While external events would often be included in the scope of an NRNF PSA, no specific guidelines are given for identifying or analysing external events.

Similarly, while non-radiological hazards may be included in the scope of some NRNF PSAs, no specific guidelines are given for identifying or analysing non-radiological hazards. Some examples, however, of how non-radiological hazards are treated in PSA studies for nuclear installations can be found in Ref. [11].

Risk and dose criteria used for evaluating risk tolerability are not provided in this report because such criteria are specific to Member States, and unique criteria may be applied for NRNF PSAs addressing unique objectives. For comparative purposes, however, examples of criteria used in various Member States are presented in Appendix IV.

1.4. Structure of the report

This report is divided into sections corresponding to the six major procedural steps for a detailed (quantitative) NRNF PSA. The six major procedural steps (illustrated in Fig. 1) are discussed in an introductory manner in the paragraphs below. The different sections of this report detail these procedural steps by breaking them down into (lower tier) tasks. Figure 2 illustrates the lower tier procedural tasks in the overall PSA procedure.

It should be emphasized that while all of the major procedural steps would often be followed in some form in an NRNF PSA, not all of the detailed tasks need to be carried out for all NRNF PSAs, and those tasks determined to be necessary do not necessarily need to be carried out to the level of detail implied in this document: as discussed in Section 1.2, the specific objectives of the PSA and the complexity and hazard level of the facility influence how the methodology is applied, in terms of procedural tasks taken, and the depth of the analysis applied.

It should also be noted that the steps and tasks should not necessarily be carried out in the specific sequence implied by the task numbering; some of the tasks described within each step can be performed in parallel with other tasks, both from within the same step, and from other steps. Generally, the third, fourth and fifth steps (Sections 5–7) are very closely linked, and activities could be defined which incorporate tasks from each of these steps. It will not be necessary to complete Steps 4 and 5 in their entirety before commencing Step 6.

1.4.1. Step 1: Management and organization (Section 2)

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 for the PSA, confirmation of the objective, scope and methodology by the PSA users[8]; 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.

[8] 'PSA users' are the individuals, organizational units, or agencies (e.g., the regulator) that will use the results of the PSA.

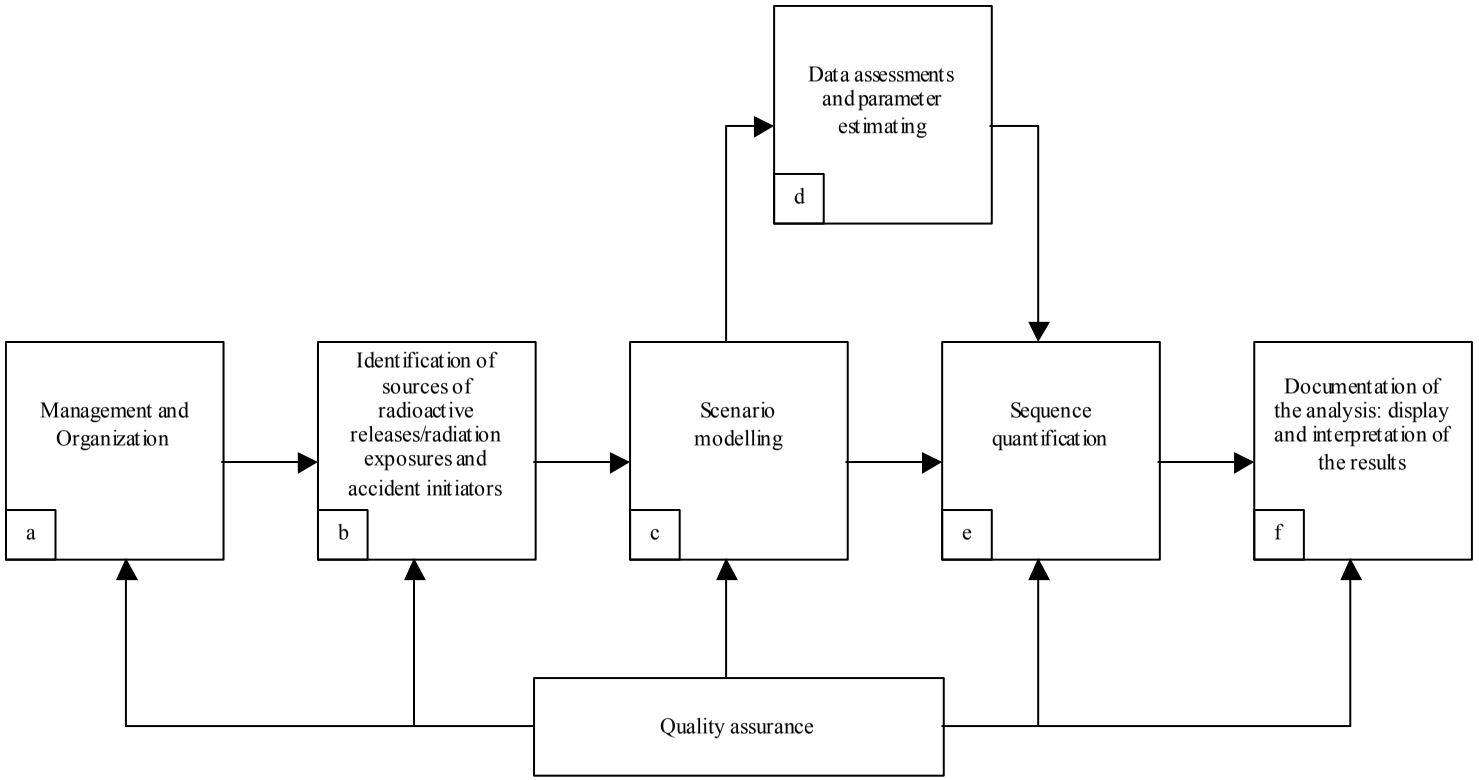

FIG. 1. Major procedural steps of a PSA.

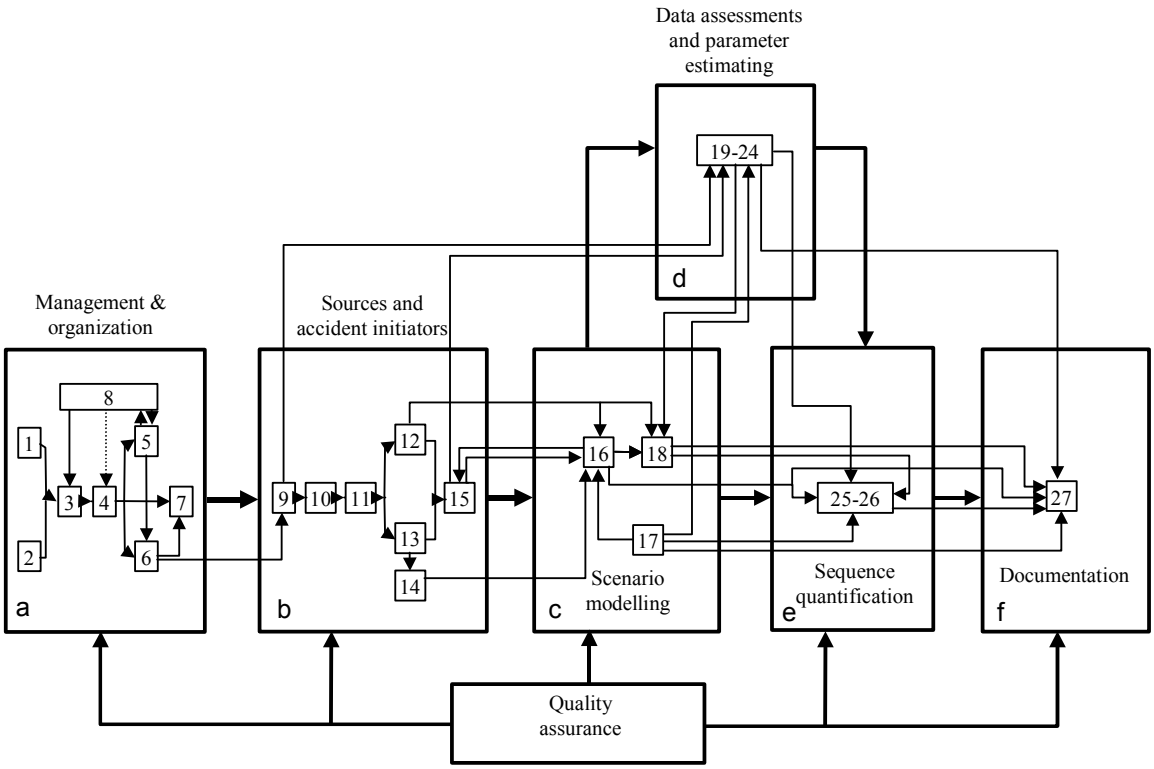

FIG. 2. The 27 procedural tasks of an NRNF PSA.

1.4.2. Step 2: Identification of sources of radioactive releases/radiation exposure, and accident initiators (Section 3)

During this step, the analysis team becomes familiar with the facility to be analysed, and collects much of the required information on which to base subsequent analysis. The potential sources of radioactive releases, or means of radiation exposure, are identified, and the initiating events that could result in such releases or exposures are determined. The same process can also be applied to non-radiological hazards, should they be included within the scope of the assessment. The safety measures[9] and features incorporated in the facility that could be challenged by the initiating events or during the event sequences are identified. The collection of this information enables the safety assessor to describe the potential accident sequences qualitatively, and to formulate a preliminary risk model.

1.4.3. Step 3: Scenario modelling (Section 4)

The third procedural step deals with the construction of mathematical models covering:

- the logic of accident sequences from Step 2 (i.e., the combination of initiating event and failure of relevant safety measures which could result in the undesirable consequences).
- the calculation of the consequences that would result from an accident sequence, generally in terms of doses to members of the public, and to members of the workforce, or in terms of impact on to the environment. For calculations associated with the

[9] For NRNF PSAs, 'safety measure' is the combined effect of protective measures, operator actions and mitigating systems which act alone or together in order to prevent or reduce the magnitude of undesired consequences.

determination of doses to workers or the public, it will generally be necessary to create (or to obtain) a set of models which achieve the following:

- evaluation of the effect of an accident in terms of quantity, type, and chemical form of radioactive material discharged to the environment, and/or released to the working area (specific models may be required for individual accident sequences; the complexity of the model required may vary widely);
- evaluation of the effect of any material released to the environment, generally in terms of dose to a member of the public (typically a small set of standard models, covering all possible release pathways, will be needed; once created they can be used for individual accident sequences. Because of the complexity, it is likely that an existing consequence analysis computer code will be used for such modelling);
- evaluation of the effect of any material released to a working area generally in terms of dose to a member of the workforce (it should be possible to create standard models which can be used repeatedly for individual accident sequences);
- evaluation of the effect of direct exposure to a radioactive source as a result of an accident, generally in terms of dose received, typically by a member of the workforce (there are generally accepted, well established methods available for this).

In some cases, largely dependent on the objectives of the PSA, and in particular the nature of any risk criteria being applied, the consequence calculations may be used to predict the detrimental health effects or monetary value of an accident (though specific guidance on these aspects is not presented in this report).

If the objectives of the PSA include the characterization of the risk associated with the potential introduction of radionuclides into a specific environmental target (for example, a local river or a source of drinking water), it will be necessary to create (or to obtain) a set of models to evaluate the transport of the radioactive material to the environmental target of interest. In general, the models of interest are likely to be a subset of the required models identified above.

1.4.4. Step 4: Data assessment and parameter estimation (Section 5)

This procedural step involves the acquisition and/or generation of all information necessary for quantification of the frequency and consequence models that were constructed in the third step. In particular, the fundamental elements of the facility 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.

For frequency estimation, the parameters that are estimated can be divided into three major categories: frequencies of initiating events, component and system unavailabilities, and human error probabilities. Parameters necessary for the modelling of potential dependencies among various events (initiating events, hardware failures or human errors) are also estimated.

A wide range of data will be required for the consequence assessment models. This will include phenomenological parameters relating to the amount, form and transport of the radioactive material and accident sequence specific data, as required to predict the degree of facility damage and subsequent release of radioactive material to operating areas and to the environment. More general data will also be required relating to the effect on a member of the workforce of exposure to radioactive material, as well as data relating to the off-site migration of radioactive material, and its uptake by members of the public or environmental receptors.

1.4.5. Step 5: Scenario quantification (Section 6)

In this step, the models constructed in the third step are quantified using the data developed in the fourth step. The result of this step is the assessment of the frequency of accident sequences, together with an estimate of the potential consequences, generally in terms of doses to worker and/or members of the public. In some cases, this is accompanied by an assessment of the associated uncertainties. Where appropriate, sensitivity studies are made for the important assumptions and the relative importance of the various contributors to the calculated results are indicated.

1.4.6. Step 6: Documentation of the analysis: display and interpretation of results (Section 7)

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 PSA users. This includes the interpretation of the results, in line with the objectives of the PSA.

2. MANAGEMENT AND ORGANIZATION (TASKS 1–8)

The information provided under Sections 2.3–2.8 in IAEA Safety Series No. 50-P-4 [2], covering the project management and organization for a PSA for NPPs is also applicable to an NRNF study, with some minor modifications. Additional guidance can be found in Sections 2.1–2.5 of IAEA Safety Series No. 50-P-8 [3] and Sections 3.1–3.4 of IAEA Safety Series No. 50-P-12 [4]. This initial procedural step consists of the following eight lower tier tasks (Fig. 3):

Task 1: Definition of the objectives of the PSA;
Task 2: Definition of the scope of the PSA;
Task 3: Project management;
Task 4: Selection of methods and establishment of procedures;
Task 5: Team selection and organization;
Task 6: Training of the team;
Task 7: Funding and scheduling, and
Task 8: Establishment of a QA programme and interactive peer review.

It is important that all of these tasks be given adequate consideration before the detailed, technical work on a PSA project starts. Task 1, which defines the objectives of the PSA together with its intended and potential uses, is of utmost importance, since this should influence every aspect of the PSA study.

Task 2 is also of primary importance since the scope determines the kind and amount of effort required in the PSA study.

In order to assure the overall responsiveness of the PSA study, the definition of objectives and scope of Tasks 1 and 2 should be preceded by a preliminary agreement between the organization performing the PSA and the end users of its results. This would assure the responsiveness of the PSA study to the requirements of the end users. The preliminary agreement phase should also include clarification of any PSA implementation aspects relevant to the NRNF being evaluated.

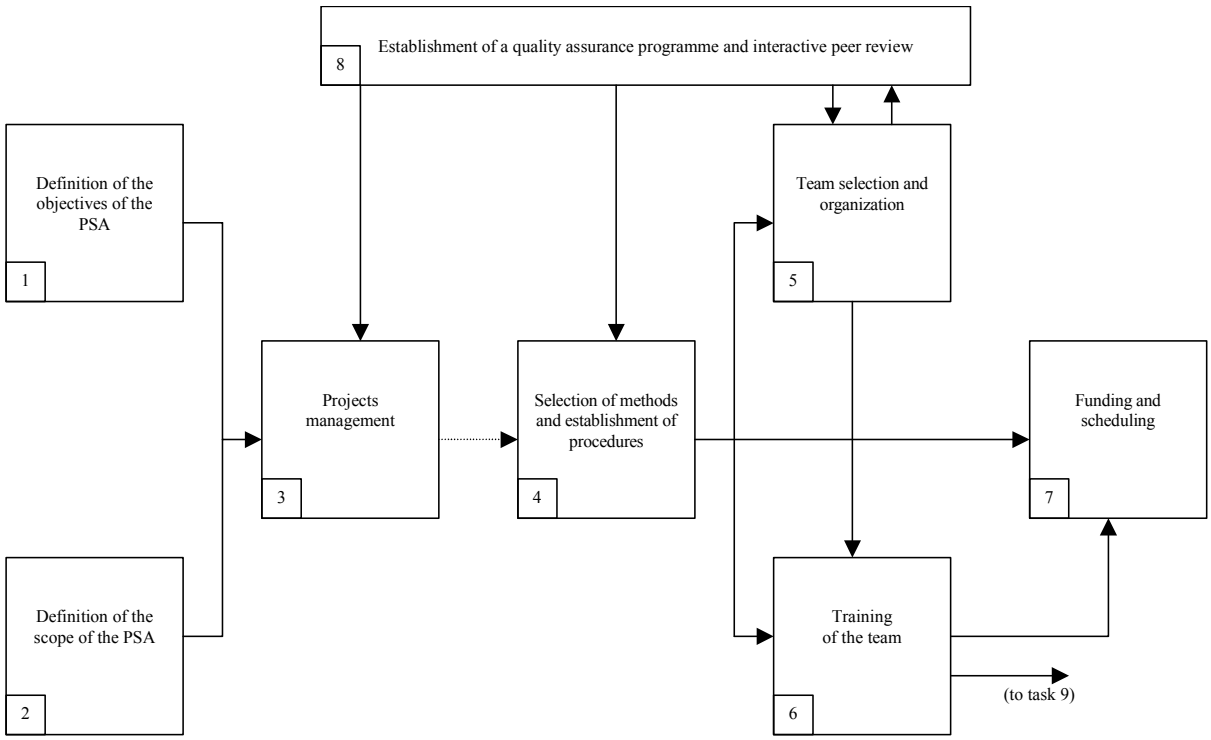

FIG. 3. Procedural tasks in the management and organization of a PSA.

Task 4 deals with the selection of methods and the establishment of procedures. The selection of methods depends on the type of NRNF under consideration and the objectives and scope (depth and range) of the analysis. Specific information concerning methodologies is presented in the discussions of the tasks throughout this report.

