10 Sept 2020

IAEA SAFETY STANDARDS

for protecting people and the environment

STATUS: Step 7

First review of the draft publication by the review Committee(s)

Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants

DRAFT SPECIFIC SAFETY GUIDE

DS523

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [1], establishes principles to ensure the protection of workers, the public and the environment, now and in the future, from the harmful effects of ionizing radiation. These principles emphasize the need to assess and control the inherent risk. In particular, para. 3.22 of SF-1 [1] on optimization of protection states:

> "To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities."

1.2. Several IAEA Safety Requirements publications establish more specific requirements for risk assessment for nuclear power plants. Requirement 42 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [2] states:

> "A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed."

Furthermore, para. 5.76 of SSR-2/1 (Rev. 1) [2] states:

> "The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to:
>
> (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;
> (b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;
> (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified."

Thus, probabilistic safety assessment (PSA) is considered to be an important tool for analysis for ensuring the safety of a nuclear power plant in relation to potential initiating events that can be caused by random component failure and human error, as well as internal and external hazards.

1.3. Paragraph 4.13 of IAEA Safety Standards Series No. GSR Part 4 (Rev.1), Safety Assessment for Facilities and Activities [3] states:

> "The safety assessment shall include a safety analysis, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety by means of deterministic and also probabilistic methods."

Paragraph 4.55 of GSR Part 4 (Rev.1) [3] states:

> "The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity, and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined."

Thus, a comprehensive PSA is required to investigate the safety of a nuclear power plant thoroughly.

1.4. PSA has been shown to provide important safety insights in addition to those provided by deterministic analysis. PSA provides a methodological approach ~~to~~ for identifying accident sequences that can follow from a broad range of initiating events and it includes a systematic and realistic determination of accident frequencies and consequences. In international practice, three levels of PSA are generally recognized:

(1) In Level 1 PSA, the design and operation of the plant are analysed in order to identify the sequences of events that can lead to core and/or fuel damage and the corresponding core and/or fuel damage ~~frequency~~ frequencies ~~is~~ are estimated[1] ~~(or fuel damage and fuel damage frequency, when spent fuel pool is also considered – see Sections 10 and 12)~~.[2] Level 1 PSA provides insights into the strengths and weaknesses of SSCs important to safety and procedures in place or envisaged as preventing core and/or fuel damage.

(2) In Level 2 PSA, the chronological progression of core and/or fuel damage sequences identified in Level 1 PSA ~~is~~ are evaluated, including a quantitative assessment of phenomena arising from severe damage to reactor fuel. Level 2 PSA identifies ways in which associated releases of radioactive material from fuel can result in releases to the environment. It also estimates the frequencies~~y, magnitude and~~ as well as other relevant characteristics of the releases of ~~radioactive~~ radionuclides ~~material~~ to the environment. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures and the physical barriers to the release of radioactive material to the environment (e.g. a containment building) [4].

(3) In Level 3 PSA, public health and other societal consequences are estimated, such as the contamination of land or food from the accident sequences that lead to a release of radioactivity to the environment.

1.5. Level 1 PSA, Level 2 PSA and Level 3 PSA are sequential analyses, where the results of each assessment usually serve as a basis for the PSA at the next level. Level 1 PSA provides insights into design weaknesses and into ways of preventing accidents leading to core and/or fuel damage, which might be the precursor of accidents leading to major releases of radioactive material with potential consequences for human health and the environment. Level 2 PSA provides additional insights into the relative importance of accident sequences leading to core and/or fuel damage in terms of the severity of the releases of radioactive material they might cause, and insights into weaknesses in measures for the mitigation and management of severe accidents and ways of improving them [4]. Finally, Level 3 PSA provides insights into the relative importance of accident prevention and mitigation measures, expressed in terms of

[1] Sections 5 to 9 focuses only on the reactor core, therefore in these sections the term "core damage" is used (sometimes when applicable mentioning fuel damage specifically, e.g. core or fuel damage). Fuel damage considerations in the context of spent fuel pool analysis are provided in Sections 10 and 12)

[2] ~~Sections 5 to 9 focuses only on the core, therefore in these sections the term "core damage" is used (sometimes when applicable mentioning fuel damage specifically, e.g. core or fuel damage).~~

adverse consequences for the health of both plant workers and the public, and the contamination of land, air, water and foodstuffs. In addition, Level 3 PSA provides insights into the relative effectiveness of aspects of accident management relating to emergency preparedness and response.