While all the requirements of each of the tasks listed above depend on the nature of the NRNF under consideration, particular attention is called to Tasks 5 and 6 (team selection, organization and training). The functions and the operations taking place at the specific NRNF under consideration may require specialized expertise to be added to the team in addition to the expertise discussed in Refs [2–4]. For example, it may be desirable for a particular facility to have expertise in process flow, chemical process safety and criticality safety. Task 9, dealing with familiarization with the facility, will provide an additional check covering the required make-up and training of the team.

3. IDENTIFICATION OF SOURCES OF RADIOACTIVE RELEASES/ RADIATION EXPOSURE AND ACCIDENT INITIATORS

3.1. General discussion

Section 3 describes the second major procedural step of a PSA. The main purpose of this step is for the PSA team to become familiar with the facility and its operation(s) and to begin the process of constructing risk scenarios. Through the completion of the tasks described in this section, a list of initiating events (IEs) will be identified. This list will be reviewed to determine which of the initiators should be subject to detailed analysis and how they can be grouped in order to simplify the analysis without the loss of important risk information. Upon completing this group of tasks, the PSA team will have developed a detailed understanding of the operation of the facility under normal and abnormal conditions and will have assembled sufficient information to permit the development of accident scenarios.

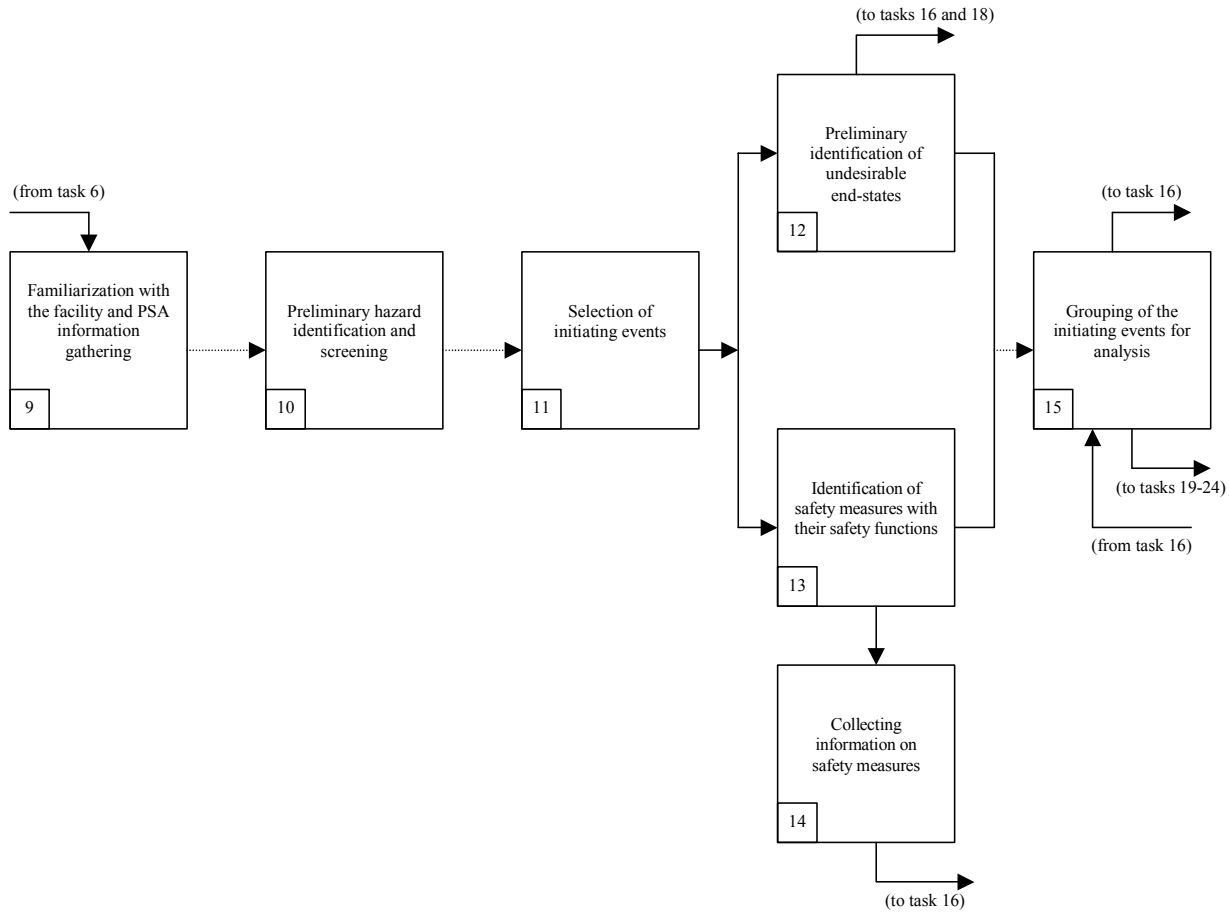

FIG. 4. Procedural tasks for the identification of sources of radioactive releases/radiation exposure and accident initiators.

This procedural step consists of the following seven tasks (Fig. 4). The task numbering follows consecutively from the eight tasks referred to in Section 2 and illustrated in Fig. 3.

Task 9: Familiarization with the facility and information gathering;
Task 10: Hazard identification and screening;
Task 11: Selection of initiating events;
Task 12: Preliminary identification of undesirable end states[10];
Task 13: Identification of safety measures with their safety functions;
Task 14: Collecting information on safety measures, and
Task 15: Grouping of the initiating events for analysis.

The sequence of tasks presented here is not necessarily the most appropriate in all cases. It will depend on the extent and detail of the information available as well as the iterative stage of the analysis. It should be noted that each task does not need to be completed before the next commences. Some tasks can run concurrently, in particular Tasks 11, 12 and 13 may be carried out for an individual initiating event, before other initiating events (from a different part of the facility, for example) are considered. The initiation of Task 9 precedes the other tasks, as Task 9 underpins each of the subsequent activities. However, it should be noted that

[10] For NRNF PSAs, 'end state' is defined as one member of a set of conditions, usually defined in discrete form, that characterizes the possible range of undesirable consequences identified in the PSA.

the ‘information gathering’ aspect of Task 9 will likely require it to continue in parallel with the activities associated with Tasks 10–15.

3.2. Familiarization with the facility and information gathering (Task 9)

Information gathering and familiarization with the facility represent the first ‘technical’ task of a PSA. These activities are important because they provide the bases for the PSA team to efficiently gain a detailed knowledge of the facility which will be needed to develop the PSA model. While gathering and reviewing important documents and information on the facility, the PSA team will develop knowledge of the normal and off-normal operations of the facility.

It is necessary that the PSA team have complete access to all relevant information and documentation. Typical information sources of interest to the PSA team include:

- descriptions of normal and abnormal operation processes including process operating ranges and limits;
- if multiple operational processes are possible, historical estimates of the fraction of time the different processes are in operation;
- emergency procedures;
- existing hazard analyses;
- existing safety analyses;
- operator training material;
- test and maintenance procedures;
- criticality analyses;
- environmental impact statement;
- descriptions of engineered safety systems and safety support systems;
- site characterization including geography, demography, meteorology, seismology and the location of nearby industrial facilities and transportation routes;
- facility layout drawings, including relation of facility to other buildings on the site;
- system flow, logic and control drawings;
- history of incidents at the facility;
- feedback from experiences at similar facilities;
- inventories of hazardous materials;
- applicable licences and licence conditions, if applicable.

A key element of this task involves direct communication with facility personnel in addition to access to facility documentation. It is anticipated that the communication with the facility personnel will continue throughout the project. Interviews with operations, maintenance and safety personnel are important; such interviews are likely to reveal important operational and safety insights.

Involvement of facility personnel is likely to have an additional benefit. By involving facility personnel early in the PSA process, they are more likely to understand the PSA results. This, in turn, will facilitate their acceptance and implementation of recommendations that might be made as a result of the PSA.

The information assembled in this task will form the basis for the subsequent definition of accident scenarios. Because of the importance of the information and the desire to make the bases of the PSA well documented and traceable, the information must be clear, sufficiently

complete and contain enough technical detail to allow correct definition of accidents and their potential consequences. It is therefore important that information be derived to the greatest extent possible from controlled sources which are designated formally by the facility staff. Additional relevant information should be collected in the form of interviews with key facility personnel. This information should also be documented. It is anticipated that, as the development of the PSA model proceeds, additional facility visits to gather information may be necessary. Information gathered from these subsequent visits should be documented and added to the existing documented information.

Because of the large amount of information gathered and because of the importance of this information, an information management system may be desirable. This system would organize and maintain the information in the form of a database. The information management system would also call for the designation of a person at the facility to be a central point of contact for additional information requests. The information management system should also include verification of the information in the database by cognizant facility personnel.

Operations at some NRNFs involve a number of distinct operations or processes intended to produce a certain product within specification. Facility processes might be of the 'batch' or 'continuous' operation type. In either case, it is important to understand and characterize the different processes (primary and auxiliary) and process phases, starting with the storage, handling and any pre-treatment of feed material. This process mapping should also include identifying the radiological, chemical and physical properties of process materials since both radiological and toxic hazards can be present. All processes should be reviewed closely for potential sources of risk. Activities associated with material processing, whether waste treatment or fuel fabrication include, for example:

- receipt of the incoming material and initial storage;
- storage of liquid material in tanks, or solid material in wet ponds and dry cells;
- transfer of liquid material through pipes between different process points or movement of solid material or containers by cranes and other transport means throughout different areas of the facility;
- physical treatment (e.g. compaction) or chemical processes (e.g. dissolution);
- processing and packaging the material for storage or further processing off-site.

As discussed previously, information on the different processes and process phases should be documented.

In addition, many NRNFs are capable of operating in a number of different modes. Modes of interest include different processing regimes, primary and backup, start-up and shutdown. An understanding of the different operational or process modes provides an important basis for the PSA. These modes should be reviewed closely for potential sources of hazards. The fraction of time the facility operates in each mode should also be determined. A complete knowledge of systems functions, capabilities (both normal and in response to off-normal conditions) is desired. It is also important to understand the training, procedures and guidance given to the operators for each facility process and for each operating mode. Safety functions which are to be fulfilled to ensure plant safety in each operational mode must be documented. System functional and support dependencies are of interest; these may also change as the operational mode of the facility or process changes. Existing safety analyses should be reviewed to identify and document safety barriers, potential end states, and the timing characteristics of important scenarios. The safety analyses may also provide

information on scenario-specific radioactive material release rates, release fractions and decontamination factors[11] that will be of interest in later PSA tasks. Any unique hazards and/or end states pertaining to specific operational modes should be identified as well.

The definition and understanding of the 'safe operating envelope' for the facility is of particular importance to this task. The safe operating envelope comprises those critical values of the technological process parameters and the physical and chemical properties of the materials that bound safe operating regimes. A facility should be designed and operated in such a way that it is not possible to breach this envelope under normal operations and very frequent events like startup, shutdown and transfer between operational modes. This enables a deterministic demonstration of safety to be made for normal and very frequent operations.

Any faults that cause the facility to move outside the safe operating envelope, and thus present a hazard, should be addressed using PSA. The identification of such faults in detail is the subject of Task 11.

Nuclear criticality hazards are of particular interest for some NRNFs. Existing analyses of nuclear criticality hazards should be identified and reviewed. Experience has shown that most commercial criticality events have involved the handling of liquids containing fissile material. Barriers and procedures controlling the amount, concentration and enrichment of material should be identified and documented. Similar information pertaining to the storage of fuel elements or other solid fissile material should be collected and examined.

Processes within an NRNF that involve toxic, hazardous, or radioactive materials that, if released, could interfere with the response of facility operators should also be identified and evaluated closely. As discussed in Section 3.3, these sources can represent indirect hazards.

3.3. Hazard identification and screening (Task 10)

Using the information gathered in Task 9, it is possible to assemble a list of potential facility hazards. Each hazard source could represent a threat to workers, members of the public, or the environment. Several techniques can be applied to assist in identifying hazards, such as hazards and operability study (HAZOPS), failure modes and effects analysis (FMEA), preliminary hazards assessment (PHA) and check lists. Performing such an analysis results usually in a large number of undesired events which need to be ranked. One methodology to rank the undesired events is a 'criticality analysis'. In this case 'a criticality analysis' is not related to 'nuclear criticality term', but is understood as a calculation of a 'criticality number'. In this number, three aspects are taken into account: the probability of occurrence (P), the severity of the consequence (S) and the probability that the most severe consequence will occur given the occurrence of the deviation (Beta).

Criticality number = P * beta * S

For a specific application, a framework has to be developed to determine the value of each parameter in a consistent manner. For instance, one can assign to each parameter a value between 1 to 5. The framework determines which number has to be used for each of the parameters in each specific case. The deviations with a high criticality number are those hazards which have to be analysed in detail.

[11] For NRNF PSAs, 'decontamination factor' is defined as the ratio of the activity per unit area (or per unit mass or volume) before a particular decontamination technique is applied to the activity per unit area (or per unit mass or volume) after application techniques.

Further information on some of the above mentioned techniques including “a criticality analysis” is provided in IAEA TECDOC-711 [12] and Ref. [9].

Both direct and indirect hazards should be identified and documented. Direct hazards are those that pose direct threats to workers, members of the public, or the environment. Indirect hazards are those that, while not leading directly to an initiator, would potentially impact the progression of events by influencing the ability of systems or facility operators to perform their functions. System functionality could be influenced, for example, by internal flooding if components of mitigative systems are damaged from immersion or spray wetting. Operator response to mitigate or terminate an event sequence could also be influenced by the presence of radiological hazards or toxic chemical materials.

Direct and indirect hazards can be from radiological and non-radiological hazard sources. Radiological hazard sources can lead to release of radioactive materials or exposure to people. These sources (comparable to the core damage category for NPPs) are the primary focus of the analysis. The complete list of hazard sources of this type should be developed and examined in order to identify possible dependencies in their behaviour under abnormal conditions. As a result of this consideration, some of the identified hazard sources may be combined and considered together in subsequent stages of the analysis.

The second type of hazardous sources are those associated with non-radiological effects, such as the release of toxic gases, the release of flammable materials resulting in fires, etc. Hazardous sources of this type should also be identified and listed. Thus within the scope of PSA for NRNF, these sources mainly affect common cause initiating event selection or sequence modelling due to their potential for systematic effect on facility systems or structures, operation and integrity.

For some NRNFs, there is significant overlap between the different types of hazards. Nevertheless, each hazard should be carefully considered with respect to its potential to result in an initiating event and its potential to influence the progression of events, given an independent initiator. It is possible that some hazards can be shown to not have the potential to cause upset of normal conditions, interact with other materials, or impact the ability of operators or systems to carry out their functions. Given the appropriate evidence, these hazards can be screened from further consideration. The disposition of each hazard must be completely documented. At this stage it is recommended that the scope be revisited in the light of the identified hazards and their anticipated consequences.

It may also be possible to show that, while the hazard has the potential to result in an initiator or impact upon the ability of the operator or systems to function, the frequency of such events is not significant. In such cases, it is suggested that this hazard be considered within another (comparable) scenario category — without the loss of significant information. It is not acceptable to completely eliminate such hazards from consideration at this point in the analysis, since at this early stage the PSA team does not know what the frequencies of other scenarios are. These hazards should be retained as a category for further consideration, once additional results are known. The amount of documentation required to justify screening out on a frequency basis should be weighted against the effort involved in retaining the hazards in the risk models.

A preliminary risk model, which would most likely be approximate in nature, and perhaps even coarse and simplified, should be developed as part of the facility familiarization and hazard identification tasks. By constructing such a simplified model early in the PSA

process, data voids can be identified early and a basis for the prioritization of specific technical activities can be established. The preliminary risk model is useful for other reasons — it allows:

- detailed consideration to be limited to the more important hazards;
- balancing of the effort which should be put into a refined and detailed analysis of the remaining hazards;
- design changes and facility improvements potentially to be made at an early stage.

Given the potential for adopting different design options for an NRNF, and for removing potential hazards by changing the design, this task is particularly useful during the design stage of a facility.

3.4. Selection of initiating events (Task 11)

Note: identification of hazard sources and selection of initiating events are usually conducted simultaneously.

The objective of this task is to produce a list of initiating events (or initiators) that is as complete as possible. As noted in Ref. [2], it should be recognized that it is not possible to produce a list that is exhaustive and complete. Judgement is required when determining that certain initiators not identified would make a negligible contribution to risk. The scope of the PSA, specified in Task 2, also influences the range of initiators that are to be considered.

Reference [2] discusses several approaches that have been used to identify potential initiating events for NPPs. These approaches involve engineering evaluation, reference to previous sets of initiating events, deductive analyses, and consideration of operational experience. Each of these approaches can assist the analyst in identifying the initiating events for an NRNF. Due to the diverse nature of NRNFs and the relatively small number of published PSAs for NRNFs, consideration of initiator categories from PSAs of other facilities may not be as important when compared with the corresponding analyses for an NPP; nevertheless, comparison with the available NRNF information will contribute to the creation of a list that is as complete as reasonably possible. Additional details for these approaches can be found in Ref. [2].

Because NRNFs many involve chemical and toxic hazards in addition to radioactive hazards, it is useful to consider additional approaches to identify potential initiators. IAEA-TECDOC-711 [12] identifies additional approaches useful in identifying and characterizing initiators. These additional methods, as mentioned in Section 3.3, include comparative methods such as safety audits; so-called fundamental methods such as hazard and operability studies (HAZOPS) and failure mode and effects analysis (FMEA); a ‘criticality analysis’ and additional logic or deductive methods such as release tree analysis or cause-consequence analysis. Additional information on these approaches can be found in Refs [9, 10, 12–15].