1.6. This Safety Guide was prepared on the basis of a systematic review of relevant publications, including Refs [1–3], current and ongoing revisions of other Safety Guides [4-7], an International Nuclear Safety Group (INSAG) reports [8,9] and other publications that address the safety of nuclear power plants.

1.7. This Safety Guide replaces IAEA Safety Standards Series No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants[3]~~, which it supersedes~~.

OBJECTIVE

1.8. The objective of this Safety Guide is to provide recommendations for meeting the requirements of GSR Part 4 [3] in relation to performing or managing a Level 1 PSA project for a nuclear power plant and using it to support its safe design and operation. This Safety Guide is applicable to existing and new nuclear power plants. The recommendations provided in this Safety Guide aim to promote technical consistency among Level 1 PSA studies in order to provide reliable support for applications of PSA and risk informed decision making. A further aim of this Safety Guide is to recommend a standard framework that can facilitate a regulatory review or an external peer review of a Level 1 PSA and its various applications.

1.9. This Safety Guide also provides a consistent, reliable means of ensuring the effective fulfilment of obligations under Article 14 of the Convention on Nuclear Safety [10].

1.10. The recommendations presented in this Safety Guide are based on internationally recognized good practices. However, it is not intended to pre-empt the use of equivalent new or alternative methods. On the contrary, the use of any method that achieves the objectives of Level 1 PSA is encouraged. However, the framework for PSA outlined in this Safety Guide is expected to apply for the foreseeable future.

SCOPE

1.11. This Safety Guide addresses the necessary technical features of a Level 1 PSA and applications for nuclear power plants (both operating and new plants), on the basis of internationally recognized good practices. Level 1 PSAs have now been carried out for most nuclear power plants worldwide. ~~In recent years, a trend has emerged for Level 2 PSAs or limited Level 2 PSAs for nuclear power plants (e.g. Level 2 PSAs in which the large early release frequency is estimated) [4], as well as in some Member States it is extended to limited assessment of the doses (e.g. limited Level 3 PSA). In addition, Level 3 PSAs have been carried out in several States.~~ The scope of a Level 1 PSA addressed in this Safety Guide includes all operating states of the plant (i.e. at power and shutdown) and all potential initiating events and potential hazards, namely: (a) internal initiating events caused by random component failures and human error, (b) internal hazards (e.g. internal fires and floods, explosions, turbine missiles) and (c) external hazards, both natural (e.g. earthquake, high winds, external floodings)

[3] ~~INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-3, IAEA, Vienna (2010).~~

and of human-induced (e.g. airplane crash, explosion pressure waves, accidents at nearby industrial facilities).

1.12. This Safety Guide focusses on the assessment of nuclear power plant respective spent fuel pools. An assessment of ~~is focused on the reactor core and the fuel in the spent fuel pool; it does not cover~~ other sources of radioactive material on the site, e.g. the interim fuel storage facilities, is not in the scope of the Safety Guide. ~~The reactor core is in the main focus of this Safety Guide; however, the specifics of the spent fuel pool analysis are addressed.~~The scope of this Safety Guide covers also Level 1 Multi-Unit PSA which is aimed to quantify the multi-unit risk metrics.

1.13. The consideration of hazards arising from malicious actions is not within the scope of this Safety Guide.

1.14. In carrying out Level 1 PSA, the most common practice is to perform the analysis for the various hazards and operating states in separate modules, having a Level 1 PSA for power operation for internal initiating events as a basis. This Safety Guide follows this approach.

1.15. The recommendations of this Safety Guide are intended to be technology neutral to the extent possible, and it is expected that the vast majority of the recommendations will be applicable to different types of nuclear power plant.

STRUCTURE

1.16. Section 2 provides recommendations on the general issues concerning the performance and use of PSA, including the scope of the PSA, validation of the PSA and a living PSA. Section 3 provides key recommendations on project management and organization for PSA and general aspects of PSA documentation. Section 4 addresses the task of familiarization of the team carrying out the PSA with the nuclear power plant. Sections 5–8 provide recommendations on the methodology of a Level 1 PSA for power operation for various initiating events and hazards. Section 5 provides recommendations on Level 1 PSA for internal initiating events. Section 6 summarizes key recommendations on the general aspects of Level 1 PSA for internal and external hazards, and Sections 7 and 8 address the specifics of Level 1 PSA for internal hazards and external hazards, respectively. Section 9 provides key recommendations for Level 1 PSA for shutdown states, whereas recommendations for Level 1 PSA for low power states are included in the previous sections. Section 10 addresses the development of PSA for spent fuel pools. Section 11 provides ~~recommendations on~~ recommendations on Level 1 multi-unit PSA aimed to quantify multi-unit risk metrics, whereas consideration of multi-unit interactions from a single unit Level 1 PSA perspective are presented in Sections 5-10. Section 12 sets out key recommendations for applications of Level 1 PSA. Three annexes provide an example of a generic list of internal and external hazards, an example of a fire propagation event tree and a seismic event tree and supporting information on PSA for shutdown states.

2. GENERAL CONSIDERATIONS RELATING TO THE PERFOMANCE AND USE OF PSA

2.1. This section describes some general issues relevant to the performance of PSA and the use of PSA results in practice. Though the scope of the Safety Guide is limited to consideration

of Level 1 PSA, this section describes the issues from a broader perspective in order to provide a complete picture of the capabilities of PSA technology and its results. Some statements in this section do not represent explicit recommendations; rather, they provide supporting information to facilitate understanding of the context of other statements and recommendations provided in other sections of the Safety Guide.

SCOPE OF THE PSA

2.2. Paragraphs 2.2–2.4 provide recommendations on meeting Requirement 1 of GSR Part 4 [3] on a graded approach and Requirement 14 of GSR Part 4 [3] relating to the scope of the safety analysis for a PSA. The scope of the PSA to be undertaken should be correlated with the ~~national~~ probabilistic safety goals or criteria, if the~~y latter~~ have been specified in national regulations or guidelines ~~set~~. At a high level, quantitative results of PSA are often used to verify compliance with probabilistic safety goals or criteria, which are usually formulated in terms of quantitative estimates of core damage frequency or fuel damage frequency, frequencies of radioactive releases of different types and societal risks and which therefore may necessitate performance of a Level 1 PSA, Level 2 PSA or Level 3 PSA, respectively. Probabilistic safety goals or criteria do not usually specify which hazards and plant operating states have to be addressed. Therefore, in order to use the PSA results for the verification of compliance with existing probabilistic safety goals or criteria, a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operating states should be performed unless the probabilistic safety goals or criteria are formulated to specify a PSA of limited scope, or alternative approaches are used to demonstrate that the risk from those initiating events and hazards and operating states that are not in the model does not threaten compliance with the probabilistic safety goals or criteria.

2.3. The scope of Level 1 PSA should include consideration of the fuel in reactor core for a single unit. The recommendations on development of Level 1 PSA for reactor core of single unit are specified in the Sections 5-9. The scope of the Level 1 PSA ~~might~~ should also include consideration of the fuel in spent fuel pool, for which recommendations are provided in Section 10. In addition, the scope of Level 1 PSA might include consideration of multi-unit risk metrics, for which recommendations are provided in Section 11.