It should be recognized that the subsequent steps in the PSA analysis may reveal additional initiators for consideration and inclusion. Appendix II contains a listing of typical initiating events, which may be identified for different types of NRNFs.

3.5. Preliminary identification of undesirable end states (Task 12)

In the development of a comprehensive risk model, it is necessary to identify and characterize the potential outcomes, given the occurrence of an initiating event. A preliminary set of scenario end states is developed in this task. Scenario modelling is discussed in more detail in Section 4. Each accident scenario developed in subsequent tasks will be mapped into one end state. It is important, therefore that the end states be developed to allow a comprehensive description of the outcomes of the analysis scenarios, while keeping with the stated scope and objectives of the PSA.

If the objective of the PSA is to determine the probabilistic expression of the individual and societal doses to the public due to the operation of a specific NRNF, a set of discrete categories are to be developed to describe the spectrum of possible scenario outcomes. If the scope of the PSA is to include individual and collective dose to facility workers, appropriate categories for these measures are to be added to the set of end states. Of course, the chemical form and type of nuclide are important considerations for characterizing the dose.

Likewise, if the scope of the analysis is limited to describing the potential introduction of radioactive material into a specific element of the biosphere, then the end states must characterize the amount, chemical form and type of nuclide involved.

Insight into the potential magnitude of scenario consequences is provided by the review of existing safety analyses (Task 9) and the consideration of the hazard analyses performed (Tasks 10 and 11). It is appropriate that the analysis end state bins be coarse at this point. Refinement of the end states will occur in Task 18.

By establishing a preliminary set of analysis end states at this early point of the PSA, some insight will be gained, which can be used in prioritizing subsequent analyses and grouping initiating events.

3.6. Identification of safety measures and safety functions (Task 13)

Safety functions were identified in Task 9 for each operational mode of the facility. The hazards and potential initiators specific to the facility were identified in Tasks 10 and 11. In Task 13, the safety measures and safety features that need to function correctly in order to prevent, mitigate, or accommodate the postulated accident should be identified for each initiating event identified.

In addition, the specific requirements of the safety functions, first identified in Task 9, are to be refined and documented. It is important to include, in the specifications of the requirements, the operational characteristics of safety measures, and the features that would distinguish between the spectrum of scenario outcomes identified in Task 12.

3.7. Collecting information on safety measures (Task 14)

This task also builds upon and expands the information gathered in Task 9. The main objective of Task 14 is to provide the necessary confidence in the capability of the identified safety measures in such a way that they can be modelled appropriately in the scenario modelling tasks described in Section 4.

Factors to consider include whether the safety measure has an appropriate sensitivity to detect the need for action following specific initiating events, and whether the safety

measure has an appropriate response time, so that the fault condition arising from the initiator can be made safe before the accident occurs.

That the safety measures are capable of functioning correctly under the conditions created by the scenario should also be demonstrated. This consideration includes the conditions brought about directly as a consequence of the initiator, as well as operational limitations that are a result of additional potential degraded conditions (such as the independent loss of environmental control leading to high ambient temperature and humidity).

Clearly, any failures of safety measures that would lead to consequences upon the initiator should be identified, and any safety measures that have failed should not be claimed to be available in the safety assessment. Likewise, the PSA team should identify limiting conditions for safety measure effectiveness that might be encountered subsequent to an initiating event.

The relevant information should be obtained from the design specifications for the safety measures, and, for an existing facility, from testing carried out during commissioning and/or as part of a regular examination, inspection, maintenance and testing programme. These bases should be documented in the PSA.

In some cases, it may be necessary to consider specific development and testing programmes (for non-standard instrumentation, for example). If expert judgement and knowledge is used, it is important that the bases for the judgement and knowledge be documented.

3.8. Grouping of the initiating events for analysis (Task 15)

The objective of this task is to determine which of the identified initiating events should be analysed in detail in the PSA, and, furthermore, to attempt to minimize the amount of detailed PSA analysis required. This latter is achieved by grouping initiating events where it is possible to use the same or bounding scenario model without loss of significant information. In turn, the frequency of a group of initiating events is the sum of all the constituent group members. Initiators having different impacts on safety measures or features (or on requirements of the safety measures or features) should not be grouped together.

The list of initiating events produced under Task 11 should be reviewed. Where possible, certain initiators with ‘trivial’ consequences (below a predefined threshold), should be excluded from the detailed PSA. The screening process and the basis for any predefined threshold should be documented and should be within the context of the scope of the PSA. This will only be possible in those cases where there is a high degree of confidence that the consequences can be calculated accurately or with sufficient conservatism. This is likely to be the case for many of the simple accident scenarios that would be expected to be postulated typically for many NRNFs. Where the accident scenario is relatively complicated, and detailed modelling of the radioactive release mechanisms is required, the decision to screen out this initiating event or scenario should be deferred until Tasks 16–18 are undertaken.

It may also be possible, at this early stage, to exclude certain initiating events which are of a very low frequency, and which will not make a significant contribution to the overall risk. It is not possible to set a quantitative frequency screening criteria a priori. The cautions described in Task 10 are also relevant here. Any screening done on a frequency basis must be revisited once the quantitative results of the PSA are available to confirm the appropriateness

of the screening. The concern here is whether relatively important contributors to low frequency/high consequence end states have been appropriately identified and retained. Any initiating events that are classified during this task as not needing further analysis should be recorded in appropriate documentation.

4. ACCIDENT SCENARIO MODELLING

4.1. General discussion

This procedural step includes all aspects of building the accident sequence models. The objective of this task is the development of a model that links the initiators of potential accidents, the response of the facility to these initiators, and the spectrum of resulting end states.

The scenario modelling portion of the PSA consists of the following three tasks:

Task 16: Logic modelling of accident sequences;
Task 17: Human performance analysis, and
Task 18: Consequence analysis.

A schematic representation of these tasks is shown in Fig. 5. Once again, the task numbering follows sequentially from the tasks described in Section 3 and shown in Fig. 4.

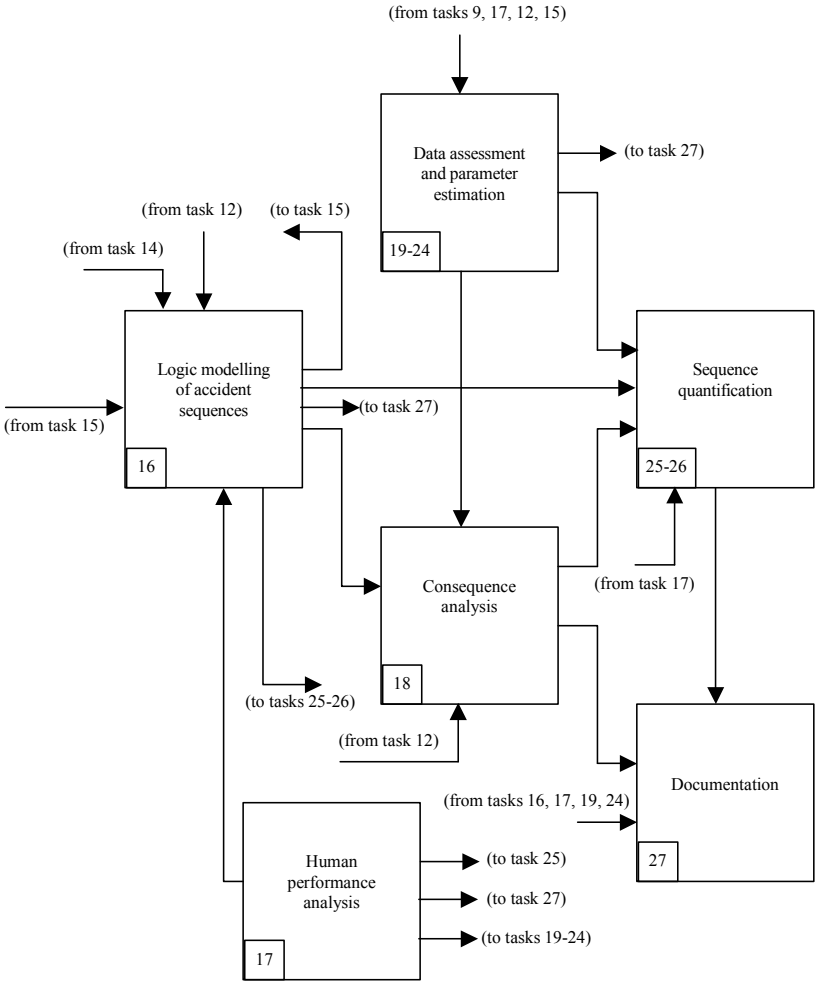

FIG. 5. Procedural tasks for accident scenario modelling.

4.2. Logic modelling of accident sequences (Task 16)

4.2.1. General discussion

Depending on the complexity of the process modelled, different methods can be applied to modelling. The most widely known methods for modelling event sequences in complicated systems and processes are the event tree analysis (ETA) and the fault tree analysis (FTA) methods. Many applications utilize a combination of event and fault trees to represent potential accident scenarios.

Regardless of the modelling methods chosen, the goal of Task 16 is to develop a logical representation linking the initiating events to the corresponding possible end states. This is accomplished by constructing an event sequence model that represents the possible combination of safety functions (associated with the equipment performance) and operator responses following the occurrence of each of the initiator groups. An event sequence model, therefore, describes the sequence of events that, following an initiating event, lead either to a successful state or to a failed state of systems and operator actions intended for mitigating the consequences of initiating events.

System failures are logical combinations of simpler events (e.g., component failures). In PSAs conducted for NRNFs, it may be convenient to represent the system response as multiple discrete states, rather than simply binary states (success or failure). Also, it may be convenient to include, along with the response of systems and facility operators, phenomenological questions, or "events," in the event sequence model. An example of the latter might be asking whether an explosive amount of hydrogen has built up in an enclosed space during a certain critical time. The probabilistic answer to such a question might be a function of the uncertainties in the hydrogen generation or release process and dependent on the outcome of a previously queried element of the scenario.

Particular techniques for event sequences and system modelling are presented in Refs [16–19]. The general techniques for constructing, manipulating and quantifying fault trees are described in Ref. [20].

Depending on the complexity of the facility, the scope of the PSA, and, to an extent, analyst preferences, other methods can be applied both for event sequence and for system modelling.

For event sequence modelling, alternate or supplementary methods include:

- cause-consequence diagrams, and
- event sequence diagrams.

For system modelling, additional methods include:

- state space diagrams and Markov analysis;
- block diagrams;
- go charts, and,
- general mathematical simulations of physical systems (e.g., Monte Carlo).

Time dependencies may be important in the consideration of accident scenarios in an NRNF PSA. In situations where time dependencies cannot be modelled satisfactorily using Markov analysis, special methods such as dynamic event tree analysis may be useful [21, 22].

Appropriate care must be taken when using any modelling technique, as each has advantages and disadvantages. For example, in the case of Monte Carlo simulations, it must be considered that incidents with a low likelihood of occurrence can be inadvertently left out of the simulations, unless care is taken. The analyst using fault trees, for example, might encounter challenges when considering circular logic or may inadvertently eliminate information involving 'high order' events (i.e., logic involving multiple failures, regardless of the likelihood of such events).

4.2.2. Attempt at simplification

In many cases, the task of modelling accident sequences may be rather simple for NRNFs. It may even be possible that frequencies of occurrences can be derived directly for accident scenarios. In such cases, a simple spreadsheet might be sufficient to represent and quantify the event sequence model. Examples of this are scenarios involving vehicle accidents in a nuclear waste repository. The collection of vehicle accidents in the different parts of the facility are directly quantified as regards their frequency of occurrence, the resulting releases of nuclear materials are assessed and the consequences associated with each type of accident are calculated directly.

In the case where PSA is performed in order to demonstrate compliance with a safety criterion, it may be worthwhile to test how easily the safety criterion is met at an early stage of the analysis. If the safety criterion is easily met, then the analysis can be made simpler and less time consuming by assuming pessimistic values for the scenario frequencies. If the criterion is met under these conditions, then 'best estimate' values need not be calculated, and sensitivity analyses need not be carried out. The savings in effort and time could be large. An obvious analysis assumption made in such a case is that by meeting the stated criteria, no unacceptable risk is posed. However, caution should be exercised when using pessimistic values for frequencies or consequences if the PSA results are to be used to determine the importance of safety measures or to support planning of plant safety upgrading. Only by using a best estimate approach or consistent level of conservatism for all fault sequences, can the relative importance of different faults and corresponding safety measures be assessed.

In cases where the safety criterion is simply radiation dose or another quantitative consequence parameter, considerable simplification can be achieved by focusing the analysis on the bounding or extreme cases relevant to the process or group of accidents to demonstrate that the criterion is met. If the maximum consequences for a particular process or group of accidents can be shown to be less than the safety criterion of interest, then modelling to identify how such accidents may occur might not be necessary. Similarly, early information on quantitative consequences can be useful in defining categories of accidents, which can be used as a basis for simplifying the modelling for the scenario. These consequence calculations can be performed both before and during detailed scenario modelling.

One should be aware that some bounding assumptions that might be considered for such calculations, such as release of 100% of the inventory, may be so physically unrealistic that the results are misleading. The ideal bounding case is one that is physically possible, but at or near the maximum. When such calculations depend upon input factors that may vary stochastically, such as weather, the probability distributions on these factors should also be modelled.

4.2.3. Fault tree/event tree

Fault trees and event trees are the most common methods used for modelling the logic representing the facility response to accident initiators. These methods are capable of

representing all credible ways in which the defined undesired state may arise. Faults can be events that are associated with component hardware failures, human errors, common cause, maintenance or unavailabilities, or any other pertinent events that lead to the undesired state. If available, the failure modes and effects analyses (FMEAs) for engineered safety measures should be consulted as a basis for producing logic models of accident sequences to assure completeness of the analysis. A detailed description of these methods is given in Ref. [20].

In the case of a nuclear waste repository, an example of a system for which event trees and fault trees are an appropriate analysis method is the automated system of moving waste by the mine hoist to an underground location. The loading of waste containers onto a low bed rail carriage may be a final manual action, before an automatic process moves the rail carrier through a series of interlocks (mechanically and digitally controlled) into the cage of the mine hoist, then the cage is lowered and the rail carrier removed from the cage at the defined underground depth. Assessing the accident scenarios associated with this process (e.g., collisions between mine cage and structural parts of the shaft, overrun of the cage, drop of heavy loads onto waste containers) and assigning frequencies of occurrences can be facilitated using the fault tree/event tree methods.

Depending on the complexity of the analysis, a cause-consequence or an event sequence diagram in addition to fault tree and event tree may be useful. While a short description is given here, more information is provided in Ref. [20].

A cause-consequence diagram may, under certain circumstances, be used instead of an event tree. One key advantage of the use of a cause-consequence diagram is that this method allows more complex branching than the simple binary (yes/no) logic offered by many common event tree computer codes. The applicability of its use is left to the analyst [2] and is to be judged given the complexity of the problem.

The event sequence diagram is a variation of the cause-consequence diagram. Its use involves determination of a significant amount of design and operational information and is mainly used as a step that is preliminary to the construction of event trees. It may be useful in complex situations.

The use of cause-consequence diagrams or event sequence diagrams offers an additional advantage. The diagrams created in these methods, in general, are more easily understood by non-PSA specialists, and therefore can greatly assist in the documentation of the event model.

Before any specific method is applied, a thorough understanding of the operation of the system and that of its components, operator actions, and the effects of their failure on system success is necessary.

4.2.4. Dependencies and common cause failures

Dependent failures can be dominant contributors to the frequency of the undesirable end states and to other PSA results and they should be taken into account in the analysis regardless of the modelling approach selected. In cases where event trees are not used for event sequence modelling, attention must be paid to the proper handling of the dependencies that would appear in the fault trees and to ensure that the they are identified and modelled correctly [2].

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

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

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

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

Functional dependencies include physical interaction between measures, systems and components which can occur when the loss of function of a system or component causes a physical change in the environment of another system or component — for example, a loss of trace heating on a section of pipe that allows it to freeze in cold weather.

Physical dependencies can arise in two ways. Firstly, an initiating event can cause the failure of a safety measures, systems and components and failure of some of the safety systems or components required to provide protection. Secondly, an internal hazard (such as a fire or a flood) or an external hazard (such as extreme environmental conditions, a seismic event, etc.) can cause an initiating event and failure of some of the safety structures, systems or components required to provide protection.

It is important to analyse the interaction between the progression of the physical process and the performance of the required measures, systems and components. To correctly incorporate the effects of physical processes on the accident sequences, the operability of the required systems must be assessed, i.e., the effect of accidental environmental conditions on the engineering safety features and their support systems must be analysed in detail.

One example of how physical processes may influence the progression of events can be found by considering the loss of the heating, ventilation and air conditioning system. Increasing temperature and humidity may affect the functioning of mechanical or electrical equipment, the ability of operators to take appropriate action and the quality of information provided to the operators.

The equipment within the facility for enabling the operator to perform his tasks is a strong influencing factor. This is also true of computer systems. As mentioned, there may exist in a modern facility more or less sophisticated operator support systems that are computer based, that monitor the facility performance and that display information to the human operator via a man-machine interface (graphic display). The functionality of such systems is influenced by the design goals specified during their development.

The ability and appropriateness of such systems to correctly inform the human operator of the different facility states needs to be investigated and included in the facility modelling process. For example, an initiating event may incapacitate some monitoring functions (the initiating event may change the temperature of the environment in which a sensor is situated in such a way that it operates out of its designed temperature range and its output may be

unreliable). Hence, the ability of the operating staff to correctly interpret the information displayed is reduced and this should be reflected in the facility model.

Human interaction dependencies arise when the operators make errors during repair, maintenance, testing or calibration tasks which lead to the unavailability or failure of safety measures, systems and components in such a manner that they will not operate when required following an initiating event. Human interaction dependencies can also arise during the 'post-accident' phase, when manual actions are to be performed that require the operator to interact with multiple components.

Component failure dependencies cover those failures of usually identical components which are otherwise not analysed. Such failures may be caused by errors in design, manufacturing, installation, calibration or operational deficiencies and are treated quantitatively by common cause failure methods or other dependence quantification approaches. Common cause failure probabilities are usually quantified by using the alpha factor approach, the beta factor approach, the 'multiple Greek letter' approach, or the binomial failure rate model to assess the probabilities of common cause failures on similar (redundant) components. Additional guidance in this area is given in Ref. [2].

4.3. Human performance analysis (Task 17)

4.3.1. General discussion

This task analyses the human performance associated with the initiating events and subsequent system responses. Human acts to be covered are all those identified during the course of model development as having a potential impact on the structure and results of the models. Usually human performance analysis considers only errors of omission, although some recent developments have been published providing guidance on how errors of commission can be evaluated and modelled in a PSA [23, 24].

The evaluation of human performance depends on the complexity and the degree of automation of the technical process. In general, there are more actions and tasks performed by humans in NRNFs than in NPPs, and therefore the evaluation of the human performance can take on a more dominant role. The depth of human performance analysis is driven by the PSA scope and objectives, and influences the selection of analysis methodology. This section segregates human performance analysis into two broad categories: qualitative or quantitative.

4.3.2. Qualitative human reliability analysis

A qualitative human reliability analysis (HRA) is necessary to identify those possible operator actions which, if not properly performed, will have an adverse impact on the development of the accidents.

HRA generally involves the evaluation of tasks within a procedure or sequence, taking into account factors such as the complexity of the task, the conditions under which it is performed and the mental and physical characteristics and limitations of the operator.

There are different forms of HRA task analysis, as detailed in Ref. [2]: task decomposition, hierarchical task analysis, time line analysis, task simulation, and ergonomics checklists. Each technique has particular applications, limitations and advantages and disadvantages. The safety assessor must decide, possibly in consultation with a Human reliability specialist, which technique should be applied and to what extent.

4.3.3. Quantitative human reliability analysis

Whenever the depth of analysis is such that potential human errors are represented in safety assessment fault trees or event trees, quantification of human error probabilities through quantitative human reliability analysis is required.

4.3.3.1. Quantification of human error probabilities

Human error probability values may be assigned to the human errors using one or more of a number of following information sources or techniques. In all cases, the individual conditions of the human error under consideration must be taken into account, such as the performance shaping factors, and the value must be adjusted as required. Suitably qualified and experienced human reliability specialists should be consulted if necessary.

Previous examples

Whenever the safety assessor is revising a safety assessment and is able to confirm that there have been no significant changes to the facility operating procedures and conditions, it may be possible to use the human errors analysis of the previous safety assessment as a basis for the current safety assessment.

Human error databases

It may be possible to select a human error value by comparing the human error with others which have been compiled as part of a database, and for which values have previously been assigned. Extreme care must be taken when using such a database. Justification must be provided that the context and factors influencing the human performance are sufficiently similar for the NRNF scenario under consideration when it is compared to the bases for the actions found in the database.

Derivation of human error probabilities using quantitative HRA methods

In the absence of previous examples or relevant human error databases, human error probabilities can be calculated using various methods published in the literature. There is a consensus on the usefulness and applicability of certain techniques for evaluating human performance, such as those discussed in Ref. [25] and in the IAEA report providing guidance on HRA [26]. Examples of specific techniques include the THERP method [27], SLIM-MAUD [28], ATHEANA [23, 24], and HEART [29].

The development of methodologies to represent and understand human performance is continuing on several fronts. In the selection and application of a specific methodology, four guidelines should be taken into consideration:

- the assessment applied to each action evaluated should be consistent;
- all actions should be evaluated within the context of specific event scenarios;
- the evaluation should have as a goal that the qualitative ranking of all actions be correct; and,
- the quantitative evaluation of the actions should be traceable.

Software based quantification tools

Some software tools are available that will calculate a value for a human error. Programs of this kind require the input of parameters that could influence the human error

probability, such as the complexity of the operation, availability of instructions, degree of training, time available to carry out the operation, etc.

Human reliability advice

Advice should be taken whenever necessary from suitably qualified and experienced human reliability specialists. The advice may result in further examination of the human errors, e.g. by qualitative methods.

4.3.3.2. Human interaction dependencies

Dependencies between different operators or between different tasks performed by the same operator can significantly affect the overall level of reliability. The safety assessor should therefore take great care to identify dependencies that may exist between different operators, between different errors committed by the same operator, and even between hardware failures and operator action.

Where dependencies exist, their effects need to be evaluated and quantified. In some cases this is already accounted for in the individual human error data, and in other cases dependencies are accounted for by the performance shaping factor effects. Specialist advice should be sought where dependencies are identified that are not accounted for in the human error data. Where specific dependencies cannot be identified, then human performance limiting values are used to limit the claims for human reliability for multiple operator actions. Human error evaluations implying error likelihoods less than 1E-4 require particular justification, while evaluations implying error likelihoods less than 1E-6 are extremely suspect and most likely should not be used.

4.3.3.3. Non-credible events

Where the safety assessor is able to determine that the adverse consequence of the human error is not credible, then a suitable argument may be made in the safety assessment, and the error need not be modelled in the fault trees. For example, where a failure to evacuate would only result in an unacceptable dose to the operator after several days, since it is not credible that an operator would remain in one place for this length of time.

4.4. Consequence analysis (Task 18)

Initiating events result in facility responses that develop in a spectrum of ways with different consequences and likelihoods. It is possible that the response to some initiators could result in the breach of the barriers of the facility and subsequently result in off-site consequences by releasing radioactive material into the environment. Other facility responses may have only on-site effects, and are of consequence only to the operating personnel. Either cases, or the combination of them, are important and it is of fundamental importance that the PSA identifies and describes all such significant scenarios.

The consequence analysis task can be divided into four sub-tasks, i.e. the estimation of:

- the source term;
- off-site consequences;
- on-site consequences (including airborne releases), and
- direct radiation consequences.

4.4.1. Source term estimation

This requires suitable calculations to estimate the effect of an accident in terms of quantity and type of radioactive material discharged to the environment, and/or released to the working area (specific models may be required for individual accident sequences, and there may be a wide range in the complexity of model required).

Certain accidents may have end states leading to the emission of direct radiation. The magnitude of this radiation should be calculated and may require complex computer codes, for example to estimate source strength from criticality accidents.

The analysis requires systematic consideration of the breach of barriers, both the process ones, such as vessels and surfaces, and safety barriers, such as cell structures, ventilation systems, and other containment.

The determining element of the consequence analysis is the source term calculation. This requires good understanding of the physical process under off-normal conditions. The source term is usually defined as time-dependent release of radioactive material from a defined boundary, which can be an internal boundary of a facility (e.g. from the breach of a waste container) or the facility perimeter. A radiation source can be generated by a criticality event or by a release of radioactive material in a compartment. The degree of sophistication of these calculations should be appropriate for the intended use.

4.4.2. Estimation of off-site consequences

This entails calculation of the effect of any radioactive material released to the environment (as liquid or airborne effluents), generally in terms of dose to a member of the public. Typically, a small set of standard models, covering all possible release and exposure pathways, will be needed. Once created, the models can be used for individual accident sequences. Because of the complexity of some of the pathway modelling, it is possible that a consequence analysis computer code would be used. See Ref. [4] for comprehensive details.

4.4.3. Estimation of on-site consequences (including airborne releases)

This sub-task requires calculation of radiation exposures to persons on-site through different models. Estimations of the dispersion within operating areas and around the facility, and other exposure related data such as breathing rate and period of exposure (related also to response to alarms, effectiveness of emergency procedures, etc.) can be used to accomplish this task. For non-radiological hazards, where applicable, the evaluation of consequences can involve calculating air concentrations of toxic substances and comparing the concentrations with published criteria.

4.4.4. Estimation of direct radiation consequences

If the accident can result in direct radiation exposure, generally only applicable to members of the workforce, the effects, typically in terms of dose received, should be calculated. An example in a fuel storage facility may be the inadvertent over-raise of irradiated fuel from a pond. There are generally accepted, well established methods available for this type of calculation, and no further guidance is given here. However, in addition to the detailed calculations for exposure, it may be necessary to estimate an exposure time. This will be dependent on the time taken to evacuate the area following the accident. This in turn is dependent on how obvious the accident is, whether and when installed alarms will be activated,

the degree of training the workforce has received in matters of emergency responses, and how easily a worker can escape from the affected area. All these matters need to be taken into account in calculating the exposure.

5. DATA ASSESSMENT AND PARAMETER ESTIMATION

5.1. General discussion

The objective of the fourth major procedural step is to acquire and generate all information necessary for the quantification of the sequence frequency and consequence assessment models developed using the methodology described in Section 4.

The data assessment and parameter estimation portion of the PSA consists of the following six tasks:

Task 19: Assessment of component/system reliability, common cause failures and initiating event frequency;
Task 20: Assessment of human error probabilities;
Task 21: Data for the determination of the facility damage and undesirable end state and source term;
Task 22: Data for estimating the effect of releases on members of the public;
Task 23: Data for estimating the effect of airborne releases on members of the workforce; and,
Task 24: Data for estimating the effect of direct radiation.

Tasks 19 and 20 are related to sequence frequency estimation, whereas Tasks 21 to 24 are concerned with consequence assessment. Completion of all the above tasks may not be required for every particular sequence assessment. For example, a sequence with the end state of an exposure to a sealed source or waste container would not require the completion of Tasks 22 and 23.

A general recommendation applicable to the derivation of most categories of data is that best estimates of key parameters should be selected over conservative estimates. The use of best estimates allows for a realistic determination of accident frequencies and consequences. In contrast, the use of conservative parameter values can lead to excessively conservative determinations that loose sight of realism. It should also be noted that because of the nature, diversity and complexity of the processes and phenomena considered within NRNFs, the uncertainty of the data used within the sequence frequency and consequence assessment models should be considered. Furthermore, simplification of the modelling of complex processes and phenomena may result in additional uncertainty. Chapter 6 provides further discussion on the issue of uncertainty within the quantification tasks. Again, the task numbering follows sequentially the tasks described in Section 4.

5.2. Data for sequence frequency estimation

Section 5 of Ref. [2] (Data Assessment and Parameter Estimating) contains information on methods that can be used for collecting, generating and using data in order to provide the necessary input to the sequence frequency model. More specifically, the assessment of initiating event frequencies is discussed in Section 5.2 of Ref. [2], component and system reliabilities and unavailabilities are discussed in Section 5.3, common cause failure probabilities are discussed in Section 5.4, and human error probabilities are discussed in

Section 5.5 (although these last topics are treated only briefly, with considerable references to supporting documents).

For certain NRNF accident sequences, there may be significant time-scales involved in the development of the accident scenarios. This may call for a more detailed evaluation of recovery actions in PSAs for NRNFs than would be the case for PSAs for NPPs. The consideration of actions that could lead to return to the safe status of the facility within the sequence frequency and consequence assessment may require careful consideration of the reliability data utilized. For example, consideration of a successful repair of a component, and the related variations in the human error probabilities (to reflect the available time-scales and scenario conditions) influence the sequence frequency and consequence. Examples of the treatment of recovery events within NRNF analyses are given in Refs [30–33].

As for all PSAs, the data used in NRNF PSAs, including the component reliability, has to adequately take account of the possible dynamic process and facility conditions that might exist at the time of the initiating event and throughout the accident scenario. An example of a review of the effect of time dependency of reliability data on the frequency is given in Ref. [34].

5.2.1. Assessment of component/system reliability, common cause failures and initiating event frequency (Task 19)

In general, data can be of two types: facility specific or generic. Facility specific data, i.e., data obtained from records of system or component failure rates or non-availabilities are the preferred data, however, in most cases plant specific data are not available for NRNFs. Generic data (data derived from an industrial facility of a similar nature or component behaviour under equivalent conditions of usage) are applied to the models whenever facility specific data are not available. Reference [35] includes a listing of eight databases of generic component reliability. Other information on component reliability is available in Ref. [36]. One of the main issues with generic data is their applicability to the facility considered, its particular components and operating regime. Rarely are data available which are entirely applicable, and the analysts should use their judgement in selecting the best sources for each case.

If facility specific data are available but sparse, one alternative is to create a facility specific database by combining facility experience with generic information using Bayesian techniques [2]. Either way, the data used should be sufficiently well justified in the PSA documentation and should be shown to be relevant, item by item.

It is important that the frequencies of common cause initiators and the probabilities of mechanical interactions on the engineered barriers (including filters) be included in the scope of detailed analyses. Information on equipment or component repair times is also important for assessing the recovery of degraded safety functions.

5.2.2. Assessment of human error probabilities (Task 20)

This task is integrated with Task 17 discussed in Section 4. Data for use in such models should preferably be derived from facility operating experience, or from similar facilities under similar operating regimes. Additional information on this topic is available in Refs [26, 37].

5.3. Data for consequence assessment estimation

5.3.1. Data for the determination of facility damage/undesirable end state and source term (Task 21)

Some degree of analysis is required to determine selected facility and process conditions following an accident. Examples of such conditions include the temperature of a vessel's contents during a loss of coolant scenario, the degree of rupture of a vessel as resulting from an internal hydrogen explosion, and the degree of damage to a container following a drop. The undesirable end state depends on the specific conditions that result from the accident. For example, the severity of a hydrogen explosion and the corresponding severity of vessel rupture will depend on the amount of hydrogen generated, the presence of oxygen or other oxidizing agent, and the characteristics of the vessel that is ruptured.

The actual data requirements depend on the damage/release model postulated. Where simplified analysis is acceptable, it may be convenient to make the conservative assumption that the undesirable end state is the rupture of the vessel with complete loss of its contents. In other cases, where a complex analytical model is to be used and/or where a more refined analysis is desired, there may be significant data demands. Also, for complex modelling, the use of best estimates for key parameters is recommended over conservative values to avoid the cumulative effect of multiple conservatisms. Finally, in some cases, actual tests can provide the data needed; for example, impact tests for a container will provide the needed data directly.

Having determined the facility and process state produced as the result of an accident, it is then possible to calculate the amount of radioactive material that will be released to the working area and to the environment. In general, this will require modelling the fraction of material released from a given source as well as the behaviour of containment barriers such as glove boxes, cell walls, building fabric, waste containers, etc. Models used to calculate this release were developed in Task 18, as described in Section 4. The data required for these models to be quantified, generally take the form of release fractions (RF) and decontamination factors (DF), and are ideally based on experiments or derived from well understood physical models. Some data are available in the open literature; some may be obtained from in-facility data acquisition processes; other data are likely to be available on a commercial basis. Every effort should be made to acquire 'good' data, or confidently pessimistic data, since the calculated consequences are generally proportional to, and thus 'sensitive' to, such values. This is especially true where a minor change in RF or DF value would affect the conclusions of the assessment. Sensitivity studies should be considered when the uncertainty in the data is high.

5.3.2. Data to estimate the effect of releases on members of the public (Task 22)

Health effects information and models are used to determine the doses to workers and the public as the result of an accident. To calculate doses for members of the public, it is necessary to consider the transport of radioactive material to the environment where it can be breathed, ingested, or absorbed. Site specific meteorological and topographical data are needed for use in the transport models, e.g., the average wind speed and direction, temperature, atmospheric stability. The locations of the nearby population groups (critical groups) must also be identified, as the distance and direction (relative to prevailing wind directions) will influence the rate of transport of radionuclides and the degree of atmospheric dispersion. Transport through surface and ground water, would require information on water

velocity and direction, water temperature, and the physical, chemical and biological agents present.

To assess the exposure of individuals from the released radioactivity, the characteristics of nearby population groups must be determined. The data required for this includes, for example, site specific information on the location and size of water sources, population density, location and size of any farms used to produce fruits, vegetables, and meats, etc. Based on these characteristics, the exposure pathways are then identified, such as inhalation, direct exposure to radionuclides in air and water, absorption of radionuclides in soil and water and subsequent biological transport through the food chain. Analysis to determine the exposure of individuals via the identified pathways (pathway analysis) requires additional data, such as soil characteristics, water chemistry, etc. The final data needed in the pathway analysis are dose conversion factors (DCFs), such as those published in Refs [38, 39]. Reference [4] contains details of the data requirements for off-site consequence modelling. Table II lists typical examples of data that might be required to calculate the dose arising from a release of radioactive material from an NRNF.

5.3.3. Data to estimate the effect of airborne releases on members of the workforce (Task 23)

For indirect exposure of the worker, models must take into account the airborne concentration of radioactive material, the breathing rate of the worker, the rate of absorption through the skin, and the biological half-life of the various radionuclides. In addition, data relevant to the dispersion of material within the working area will be required; this may involve parameters relevant to ventilation flows, etc. The final data needed in calculating worker exposures are dose conversion factors (DCFs), such as those published in Refs [38–40].

5.3.4. Data to estimate the effect of direct radiation (Task 24)

There are well established methods for calculating the dose resulting from direct exposure. The data needed for these models include the amount and configuration of radioactive material, the shielding provided, and the distance of the material from the affected individual.

6. SCENARIO QUANTIFICATION

6.1. General discussion

This section addresses the process of scenario quantification, sensitivity and importance measure analyses, which greatly aid in the interpretation of the PSA results. Again, the numbering of these tasks follows sequentially from the tasks discussed in the previous section.