2.4. A major advantage of PSA is that it provides an explicit framework for the analysis of uncertainties in risk estimates. The identification of sources of uncertainty and an understanding of their implications on the PSA model and its results should be considered an inherent part of any PSA, so that, when the results of the PSA are to be used to support a decision, the impact of the uncertainties can be taken into account.

VALIDATION AND REVIEW OF THE PSA

2.5. Paragraphs 2.5 and 2.6 provide recommendations on meeting Requirement 18 of GSR Part 4 [3] on the use and validation of computer codes for a PSA and Requirement 21 of GSR Part 4 [3] on the independent verification of PSA. PSA involves a number of analytical methods. These include the analysis of accident sequences and the associated systems, typically through the development of event tree and fault tree logic models, the methods for solution of the logic models, the models of phenomena that could occur, for instance, within the containment of a nuclear power plant following core damage, and the models for the transport of radionuclides in the environment to determine their effects on health and the environment~~economy~~, depending on the scope of the analysis (Level 1, 2 or 3). Prior to their application, it should be demonstrated that these analytical methods provide an adequate

representation of the processes taking place. The computer codes that support these analytical methods are required to be adequate for the purpose and scope of the analysis, and the controlling physical and logical equations are required be correctly programmed in the computer codes: see para. 4.60 of GSR Part 4 [3].

2.6. It is a widely accepted practice for the organization conducting a PSA to commission an independent peer review of the PSA from an outside body, sometimes from a different State, to provide a degree of assurance that the scope, modelling and data are adequate, and to ensure that they conform to current, internationally recognized good practices in PSA. The experts involved in the review of the PSA should not be engaged in any activities relating to performance of the PSA under consideration and should represent an organization that is independent of the developer of the PSA.

LIVING PSA

2.7. Paragraphs 2.7–2.9 provide recommendations on meeting Requirement 24 of GSR Part 4 [3] on maintenance of the safety assessment for Level 1 PSA. In the operating lifetime of a nuclear power plant, modifications are often made to the SSC design ~~of safety systems~~ or to the way the plant is operated. Such modifications could have an impact on the level of risk associated with the plant. Additional statistical data on the frequencies of initiating events and the probabilities of component failure will become available during plant operation. Likewise, new information and more sophisticated methods and tools may become available, which may change some of the assumptions made in the analysis and hence the estimates of the risk given by the PSA. Consequently, the PSA should be kept up to date throughout the lifetime of the plant to ensure that it remains relevant for the decision making process. A PSA that undergoes regular periodical updating is termed a 'living PSA'. In updating a PSA, account should be taken of changes in the design and operation of the plant, new technical information, more sophisticated methods and tools that become available and new plant specific data derived from the operation of the plant, e.g. data to be used for the assessment of initiating event frequencies or component failure probabilities. The updating of a PSA should be initiated by a specified process and the status of the PSA should be reviewed regularly to ensure that it is maintained as a representative model of the plant and fits the purpose it is intended for.

2.8. Data should be collected throughout the lifetime of the plant to check or update the analysis. Such data should include data on operating experience, in particular data on initiating events, data on component failures and unavailability during periods of testing, maintenance and repair, and data on human performance. The results from the analysis should be periodically reassessed in the light of new data.

2.9. The development of a living PSA should be encouraged to assist the decision making process in the normal operation of the plant. Many issues, such as evaluation of the change in risk associated with a change to the plant or a temporary change in the allowed outage time of a component, can be supported by arguments derived from a PSA. Experience has shown that such a living PSA can be of substantial benefit to the operating organization and its use is generally welcomed by regulators.