6.2. Quantification of the accident scenarios and calculation of risk (Task 25)

The intent of a PSA is to deliver qualitative and quantitative results that enable the safety of the facility to be assessed. The depth of analysis, whether semi-quantitative or quantitative, is dictated by the objectives of the PSA study and the nature of the facility (Section 1.3). In connection with the objectives of the study, it is important to determine what

TABLE II. INFORMATION/DATA REQUIRED TO CALCULATE THE DOSE DERIVED FROM A RELEASE OF RADIOACTIVE MATERIAL FROM AN NRNF

Failed fuel, gap release	Release rate for noble gas, halogens, volatile solids, and non-volatile solids (aerosol)
Boiling pool release, evaporating pool release	Release rate for noble gas, halogens, volatile solids, and non-volatile solids (aerosol)
Fire release	Release rate for noble gas, halogens, volatile solids, non-volatile solids (aerosol), and fly ash airborne particle size
Explosions	Release rate for noble gas, halogens, volatile solids, and non-volatile solids (aerosol) airborne material density and particle size
Criticality	Initial pulse — number of fissions Secondary pulse — number of fissions and pulse interval Total number of fissions and total time Gas release fraction Halogen release fraction Solid release fraction Material release fraction
Particulate filters	HEPA filter DF for each stage Sand filter bed filter DF Fiberglass — deep bed filter DF
Halogen filter	Inorganic absorber DF Silver zeolite DF
Miscellaneous parameters	Resuspension factors Plate-out DF for iodine and particulate Pool DF for gas, inorganic and organic iodine, and solids
Release from free liquid surface	Release rate of radioactive material from liquid phase to atmosphere
Release from surface of molten glass	Release rate in the compartment of volatile radioactive material from glass

types of results are required. The regulations in several Member States (refer to Appendix IV) provide various criteria that must be complied with for facilities resident in those States and there may be operational reasons for understanding the significant risk contributors in a facility so that operations may be optimized. The PSA analyst should be fully aware of these requirements and focus the analysis so as to provide information to address them directly.

It should be noted that the PSA process, by its nature, is iterative. Initial results are obtained, the results are reviewed, the models refined, and new results sought. This process is repeated until subtle modelling and expert judgement errors have been corrected and analysis conservatisms relaxed to a sufficient degree to permit the PSA results to be used. Sections 6.2, 6.3 and 6.4 of Ref. [2] contain additional guidance in this regard.

Generally, but not always, an important goal for a PSA for an NRNF is to quantify risk. Various risk measures can be defined depending on regulatory and operational requirements. These include:

— Semi-quantitative risk, i.e., the use of a mixture of quantitative and qualitative information to make risk informed decisions about the facility.
— Frequencies of important fault sequences. This is generally not used as a risk measure in itself, but in conjunction with dose information to aid risk informed decision making.

— Dose to an individual worker or member of the public from the worst fault sequence.
— Frequency of dose uptake per year from all pathways to an individual worker or member of the public, integrated over all fault sequences.
— Frequency of fatality per year to an individual worker or member of the public, integrated over all fault sequences.

These risk measures can be applied to workers and/or members of the public. Different definitions of these categories of persons are given by Member States; the analyst must understand the definition that applies to his analysis so that the correct consequence models can be used. Other factors might also be considered in particular cases, such as rate of dose uptake or duration of release of radioactive material. These are often important for emergency planning purposes.

For the quantitative risk measures (e.g., annual frequency of fatality), either fault sequence frequency, or dose consequence, or both must be quantified. Description of techniques for this quantification used in NPP PSAs can be found in Refs [3, 4, 41]. Although specific to NPP PSAs, these techniques can be extrapolated for use in PSAs for NRNFs. Often, regulatory bodies or individual organizations provide specific guidance on PSA quantification methods.

When integrated risk for a facility or process is calculated, this is generally taken as the sum of the individual risks for all fault sequences in the facility. The analyst must take care to account for the following effects:

— All significant faults should be assessed in sufficient detail to enable the required risk measures to be reliably computed.
— When bounding fault sequences are assessed, an estimate of the effect of the faults they bound should be included (e.g., by summing all the bounded fault frequencies and using this as the frequency of the bounding fault).
— The effect of screened out faults should be simplistically assessed. Individual screened out faults may be trivial, but if a large number of such faults exist, their cumulative effect may not be. An allowance for this effect, if it exists, should be made.

The proper calculation of accident frequency requires the correct construction of event trees, fault trees, or other logical representations, including a realistic representation of all dependencies between equipment failures and human actions. Data must be supplied for initiating events, equipment unavailabilities, and operator errors (see Sections 4 and 5). It is inevitable that there will be simplifying assumptions and idealizations of rather complex processes and phenomena. These simplifications and idealizations will involve uncertainties that are reflected in the probabilistic nature of the parameters.

With regard to this probabilistic nature, the analyst may choose to calculate these uncertainties explicitly. This requires explicit probability distributions to be defined for input parameters and results in probability distributions being calculated for risks, rather than single values. If single values of risk are needed they can be extracted from the probability distributions as, for example, the mean value or 95% confidence level value. Explicit uncertainty calculations are generally complex and require the use of computer codes and specialist techniques. Guidance on these techniques can be found in Refs [42, 43]. One of the main advantages of PSA is that it can identify a number of sources of uncertainty, and

quantify and describe a substantial part of it. This approach would be suitable for application to more complex facilities or to those with large radioactive inventories.

Apart from the uncertainties in the numerical computation of PSA results, there are some other sources of uncertainties, which may include, but are not restricted to:

- incompleteness in the selection of initiating events and scenarios;
- incompleteness in recognizing dependencies of systems or system functions in complex facilities (including common cause);
- shortcomings in modelling process situations or time dependencies because of missing experience and/or information regarding the process under analysis;
- incompleteness regarding human behaviour, for example modelling the behaviour of an individual instead of a group of operators or vice versa;
- incompleteness in the evaluation of expert opinions;
- reliability of software/hardware of computer based functional control systems or operator support systems;
- shortcomings in the computer codes used in the PSA;
- false estimation of the general safety culture of the facility staff.

The impact of these uncertainties on the final results may be minimized through an iterative process of re-evaluation of the PSA modelling process. In the case of software used in performing the PSA, the use of verification and validation procedures may be advisable. An example of a validation procedure is given in Ref. [44].

6.3. Importance and sensitivity analyses (Task 26)

Importance analysis requires the determination of the importance of contributors to facility end states, fault sequence frequencies, system unavailabilities, and consequences. Importance measures aid in the interpretation of the results of the PSA.

The purpose of sensitivity analysis is twofold: (1) to determine the sensitivity of the facility end states to possible dependencies among component failures and among human errors, and (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. That is why sensitivity analysis may need attention for an NRNF.

The nature and extent of sensitivityy analyses will be driven by the needs of the PSA and the nature of the dominant fault conditions. Where the data used are very uncertain or unreliable, more extensive studies are advisable. Given the range of PSA applications to NRNFs, specific guidance cannot be provided. However, the extent of sensitivity analysis can be judged sufficient if the analyst is confident that the PSA results can be used for their intended purpose, e.g., that the risk measures can be reliably compared against risk criteria.

7. DOCUMENTATION

7.1. General discussion

The final procedural step presented in this report pertains to documentation and quality assurance. The discussion of these two important aspects of the PSA at the end of a set of

guidelines such as this by no means implies that these activities are to take place solely at the end of the PSA effort. As stated in the discussion of the previous tasks, documentation is a key aspect of the analysis and should be initiated concurrently with the analysis. To the extent possible, the same can be said of the quality assurance and the review process. Focused review efforts made during strategic points of the analysis can be most efficient. Of course, a portion of the documentation and review efforts must be drafted and performed near the end of the PSA effort. Once again, the task numbering follows sequentially from the tasks in the previous section.

7.2. Documentation (Task 27)

The nature of the PSA documentation that is developed depends on the objectives of the PSA. The overall objective of PSA documentation is to record the analysis basis (assumptions made, data and methods used, etc.) and the results (detailed analysis results, interpretation of results, etc.). The documentation enables a technical review of the analysis to be carried out.

In general, there are two key uses for the finalized PSA document. First, the PSA document can be used by the facility management to help establish good risk management practices. Thus, the results of the PSA can be used to help define the requirements for various elements of the facility safety programme including maintenance, training, operating procedures, safety inspections and audits, and management of change. Second, the documentation of the PSA process and its results can be used to demonstrate to facility management, regulators and the public that the risk associated with the facility is known, and, furthermore, that the facility is 'safe' to operate. That is, the documentation can provide assurance that the PSA was conducted using sound practices, and that the risk from operating the facility meets some specified (risk) criteria.

The PSA documentation should include not only the results of the assessment (e.g., logic diagrams showing potential accident sequences and safety controls used to prevent or mitigate accident consequences), but also other information related to the conduct of the PSA. The amount of information used and generated during the PSA process can be substantial. The process safety information alone can include many detailed drawings and diagrams as well as hundreds of pages of specifications, procedures, etc. In addition to the process safety information and the results of the PSA, the documentation of the PSA should include a description of the site, the facility, the processes that were analysed, the method that was used, the people who performed the analysis, the time frame during which it was performed, and any assumptions made. Several specific documentation requirements have been identified in previous sections of this document. Table XVI of Ref. [2] provides sample contents of typical documentation for a PSA study for an NPP. Reference [5] also provides guidance on type of documentation to be produced within a PSA for an NRNF. All documentation associated with the PSA process should be maintained by the facility's configuration management system to assure that it is representative of the current facility configuration. Thus, the conclusion that a facility is safe to operate is based on the current facility configuration. Also, keeping the PSA documentation current permits an accurate evaluation of the risks associated with any proposed changes to the facility.

The structure and format of the PSA documentation is dependent upon in the scope of the analysis. Documentation of the analysis of lower hazard facilities, where less depth of analysis is applied, can follow the guidance in Appendix I of Ref. [5]. Where considerably more information requires documentation, such as in the case of a detailed, quantitative PSA study of a high hazard or complex facility, the guidance in Ref. [2] is more applicable. The

recommendation in this case is that the PSA study be divided into three major parts: summary report, main report, and 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 nuclear safety specialists and which is adequate for high level review. If the PSA results are used to demonstrate compliance with regulatory requirements, the PSA documentation that is submitted for regulatory review will consist of the main report plus any additional information needed for the regulator to make a safety determination. The amount of detail that needs to be submitted depends on the nature of the review with a more comprehensive review requiring a higher level of detail. If the requisite detail is not submitted in the summary and main report, the regulatory reviewer may consider visiting the facility to see the internal PSA documentation in its entirety.

REFERENCES

[1] NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, Rep. WASH-1400-MR (NUREG-75/014), Washington, DC (1975).

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

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

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Series No. 35-G1, IAEA, Vienna (1994).

[6] NUCLEAR REGULATORY COMMISSION, Nuclear Fuel Cycle Facility Accident Analysis Handbook, Rep. NUREG/CR-6410, Washington, DC (1998).

[7] UNITED STATES DEPARTMENT OF ENERGY, Preparation Guide for US Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports, Rep. DOE-STD-3009-94, Washington, DC (1994).

[8] UNITED STATES DEPARTMENT OF ENERGY, Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Reports, Rep. DOE-STD-1027-92, Washington, DC (1992).

[9] AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, Guidelines for Hazard Evaluation Procedures, 2nd edn, ISBN 0-8169-0491, New York, NY (1992).

[10] AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, Guidelines for Chemical Process Quantitative Risk Analysis, ISBN 0-8169-0402-2, New York, NY (1989).

[11] HIRSCHBERG, S., SPIEKERMAN, G., DON, R., Project GaBE: Comprehensive Assessment of Energy Systems – Severe Accidents in the Energy Sector, Paul Scherrer Institut (PSI) Bericht Nr. 98-16, 1st edn, Villingen (1988).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Probabilistic Safety Assessment for Nuclear Installations With Large Inventory of Radioactive Material, IAEA-TECDOC-711, Vienna (1993).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of and Regulations for Nuclear Fuel Cycle Facilities, IAEA-TECDOC-722, IAEA, Vienna (2001).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas, IAEA-TECDOC-994, IAEA, Vienna (1998).

[15] KLETZ, T.A., HAZOP and HAZAZ — Identifying and Assessing Process Industry Hazards, The Institute of Chemical Engineers, 3d edn, London (1992).

[16] BROOKHAVEN NATIONAL LABORATORY, Probabilistic Safety Analysis: Procedures Guide, Rep. NUREG/CR-2815 BNL-NUREG-51559, Rev. 1 (2 volumes), United States Nuclear Regulatory Commission, Washington, DC (1985).

[17] NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Analysis: Procedures Guide, Rep. NUREG/CR-2300, Washington, DC (1983).

[18] DINSMORE, S. (Ed.), PRA: Uses and Techniques: a Nordic Perspective, Summary Rep. NKA Project SaeK-1, Nordic Liaison Committee for Atomic Energy (NKA), Risø National Laboratory, Roskilde (1985).
[19] NUCLEAR REGULATORY COMMISSION, Interim Reliability Evaluation Programme: Procedures Guide, Rep. NUREG/CR-2728, Washington, DC (1983).
[20] NUCLEAR REGULATORY COMMISSION, Fault Tree Handbook, Report NUREG-0492, Washington, DC (1981).
[21] ALDEMIR, T., SIU, N., MOSLEH, A., CACCIABUE, P.C., GOKTEPE, G. (Eds), Reliability and Safety Assessment of Dynamic Process Systems, Springer-Verlag, Berlin (1994).
[22] SIU, N., Risk Assessment for Dynamic Systems: An Overview, Reliability Engineering and System Safety, **43** 1 (1994) 43–73.
[23] NUCLEAR REGULATORY COMMISSION, A Technique for Human Error Analysis (ATHEANA), Rep. NUREG/CR-6350, Washington, DC (1996).
[24] NUCLEAR REGULATORY COMMISSION, Technical Basis and Implementation Guidelines for a Technique for Human Error Analysis (ATHEANA), Rep. NUREG-1624, Washington, DC (1998).
[25] KIRWAN, B., A Guide to Practical Human Reliability Assessment, Taylor & Francis, ISBN 0-7484-0052-4, London (1994).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probability Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10 Vienna (1996).
[27] NUCLEAR REGULATORY COMMISSION, Handbook of Human-Relability Analysis with Emphasis on Nuclear Power Plant Applications, Rep. NUREG/CR-1278, Washington, DC (1983).
[28] NUCLEAR REGULATORY COMMISSION, SLIM-MAUD: An Approach to Assessing Human Error Probabilities using Structured Expert Judgement, Rep. NUREG/CR-3518, Washington, DC (1984).
[29] WILLIAMS, J.C., A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance (Proc. 4th IEEE Conf. on Human Factors and Power Plants, Monterey, 1988), IEEE, New York (1988) 436–450.
[30] UEDA, Y., et al., Quantitative Study of Effect of Process Condition on Occurrence Frequency in Reprocessing Facility — Hydrogen Explosion in Plutonium Solution Vessel (Proc. Annual Mtg of the Atomic Energy Society of Japan, Ehime, Aomori 2000), Matsuyama, Tokyo (March 2000) (in Japanese).
[31] SCHAEFER H., Reliability Analysis of Repairable Safety Systems of a Reprocessing Plant Allowing for Tolerable System Downtime (Proc. RECOD 87, Int. Conf. on Nuclear Fuel Reprocessing and Waste Management. Paris, 1987) Vol. 3, Société Française d'Energie Nucléaire, Paris (1987).
[32] INSTITUTE OF NUCLEAR SAFETY/NUCLEAR POWER ENGINEERING CORPORATION, Annual Report about Development of Nuclear Facility Safety Analysis Code in Heisei 8, Rep. INS/S96-15, INS, Tokyo (1997) (in Japanese).
[33] INSTITUTE OF NUCLEAR SAFETY/NUCLEAR POWER ENGINEERING CORPORATION, Annual Report about Development of Nuclear Facility Safety Analysis Code in Heisei 9, Rep. INS/S97-10, INS, Tokyo (1998) (in Japanese).
[34] INSTITUTE OF NUCLEAR SAFETY/NUCLEAR POWER ENGINEERING CORPORATION, Annual Report about Development of Nuclear Facility Safety Analysis Code in Heisei 10, Rep. INS/S98-12, INS, Tokyo (1999) (in Japanese).

[35] ZENTNER, M.D., A Comparison of Reactor and Non-Reactor Risk Assessment Approaches, Rep. WHC-SA—1560 (Proc. of Probabilistic Safety Assessment International Topical Meeting (PSA), Clearwater Beach, 1993) Westinghouse Hanford Co., Richland, WA (1992).
[36] DEXTER, A.H., PERKINS, W.C., Component Failure Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant, DuPont de Nemours, Savannah River Lab., Rep. DP-1633, Aiken, SC (1982).
[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Models and Data Requirements for Human Reliability Analysis, IAEA-TECDOC-499, Vienna (1989).
[38] INTERNATIONAL COUNCIL ON RADIATION PROTECTION, Age-Dependent Doses to Members of the Public from Intake of Radionuclides: Part 5, Compilation of Ingestion and Inhalation Dose Coefficients, ICRP Publication 72, Annals of ICRP, Volume 26, Number 1, Pergamon Press, Oxford (1996).
[39] ECKERMAN, K.F., RYMAN, J.C., External Exposure to Radionuclides in Air, Water, and Soil, US EPA Federal Guidance Report No. 12, US Environmental Protection Agency, Washington, DC (1993).
[40] INTERNATIONAL COUNCIL ON RADIATION PROTECTION, Dose Coefficients for Intakes of Radionuclides by Workers, ICRP Publication 68, Annals of ICRP **24** 4, Pergamon Press, Oxford (1994).
[41] FULLWOOD, R.R., HALL, R.E., Probabilistic Risk Assessment in the Nuclear Power Industry: Fundamentals and Applications, Pergamon Press, Oxford (1988).
[42] NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Final Summary Report, Rep. NUREG/CR-1150, 3 Volumes, Washington, DC (1990).
[43] KAPLAN, S., Formalisms for Handling Phenomenological Uncertainties: The concepts of Probability, Frequency, Variability and Probability of Frequency, Nucl. Tech. **102** (1993) 137–142.
[44] SCHOTT, H., BERG, H.P., GOETZ, K., Qualification Procedure for Computer Codes to Perform Probabilistic Safety Analysis, in Safety and Reliability, SCHUELLER, G.I., KAFKA, P. (Eds), Balkema, Rotterdam (1999) 1549–1552.

Appendix I

TYPICAL DIFFERENCES BETWEEN REACTOR, CHEMICAL PROCESS AND NON-REACTOR NUCLEAR FACILITIES OF RELEVANCE TO PSA STUDIES

The qualitative differences between NPPs and NRNFs have to be considered when conducting PSA for such NRNFs. Whereas the reactor core of an NPP presents a very large inventory of radioactive material at high temperature, high pressure, and within a relatively small volume, an NRNF, generally, operates at near ambient pressure and temperature and with comparatively low inventories at each stage of the overall process. In nuclear waste repositories, the total nuclide inventory will progressively increase to a maximum over the operating period of the facility.

Usually in NRNFs there are long time scales involved in the development of accidents and, compared to reactors, less stringent process shutdown requirements are required to maintain the facility in a safe state. Such facilities also often differ from reactors with respect to the critical importance of ventilation systems in maintaining their safety — even under normal operation. This is because materials in these facilities are in direct contact with ventilating or off-gas systems. In general, the robustness of barriers between radioactive inventories and the operators as well as the environment differ strongly to those of reactor systems.

With fuel reprocessing or fuel fabrication facilities, the wide variety of processes and material states such as liquids, solutions, mixtures and powders must all be considered in a PSA. From this point of view, the safety features of NRNFs are often more similar to chemical process plants than those of reactors. In addition, criticality issues are likely to warrant more attention in NRNFs compared to NPPs.

A further comparison of relevant features of an NPP, a chemical process plant and an NRNF is presented below and in Table I.1.

— NPP:
  - Source of hazard is limited to the core (although significant inventories of irradiated fuel may be stored on site and off-gas inventories might be significant enough to be considered a hazard to on-site personnel).
  - There are only a relatively few basic design variants.
  - PSA methodology for NPP is relatively mature.

— Chemical Process Plant:
  - Sources of hazard are many, depend on type of plant, and are distributed through the process.
  - Fault sequences are more varied.
  - Hazard and accident scenarios have to be identified at first by qualitative analysis.

— NRNF (has both the characteristics of an NPP and a chemical process plant):
  - Hazardous inventories are generally in a non-energetic state.
  - Hazardous radioactive inventories are spread widely in the facility.
  - Inventories, safety functions and barriers are varied.

TABLE I.1. TYPICAL DIFFERENCES BETWEEN NPPs, CHEMICAL PROCESS PLANTS AND NRNFs

Feature	NPP	Chemical Process Plant	NRNF
Areas of hazardous sources and inventories	Localized at core and spent fuel pool. Standardized containment system. Cooling of residual heat. Criticality management.	Distributed in the process. Flowing through the process.	Consisting both of nuclear materials and chemical materials. Co-existence of NPP features and chemical plant features. Flowing through the process mainly handling materials in the facility.
Type of hazardous materials	Mainly nuclear materials.	Wide variety of materials dependent on the plant, e.g., oil, poisons, acids, explosions.	Fissile materials, nitric acid, hydrogen fluoride, solvents, process and radiolytic hydrogen, etc.
Physical forms of hazardous materials	The core is solid. Liquid, gas and dust (aerosol) of radioactive materials released to the environment in accident phase.	Wide variety of physical forms depend on the process, e.g., as solid, liquid, gas, slurry, powder.	All physical forms of fissile material and a wide variety of chemical materials. Immobilized radioactive materials.
Potential causes of accidents	Incidents related to the core and the safety system, initiated by internal or external events.	Agitator failure; Loading of the wrong amount of or wrong raw material into the reactor or storage tank; Accumulation of the reactant in the reactor; Too high temperature of the reactor; Operator failures.	Incidents related to safety function and barriers, fire, explosion, loss of ventilation, loss of barriers, transport failures.
Consequences of accidents	Core damage, failure of containment, radioactive release and radioactive exposure.	Wide variety, e.g., the number of casualties and time-scale of the contamination (both on-site and off-site), Releases of toxic gasses, Damage to the facility.	Possible radioactive release and exposure to personnel, public and environment.
Recommended PSA methodology	Plant specific quantitative risk analysis.	Initially, qualitative analysis for each plant. Based on the qualitative analysis, conduct quantitative analysis for areas of key hazard sources.	Hazard identification and screening. Evaluation of accident scenarios and failures of barriers. Combination of qualitative and quantitative analysis.

Appendix II

TYPICAL INITIATING EVENTS TO BE CONSIDERED IN PSA STUDIES FOR NON-REACTOR NUCLEAR FACILITIES

This appendix provides listings of initiating events that might be considered when performing PSA on NRNFs. The lists are presented in tables: each table pertaining to a different type of NRNF. The initiating event lists are not intended to be complete, nor necessarily applicable for each of the NRNFs — they are provided only as examples, and should be used only as guidance in deriving facility specific initiating event lists.

TABLE II.1. INITIATING EVENTS FOR NUCLEAR FUEL REPROCESSING FACILITIES

INCIDENT	INITIATING EVENT
Fuel receiving and storage	
Leakage of coolant from irradiated fuel cask	Cask damage in transit Valve failure
Cask inadvertently vented	Valve failure Erroneous instructions/procedural mistake
High temperature in cask primary coolant	Fuel cooling time too short Failure of secondary heat transfer system
Off-gas treatment	
Loss of off-gas header vacuum	Flow restriction/blockage Fan failure Loss of power Operating error
High radioactive particulate release to building ventilation filters	Damaged process ducts or filters Maintenance errors
Filter failure	Dust explosions In-cell fires Condensation on HEPA filters
Vitrification and high level vitrified waste storage	
High activity level in the storage pool water	Release from storage canisters Contamination from canisters to water
Contaminated canisters	Cracks in welds Canisters not properly decontaminated
Inadvertent criticality	Violation of operational procedures, Changes in the ambient atmosphere, e.g. increased humidity, etc.
Loss of cooling water and shielding	Pool leak Loss of heat exchanger/tower cooling Power outage
Solidification of intermediate level liquid waste	
Fissile material in feed	Transfer error in another facility Leaks in another facility
Uncontrolled reaction in mixer or product container	Chemical addition error in dry mix added to grout mixer Chemical addition error to feed

TABLE II.2. INITIATING EVENTS FOR FUEL FABRICATION FACILITIES

INCIDENT	INITIATING EVENT
Flow transient	Degradation of control function Single active component failure/Operator error
Fissile material density transient	Degradation of control function Single active component failure/Operator error
Solvent density transient	Degradation of control function Single active component failure/Operator error
Inventory transient	Single active component failure/Operator error Leakage from pipes/vessels
Uncontrolled changes in heating capability	Degradation of control function Single active component failure/Operator error
Uncontrolled process change	Leakage from pipes/vessels Intervential operator actions leading to deviation Loss of power supply Fire/explosion in plant
Disturbance of temperature regime	Degradation of caution function
Hydrogen burner extinguished in UF6 conversion unit	Operator error
Humification of output product	Operator error
Self-supported chain reaction	Increase of uranium concentration Violation of loading norms Increase of the product moisture Clog of gas-line Decrease of the unit temperature Extinguished hydrogen burner Depressurization of the filter Leakage of the cooling system

TABLE II.3. INITIATING EVENTS FOR DRY INTERIM SPENT FUEL STORAGE FACILITY

INCIDENT	INITIATING EVENT
Mechanical failure/radioactive release	Drop of load from crane (result of failure of crane or hoist). Fall of heavy body on the cask from crane as result of failure of building
Mechanical failure/radioactive release/ fire	Fall of the cask during transportation or manipulation as a result of collision (may be followed by fire)
Seal failure/radioactive release	Failure of sealing of the cask Loss of heat removal in underground storage

TABLE II.4. INITIATING EVENTS FOR RADIOACTIVE WASTE INSTALLATION

INCIDENT	INITIATING EVENT
Mechanical failure	Drop of load from crane (result of failure of hoist) onto container
Radioactive release from the cask	Cask failure due to overpressure
Radioactive release from tank	Leakage in the tank
Overexposure	Loss of shielding Cask failure
Radioactive release	Cask failure during transportation
Radioactive release	Overheated Cooling failure

Appendix III

NON-REACTOR NUCLEAR FACILITY PSA CASE STUDY — WASTE STORAGE FARM

This appendix presents an example of the development of an NRNF PSA to aid in understanding and applying the techniques reviewed in this publication.

III.1. INTRODUCTION

This study considers the safety of the high level liquid waste (HLLW) tanks in a waste storage farm. Although the study was not undertaken, and is not described in a way that follows rigidly the process described in the main report, most of the task elements have been addressed. The management and organizational elements (Tasks 1–8) are not described. More detail on the study may be obtained from Ref. [III.1]. The process is described in the following steps:

- system description (Tasks 9, 13, 14);
- initiating events (Tasks 10, 11, 15);
- accident sequence modelling and quantification (Tasks 16, 17, 19–21); and
- consequence assessment (Tasks 18, 22–25).

III.2. SYSTEM DESCRIPTION

The HLLW tank consists of three concentric structures: (first) an outer, reinforced tank designed to sustain induced loads from soil and seismicity; (secondly) a secondary, carbon-steel tank that lines the concrete tank and is designed to serve as a barrier to primary tank leaks; and (thirdly) a free-standing carbon-steel primary tank that rests on an insulating concrete pad within the secondary tank. The primary tank contains the waste material; the secondary tank, which is larger than the primary tank, encloses the primary tank to create a surrounding annular space. The annulus is ventilated and monitored constantly for evidence of primary tank leakage. The active induced-draft ventilation system for the tank has two completely separate subsystems: a primary tank ventilation system and an annulus ventilation system. The tank is connected to the two subsystems by manifolds, which maintain a slightly negative pressure within the tank and annulus. The ventilation subsystems have no redundancy; the ductwork is above-ground in some cases, and underground in others. The ductwork routes the ventilation air from the primary tank and annulus of each tank to the respective filter trains and exhaust fans.

III.3. INITIATING EVENTS

The first step in developing a risk model is to define a set of initiating events. For an accident sequence to occur, an event must first perturb the steady-state condition of a waste tank or its contents. Subsequent events may (or may not) result in a release of radionuclides or chemicals.

The primary objectives of the initiating event definition exercise are:

- to provide a comprehensive list of initiating events with adequate assurance that all possible events are taken into account;
- to account for unique tank design and operational features;

TABLE III.1. INITIATING EVENTS

EXAMPLE CAUSAL EVENTS	MLD BASIC EVENTS																
	Primary Tank Shell Breach	Secondary Tank Shell Breach	Tank Dome Failure	Annulus Vent Line Breach	Riser Breach	Primary Exhaust Vent Line Breach	Exhaust HEPA Filter Breach or Bypass	Vent. Drain Line Leak	Vent. Seal Pot Leak	Waste Transfer Event	Waste Transfer System Boundary Failure	Inadequate Primary Ventilation Flow	Inadequate Level Control	Criticality Event in Waste	Bound Flammable Gas Release	Flammable Gas Accumulation	Uncontrolled Waste Heatup
Drilling contact with tank	x	x															
Excavation contact with tank	x	x	x		x												
Tank thermal stress	x																
Tank liner corrosion	x																
Vehicle Overloads Dome			x														
Load dropped over tank			x	x	x	x											
Vehicle impact with above ground equip.				x	x	x	x	x	x								
Vent. duct corrosion				x													
Human error, equipment not restored after maintenance				x	x	x	x	x	x		x	x					
Vent. drain line corrosion								x	x								
Vent. drain line freezing								x									
Excessive moisture in vent system							x										
Ventilation exhaust filter blockage												x					
Ventilation inlet blockage												x					
Vent fan failure												x					
Loss of power to vent fan												x					
Loss of air supply to ALCs																	x
Dryout of waste																	x
Tank inundated by transfer spill			x										x				
Tank inundated by raw water leak			x										x				
Tank inundated by heavy precipitation			x										x				
New waste transfers from other facilities										x			x	x	x	x	x
Salt well transfers to collector tank										x				x	x		
Liquid transfers to 242-A evaporator										x			x	x	x	x	
Surry transfers from 242-A to DST storage										x			x	x	x	x	x
Radiolysis of water in waste																x	
Bound gas release	x	x	x	x	x	x	x	x	x			x				x	
Lightning strike on tank												x					
Seismic event	x	x	x	x	x	x	x	x	x		x	x					
Aircraft crash	x	x	x	x	x	x	x	x	x		x	x					
Range fire*												x					
High wind & dust storm*				x		x						x					
Volcanism*												x					
Dam break*			x										x				

TABLE III.2. INITIATING EVENT GROUPS

EXAMPLE CAUSAL EVENTS	HTF INITIATING EVENT GROUPS											
	Tank Shell Breach	Tank Dome Failure	Riser Breach or Vent Line Breach	Exhaust HEPA Filter Breach or Bypass	Vent. Drain System Leak	Waste Transfer Event	Inadequate Primary Ventilation Flow	Uncont. Waste Heatup	Flammable gas Accumulation	Bound Gas Release	Water Intrusion to Tank	External Events
Drilling contact with tank		x										
Excavation contact with tank		x										
Tank thermal stress	x											
Tank liner corrosion	x											
Vehicle Overloads Dome		x										
Load dropped over tank		x										
Vehicle impact with above ground equip.			x									
Vent. duct corrosion			x									
Human error, equipment not restored after maintenance			x									
Vent. drain line corrosion					x							
Vent. drain line freezing					x							
Excessive moisture in vent system				x								
Ventilation exhaust filter blockage							x					
Ventilation inlet blockage							x					
Vent fan failure							x					
Loss of power to vent fan							x					
Loss of air supply to ALCs								x				
Dryout of waste								x				
Tank inundated by transfer spill											x	
Tank inundated by raw water leak											x	
Tank inundated by heavy precipitation											x	
New waste transfers from other facilities						x						
Salt well transfers to collector tank						x						
Liquid transfers to 242-A evaporator						x						
Surry transfers from 242-A to DST storage						x						
Radiolysis of water in waste									x			
Bound gas release										x		
Lightning strike on tank							x					
Seismic event												x
Aircraft crash												x

- to provide a way of categorizing events into a set of sequences covering all the ways that the event may developed, and
- to group events that present similar threats to safety functions for quantification.

The concept of grouping initiating events by similarity of expected response is common to most PSA models and helps to limit the number of event sequence models that need to be developed. Given knowledge of the approximate frequency of the initiating events and the relative effect of these events on the tank, it is possible and desirable to group and screen initiating events to simplify the quantification of risk without introducing large errors into the risk estimates.

The individual initiating events listed in Table III.1 are put into initiating event groups in Table III.2. Different individual events that affect the tank in a similar way are grouped together. Where an event could be applied to multiple groups, the event has been assigned to the more severe initiator group. This grouping results in a one to one correspondence between an individual event and an initiating event group.

A master logic diagram (MLD) was used to identify the potential initiating events. A MLD is similar to a fault tree and provides a deductive approach for directly answering the question: "how can a significant release of radioactivity, chemicals, or toxic gas occur?" This technique is one of the "deductive" tools identified in Ref. [2] of the main report. The first page of this study's MLD is depicted in Fig. III.1. A key objective of developing the MLD is to identify all possible types and sources of the hazardous materials and pathways by which the top event can be satisfied down to a level of detail at which all important safety functions and barriers have been taken into account. When this is accomplished, specific causal events that can threaten a safety barrier or function can be listed.

Many of the initiator events shown at the bottom of the MLD may be subdivided to reveal more specific causal events. Table III.1 is a list of events that could threaten the safety barriers of functions shown at the bottom of the MLD. The events listed also are matrixed against the MLD initiator events to help identify common cause initiators that can threaten multiple safety barriers or functions simultaneously.

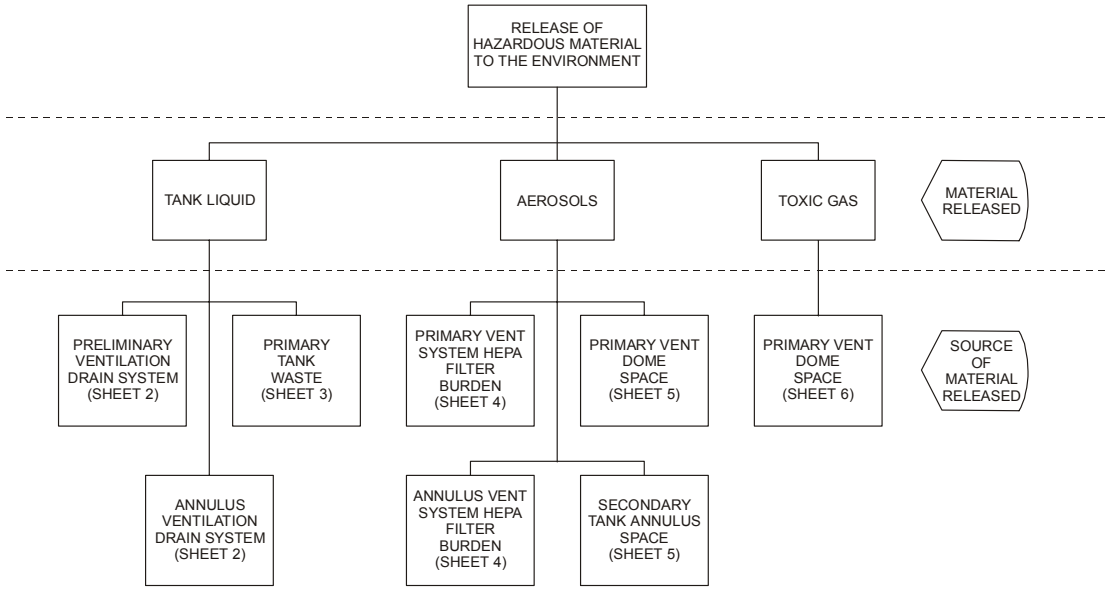

FIG.III.1. Top of master logic diagram for HLLW tanks.

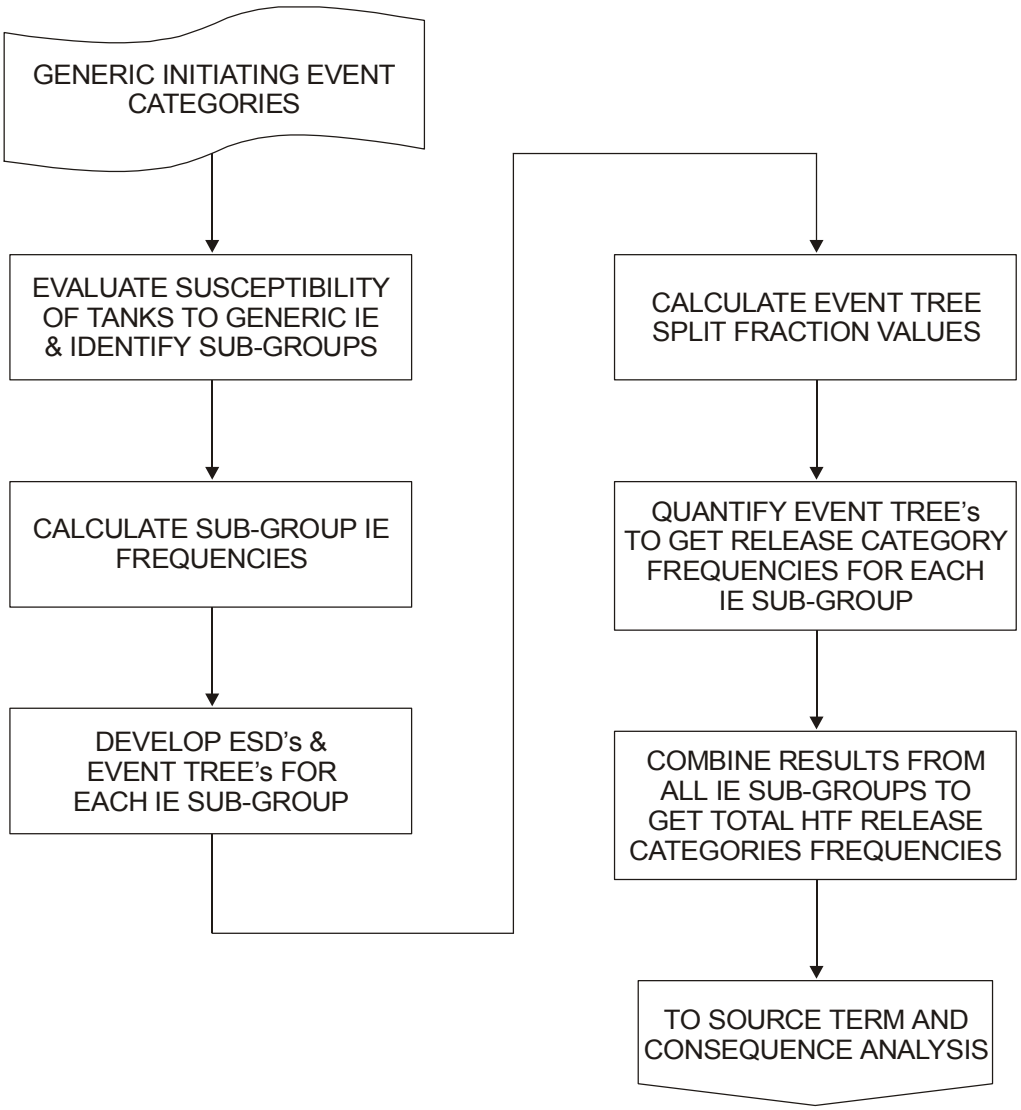

FIG. III.2. Accident sequence modelling steps.

III.4. ACCIDENT SEQUENCE MODELLING AND QUANTIFICATION

The accident sequence model serves two primary purposes: to document the PSA team's understanding of how radionuclide and/or toxic gas releases from the facility could occur and to create a logic model describing the potential release scenarios that can be used to quantify the likelihood of releases. The general approach used to develop accident-sequence models is shown in Fig. III.2.

Generic initiating event groups that had the potential to lead to material releases from one or more tanks were identified in the initiating events section. The accident sequence modelling process began by examining each generic initiator to identify any characteristics of the tank or waste material that could influence the assessment of the frequency of occurrence of radioactive releases.

Event sequence diagrams (ESDs) and event trees were developed for each initiator family. The ESDs describe and document the subsequent system responses, phenomenological events, and mitigating actions that can occur in response to the initiator. The ESDs can also specify the accident sequence time lines and thereby the most appropriate release category describing the end state of each sequence. The release categories defined for this study are presented in Table III.3. To quantify the accident sequence frequencies for each initiator, event trees corresponding to the ESDs were developed and quantified. The results represent the total frequency per year of each release category for each initiator.

The frequencies of accident sequences were determined by combining initiating event frequency estimates with the branch point probabilities, or split fractions, for the occurrence of each event on the event tree paths. The quantification of the branch-point probabilities used a combination of historical operating databases and occurrence reports, generic component/system failure data.

III.5. CONSEQUENCE ASSESSMENT

The consequence analysis provides estimates of radiological health risks for both co-located workers and off-site residents via the airborne pathway and, for off-site residents only for the ground-water pathway. Details of the source term/dose modelling are shown in Fig. III.3.

The atmospheric dispersion of released aerosols was calculated with a gaussian plume model code that tracks the dispersion of particles. To estimate the range of potential doses to an individual, a cumulative probability distribution of dose values was constructed by using the joint-frequency meteorological data for the site.

Inhalation dose factors were calculated based on values of committed dose equivalent factor per unit intake given in ICRP publications. Particle size dependent and solubility class dependent DOS factors for various radionuclides were used to calculate appropriate long-term off-site dose (50 years) resulting from continuous ingestion of contaminated food and water.

Airborne releases were characterized by three frames: short term energetic (occurring in less than 2 hours), short term (occurring in less than 8 hours), and long term (occurring from 8 hours to 60 days). The long term, ground-level releases were considered only in the evaluation of the off-site population doses because the on-site personnel would not be permitted to return if there was a release lasting for days.

To obtain the maximum individual doses corresponding to the various release quantities, it was necessary to obtain the product of the appropriate release quantities.

III.6. RESULTS

The final results of the PSA for this study are the unconditional risk curves. Risk curves present the relationship between the frequency of occurrence of radionuclide release events and the level of damage sustained as the result of the release; they are presented as complementary cumulative distribution functions (CCDFs) for total health and economic consequences and for those release categories that contribute significantly to these risk indices. In addition, an uncertainty quantification was performed to generate risk bands (i.e., percentile curves) for the total unconditional health effects for both on-site and off-site receptors.

TABLE III.3. PSA RELEASE CATEGORIES

RELEASE PATHWAY		RADIONUCLIDE CONTENT	ENERGY OF RELEASE	RELEASE CATEGORY CODE
	Unfiltered release	Very low	Low	BPL
	Unfiltered release	Low (Ageing waste)	Low	BPH
	HEPA breached	Low	Low	HEPAL
	HEPA breached	High	Low (H_2 burn)	HEPAH
To Atmosphere	Dome collapsed	High (101-SY waste)	H_2 burn	DCH
	Dome collapsed	High (Wet waste)	High (Aircrash & fire)	DCVH
	Dome collapsed	High (Dry, Inert waste)	High (Aircrash & fire)	DCVHI
	Dome collapsed	High (Dry, FECN waste)	High (Aircrash & fire)	DCVHF
	Dome collapsed	High (Organic waste)	High (Aircrash & fire)	DCVHO
	Subterranean leak	Small	N/A	SLK
To Ground	Subterranean leak	Large, SST	N/A	LLKSST
	Subterranean leak	Large, DST	N/A	LLKDST
	Surface spill	Small	N/A	SSP
	Surface spill	Large	N/A	LSP
	Spray leak	Small	Low	SSPRY
	Spray leak	Large	Low	LSPRY
To Atmosphere	Dome collapse + Subterranean leak	High	Moderate (H_2 burn)	DCLLK
and Ground	Dome collapse + Subterranean leak	High (C-103 waste only)	High (H_2 burn & fire)	DCHORG
	Dome collapse + Subterranean leak	4 tanks	Low (Seismic event)	DCL4
	Dome collapse + Subterranean leak	12 tanks	Low (Seismic event)	DCL12
	Dome collapse + Subterranean leak	45 tanks	Low (Seismic event)	DCL45
	Dome collapse + Subterranean leak	122 tanks	Low (Seismic event)	DCL122

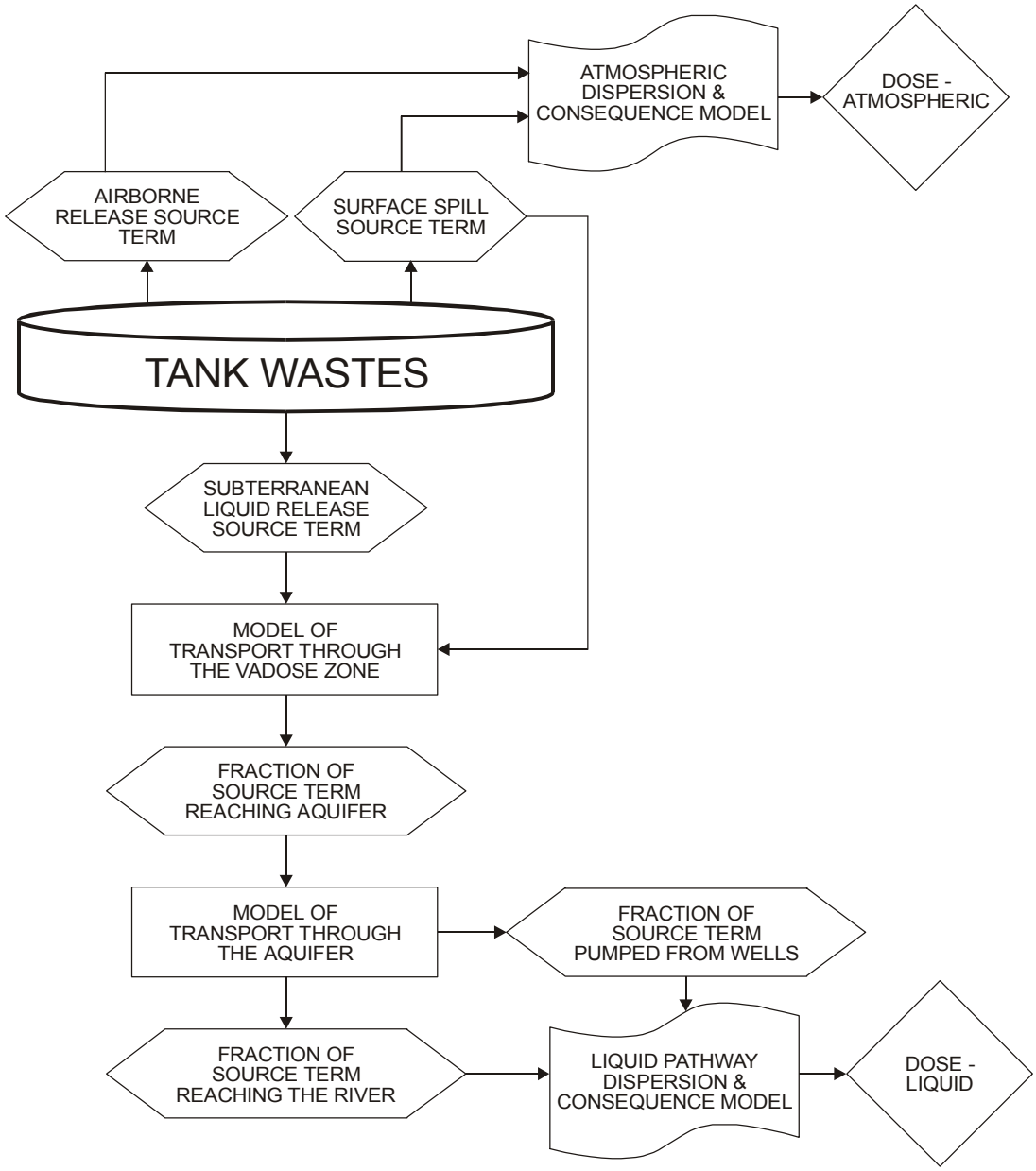

FIG. III.3. Source term and consequence model assessment.

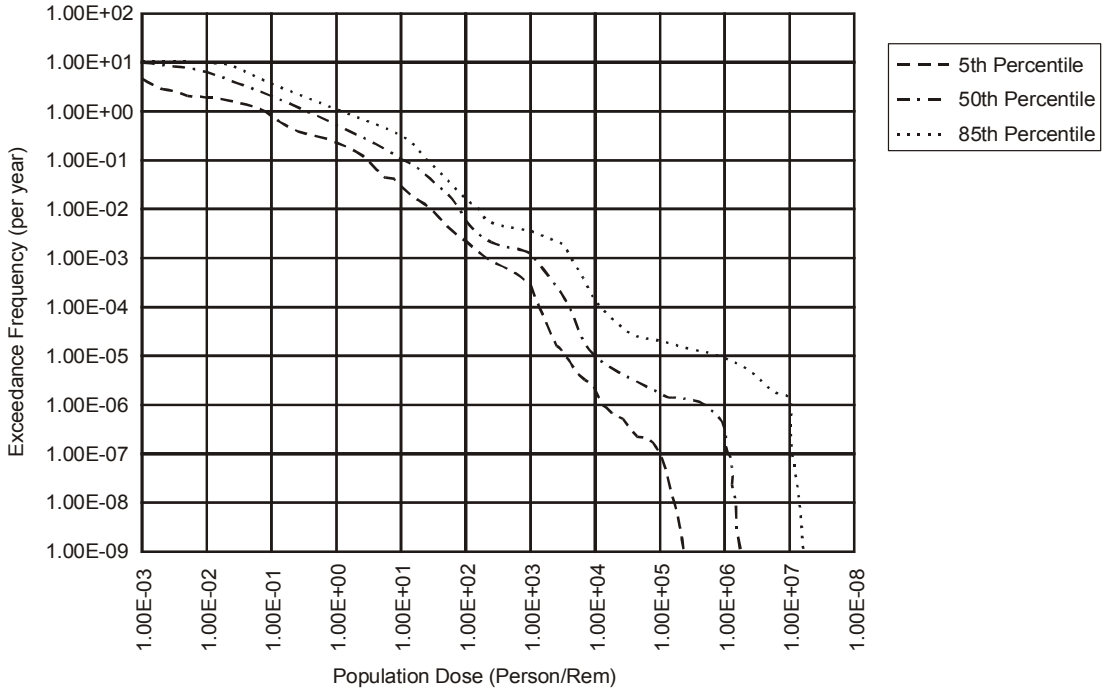

FIG.III.4. Off-site total unconditional consequences for airborne releases.

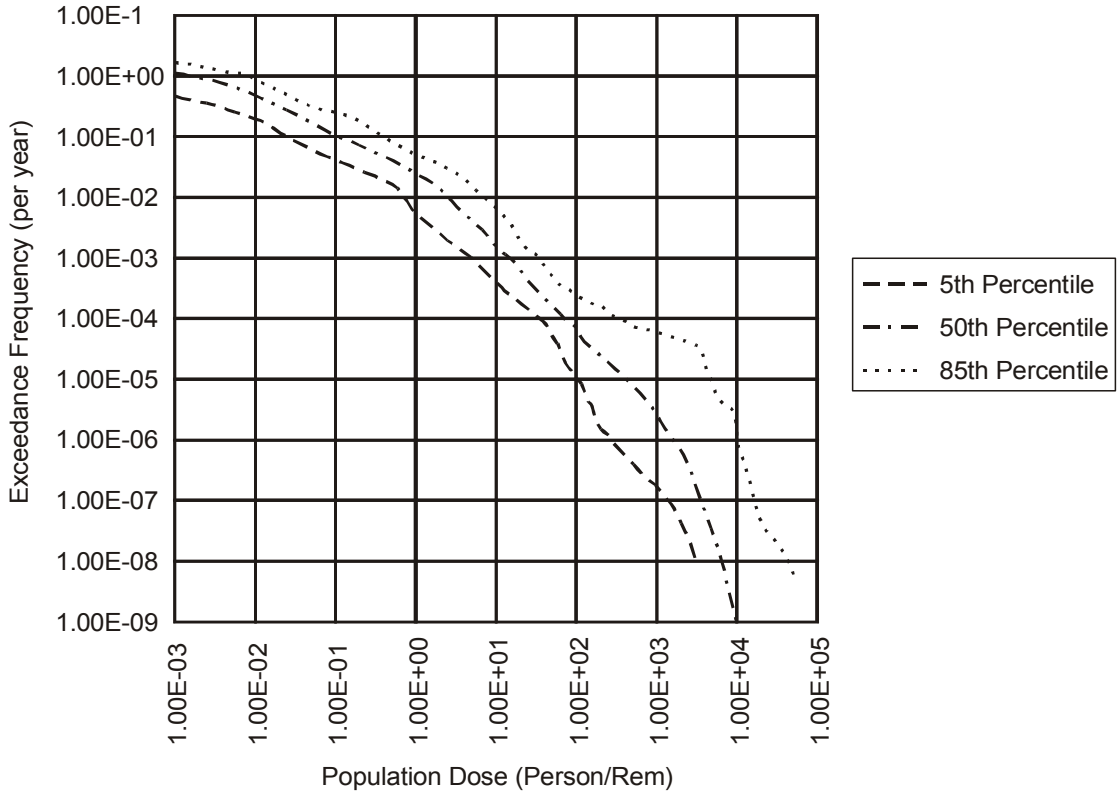

FIG.III.5. On-site total unconditional consequences for airborne releases.

The CCDFs for total off-site and on-site risk of airborne release were calculated by summing the appropriate probability distributions for exceeding frequencies at corresponding damage levels for all contributing release categories. The 5th, 50th, and 85th percentile curves and mean risk curves were calculated for total off-site and total on-site consequences. Figure III.4 shows the 5^{th}, 50^{th}, and 85^{th} percentile total off-site consequence curves. The 5^{th}, 50^{th}, and 85^{th} percentile total on-site consequence curves are presented in Fig. III.5.

REFERENCE TO APPENDIX III

[III.1] SULLIVAN, L.H., et al., Probabilistic Safety Assessment for High-Level Waste Tanks at Hanford, LA-UR-96-3912, Los Alamos National Laboratory, Los Alamos, NM (1996).

Appendix IV

PROBABILISTIC SAFETY CRITERIA FOR NON-REACTOR NUCLEAR FACILITIES

The objectives of some PSAs can include comparing the risk profile of the subject facility (defined by accident probabilities and related consequences) to defined quantitative risk criteria in order to decide whether the overall facility risk is acceptable.

There is a variety of risk acceptance criteria proposed or in use in different countries. The following sections summarize some of the practices used. Their presentation in this document is not intended to indicate their suitability for any purpose. They are presented for illustrative purposes only, and caution should be exercised when comparing criteria for different countries/organizations, since their exact interpretation will be subject to specific rules and requirements.

IV.1. CANADA

In Canada, safety criteria and licensing criteria proposed for small reactors [IV.1] have also been applied to non-reactor nuclear facilities.

The criterion is divided into two portions: individual dose criterion, and collective dose criterion, as given in the tables below. Each criterion is defined by three frequency ranges, and for each range, there is a dose band spanning approximately a factor of ten in dose. Predicted doses below the band are applied as 'design targets' and would normally be considered acceptable, while those above the band are applied as 'safety goals' and would normally be considered unacceptable. Predicted doses within the band require justification as to why they cannot be reduced.

Dose criterion for the most exposed individual

Effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
0.1 to 0.5	3×10^{-1}	3×10^{-2}
0.5 to 5.0	3×10^{-2}	3×10^{-4}
5 to 100	10^{-4}	10^{-6}

Collective dose criterion

Effective dose (Person-Sv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
0.1 to 1.0	3×10^{-1}	3×10^{-2}
1.0 to 10	3×10^{-2}	3×10^{-4}
10 to 100	10^{-4}	10^{-6}

Note: these criteria are different from those used for CANDU reactors.

IV.2. FRANCE

In a reprocessing plant design study in France, an acceptability graph was used in applying a probabilistic approach [IV.2]. The acceptability graph gives the correlation of probabilities and consequences.

In the acceptability graph, situations are divided into five frequency categories.

The first category covers the common operating incidents, with a frequency of greater than 10^{-1} per year. They are classified as normal operation. The release limit of the annual liquid and gaseous radioactive waste correspond to an irradiation of the population far lower (by a factor of around 100) than the regulatory limit of 5 mSv per year.

Categories 2 to 5 are defined in the following table. Category 5 events are extremely low frequency events that correspond to 'beyond design basis' accidents for an NPP and should not pose bigger risks than those posed by PWRs.

Category	Maximum effective dose (mSv)	Total predicted frequency (per year)	
		Upper limit	Lower limit
1	<0.05	Normal operation (>10^{-1})	
2	<0.5	10^{-1}	10^{-3}
3	<5	10^{-3}	10^{-5}
4	<150	10^{-5}	10^{-7}
5		Lower than 10^{-7}	

This approach is not of a regulatory nature but has been judged an acceptable practice by the French safety authorities.

IV.3. GERMANY

In Germany, protection from radiation exposure, i.e., maximum exposure limits, have been laid down in the Radiation Protection Ordinance [IV.3].

It is generally accepted that incidents occurring with a frequency from 1 to 10^{-2} per year fall into a range covering the normal running of a facility. Hazardous incidents are defined as those occurring with a frequency between 10^{-2} to 10^{-5} per year. Accidents that occur with a frequency of <10^{-5} per year are considered to belong to a class of accidents that form the remaining small risk of the facility.

From this, a probabilistic safety criterion for an individual member of the public has been derived, as given in the table below:

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
<1.5	1	10^{-2}
<50	10^{-2}	10^{-5}
>50	Less than 10^{-5}	

IV.4. INTERNATIONAL COMMISSION ON RADIATION PROTECTION (ICRP)

The ICRP has proposed radiation safety considerations as listed in the table below [IV.4]. From the ICRP point of view, these are intended to illustrate the type of constraints that might be imposed based on experience, and taking into account the benefits derived from the particular practice. They might also be imposed as tentative constraints in the absence of operating experience, subject to revision as experience is gained. In such cases, the constraints may be regarded as upper bounds for selecting the desired performance objectives, e.g., in the design of safety systems.

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
< 50	10^{-1}	10^{-2}
1–500	10^{-2}	10^{-5}
200–5000	10^{-5}	10^{-6}
> 2000	Less than 10^{-6}	

These constraints refer to potential exposure of an individual, and are consistent with risk criteria as specified by the Commission for Solid Waste Disposal.

IV.5. SOUTH AFRICA

In South Africa, the fundamental safety criteria are given in a licensing guide [IV.5]. The following summarizes the fundamental safety criteria.

Normal operation, classified as Category A, includes exposures resulting form minor mishaps and misjudgements in operations, maintenance and decommissioning. Events that could give rise to facility damage leading to radiation hazards to facility personnel and members of the public are classified as Category B and occur with a frequency between 10^{-2} and 10^{-6} per year.

Risk to the public

The safety criterion for a member of the public is given in the following table:

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
0.25	1	$>10^{-2}$
50	10^{-2}	10^{-6}

Risk to facility personnel

The safety criterion for facility personnel is given in the following table:

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
20	1	$>10^{-2}$
500	10^{-2}	10^{-6}

Note: in addition to the above stated criteria, the facilities must also meet annual fatality risk criteria.

IV.6. SWITZERLAND

In Switzerland, a tentative probabilistic risk criterion has been established for nuclear waste repositories [IV.6]. For an individual member of the public, this risk criterion is given in the following table.

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	Upper limit	Lower limit
<0.2	10^{-1}	10^{-2}
<1	10^{-2}	10^{-4}
<100	10^{-4}	10^{-6}
>100	Less than 10^{-6}	

IV.7. UNITED KINGDOM

In the UK, safety assessment principles for nuclear plants (SAPs) have been published by the Health and Safety Executive for the regulation of nuclear facilities [IV.7]. The following summarizes the particular SAPs relevant to PSA criteria for NRNFs.

Risk to the public

The total predicted frequencies of accidents that would give doses to a person outside the site should be less than the values given in the following table.

Maximum effective dose (mSv)	Total predicted frequency (per year)	
	BSL	BSO
0.1–1	1	10^{-2}
1–10	10^{-1}	10^{-3}
10–100	10^{-2}	10^{-4}
100–1000	10^{-3}	10^{-5}
>1000	10^{-4}	10^{-6}

BSL = Basic safety limit
BSO = Basic safety objective

A subsidiary aim should be that no single class of accident contribute more than about one tenth of the total frequency in any dose band, to avoid placing excessive reliance on particular features of the plant or on particular assumptions in the analysis.

Risk to workers

The total predicted individual risk of death (early or delayed) to any worker on the plant attributable to doses of radiation from accidents should be less than:

Basic safety limit: 10^{-4} per year
Basic safety objective: 10^{-6} per year

It is recognized that calculation of individual risk to workers may be difficult and hence only a broad estimate will normally be required, sufficient to show that the BSL is very unlikely to be exceeded and the ALARP aim has been appropriately applied. This principle is not intended to apply to personnel returning to perform actions after an accident.

Large release criterion

The total predicted frequency of accidents on the plant with the potential to give a release to the environment of more than:

- 10 000 TBq of iodine-131, or
- 200 TBq of caesium-137

Quantities of any other isotope or mixture of isotopes which would lead to similar consequences to either of these should be less than:

Basic safety limit:	10^{-5} per year
Basic safety objective:	10^{-7} per year

Plant damage criterion

The total predicted frequency with which the plant suffers damage and a significant quantity of radioactive material is permitted to escape from its designed point of residence or confinement, in circumstances which pose a threat to the integrity of the next physical barrier to its release, should be less than:

Basic safety limit:	10^{-4} per year
Basic safety objective:	10^{-6} per year

Such plant damage is interpreted as a degraded core in the case of a reactor. For other plant, it would include a major breach of vessel pipework, for example, together with the potential for events such as fire, explosion, or aggressive chemical attack which might lead to degradation of the containing cell or its ventilation/filtration system (even though there may be a safety system provided to prevent such degradation).

Criticality incidents

The total predicted frequency of an accidental criticality excursion on an NRNF should be less than:

Basic safety limit:	10^{-3} per year
Basic safety objective:	10^{-4} per year

This principle is also applied to facilities handling or storing fissile material outside the reactor core on a nuclear power station.

IV.8. COMPARISON OF SAFETY CRITERIA

A graphical comparison of the safety criteria of the ICRP, the UK, Switzerland and Germany is given in Fig. IV.1.

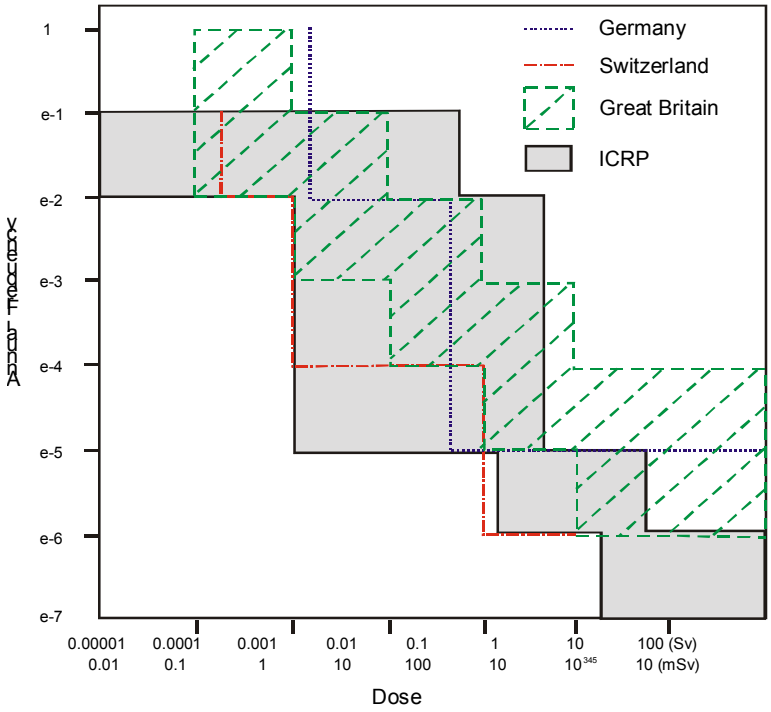

FIG. IV.1. Comparison of safety criteria (risk based) for nuclear installations.

REFERENCES TO APPENDIX IV

[IV.1] ERNST, P.C., FRENCH, P.M., AXFORD, D.J., SNELL, V.G., Development of Small Reactor Safety Criteria in Canada, (Proc. Int. Symp. on Research Reactor Safety Operations And Modifications, Chalk River, ON, 1989) IAEA-SM-310/93, Atomic Energy of Canada Ltd., Chalk River Nuclear Labs.; Chalk River, ON, International Atomic Energy Agency, Vienna (1990) 1177–1194.

[IV.2] MERCIER, J.P., BONNEVAL, F., WEBER, M., Application of the Probabilistic Approach to the UP3-A Reprocessing Plant, in Use of Probabilistic Safety Assessment for Nuclear Installations With Large Inventory of Radioactive Material, IAEA-TECDOC-711, Vienna (1993) 95.

[IV.3] BUNDESGESETZBLATT, Bekanntmachung der Neufassung der Strahlenschutz-verordnung vom 30. Juni 1989, Teil 1, Z 5702 A, Ausgegeben zu Bonn am 12. Juli 1989, Nr. 34, paragraphs 28 and 45.

[IV.4] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Protection from Potential Exposure: A Conceptual Framework - A Report of a Task Group of Committee 4 of the International Commission on Radiological Protection, ICRP Publication 64, Pergamon Press, Oxford (1993).

[IV.5] COUNCIL FOR NUCLEAR SAFETY, Licencing Guide LG-1037, Licensing Requirement for Pebble Bed for Modular Reactor, Hennopsmeer (1999).

[IV.6] HAUPTABTEILUNG FÜR DIE SICHERHEIT DER KERNANLAGEN, Bau, Betrieb und Verschluß eines Endlagers für radioaktive Abfälle, Rep. HSK-R-10/d, Juli 1994, 2. Entwurf, Villigen.

[IV.7] HEALTH AND SAFETY EXECUTIVE, Safety Assessment Principles for Nuclear Plants, H.M. Stationery Office, London (1992).

ABBREVIATIONS

ALARA	as low as reasonably achievable
ALARP	as low as reasonably practicable
ATHEANA	a technique for human error analysis
BSL	basic safety limit
BSO	basic safety objective
CANDU	Canada deuterium–uranium (reactor)
CCDF	complementary cumulative distribution function
DF	decontamination factor
ET	event tree
ETA	event tree analysis
ESD	event sequence diagram
FMEA	failure modes and effects analysis
FT	fault tree
FTA	fault tree analysis
HAZOPS	hazard and operability study
HEART	human error assessment and reduction technique
HEPA	high efficiency particulate air
HLLW	high level liquid waste
HRA	human reliability analysis
HVAC	heating ventilation and air conditioning
IE	initiating event
MLD	master logic diagram
NPP	nuclear power plant
NRNF	non-reactor nuclear facility
PSA	probabilistic safety assessment
PWR	pressurized water reactor
QA	quality assurance
RF	release fraction
SAP	safety assessment principle
SLIM-MAUD	success likelihood index model
TA	task analysis
THERP	technique for human error rate prediction

CONTRIBUTORS TO DRAFTING AND REVIEW

Adrian, H.	Institute for Safety Technology (ISTec) GmbH, Germany
Audet, M.C.	Atomic Energy of Canada Limited (AECL), Chalk River Laboratories, Canada
Benito, M.	Iberdrola Ingeniería Consultoría, Spain
Damon, D.R.	Office of Nuclear Material Safety and Safeguards, United States of America
Drake, S.	British Nuclear Fuel plc, United Kingdom
Ferjencik, M.	Czech Republic
Ford, P.J.	United Kingdom Atomic Energy Authority, United Kingdom
Giannone, B.	Agenzia Nazionale per la Protezione Dell'Ambiente, Italy
Gibson, I.K.	Health and Safety Executive, United Kingdom
Groche, K.	Advanced Nuclear Fuels GmbH, Germany
Grozovosky, G.	Gosatomnadzor of Russia, Russian Federation
Johnson, D. H.	EQE International, Incorporated, PLG Risk and Performance Engineering, United States of America
Hugron, R.	Department of National Defence, Canada
Kornfeld, C.	Nuclear Research Centre Negev, Israel
Kusumo, H.	Nuclear Energy Control Board, Indonesia
Lee, C.-J.	Korea Institute of Nuclear Safety, Republic of Korea
Lim, H.-K.	Korea Power Engineering Co., Republic of Korea
Mercier, S.	Technicatome, France
Milstein, R.	US Nuclear Regulatory Commission, United States of America
Morozov, V.	Atomenergoproekt, Russian Federation
Nojiri, I.	Tokai Reprocessing Center, Japan
Pather, T.	National Nuclear Regulator, South Africa
Ranguelova, V.	International Atomic Energy Agency

Reinhardt, C.	Urenco Deutschland GmbH, Germany
Rogers, P.	Rolls-Royce plc, United Kingdom
Schuller, J.	NRG Arnhem, Netherlands
Schäfer, H.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH (GRS), Germany
Suprawhardana, S.	Nuclear Energy Control Board (BAPETEN), Indonesia
Tjahyani, D.T.S.	Indonesia National Nuclear Energy Agency, Indonesia
Ueda, Y.	Nuclear Power Engineering Corporation, Japan
Vazquez, M.T.	Consejo de de Seguridad Nuclear, Spain
Watanabe, N.	Japan Atomic Energy Research Institute, Japan
Xue Xiaogang	China Institute of Atomic Energy, China
Yousefpour, F.	National Nuclear Safety Department (NNSD), Atomic Energy Organization of Iran, Islamic Republic of Iran
Zambardi, F.	Agenzia Nazionale per la Protezione dell'Ambiente, Italy