PROBABILISTIC SAFETY GOALS OR CRITERIA

2.10. Paragraphs 2.10–2.15 provide recommendations on meeting Requirement 4 of GSR Part 4 [3] for the purpose of conducting a PSA. When the aim of the PSA is to identify significant contributors to risk or to choose between various design options and plant configurations, a

reference value may not be necessary. However, when the aim of the PSA is to assist in reaching a judgement on whether (i) a calculated risk is acceptable, (ii) a proposed change to the design or operation of the plant is acceptable, or (iii) a change is necessary to reduce the level of risk, then probabilistic reference values should be specified to provide guidance to designers, operating organizations, regulators and other interested parties in fulfilling their respective roles in the provision of safe nuclear power, on the level of safety desired or required for the plant. In some States, current practice is for reference values to be formulated as probabilistic safety goals, with the implication that they represent orientation values whose achievement is to be aimed for. In other States, the reference values are criteria that specify strict limits for which compliance is required.

2.11. A PSA will yield numerical values relating to risk at various levels, depending on the consequences to be evaluated. Probabilistic safety goals or criteria may be set in relation to any or all of the following measures:

(a) The probability of failure of particular safety functions or systems involved in performance of safety functions;
(b) The frequency of core[4] or fuel damage (Level 1 PSA);
(c) The frequency of a specific release (specified, for example, in terms of its quantity, isotopes, timing) of radioactive material from the plant or the frequency of a release of radioactive material as a function of its magnitude (Level 2 PSA) [4];
(d) The frequency of occurrence of specific health effects to members of the public or the frequency of occurrence of particular environmental consequences (Level 3 PSA).

2.12. ~~The available frameworks and examples for the definition of probabilistic safety criteria are discussed in Ref. [11].~~ In the Member States the probabilistic safety criteria are typically identified as targets, goals, objectives, guidelines or reference values for orientation. In addition, the numerical values for the levels of risk, which correspond to the threshold of tolerability and the design targets, differ from State to State.[5]

2.13. For the probability of failure of safety functions or ~~safety~~ systems, the probabilistic targets can be set at the level of the safety function or ~~safety~~ system. Such probabilistic targets are useful for checking that the level of redundancy and diversity provided is adequate. Such targets will be specific to the plant design and therefore no recommendations on setting such targets can be provided here. In the safety assessment, it should be checked whether these targets have been met. If they have not, the design may still be acceptable provided that the higher level criteria have been met. However, particular consideration should be given to the ~~safety~~ systems in question to see whether any reasonably practicable improvements can be made.

2.14. On the basis of current experience with the design and operation of nuclear power plants and on the basis of acceptable risks, there are proposed numerical values that are to be used for existing and new nuclear power plants, which are defined on a national level in some Member

[4] For the concept of core damage, specific probabilistic safety goals or criteria needs to be specified, as described in Section 5 of this Safety Guide. These safety goals or criteria may be different for different reactor designs.
[5] The available frameworks and examples for the definition of probabilistic safety criteria are discussed in Ref. [11].

States. For example, INSAG (see Ref. [98]) has proposed the objectives for core damage frequency separately for existing plants and future plants.[6]

2.15. Core or fuel damage frequency are the most common measures of risk used in Level 1 PSA. In many States, numerical values of this type are used either formally or informally as probabilistic safety goals or criteria.

USE OF PSA IN DECISION MAKING

2.16. Paragraphs 2.16–2.24 provide recommendations on meeting Requirement 23 of GSR Part 4 [3] on the use of a Level 1 PSA. The PSA should be used during the lifetime of the plant to provide an input into decision making in combination with the results and insights of deterministic safety analyses and considerations of defence in depth.

2.17. PSA can provide useful insights and inputs for various interested parties, such as operating organizations plant staff (management and engineering, operations and maintenance personnel), regulatory bodies, technical support organisations, designers and vendors, for making decisions on:

(a) Design modifications and plant modifications;
(b) Optimization of plant operation and maintenance;
(c) Safety analysis and research programmes;
(d) Regulatory issues.

2.18. Where the results of the PSA are to be used in support of the decision making process, a formal framework for doing so should be established (see Ref. [9]). The details of the decision making process will depend on the purpose of the particular PSA application, the nature of the decision to be made and the PSA results to be used. If numerical results from the PSA are to be used, reference values against which these results can be compared should be established.

2.19. The PSA should address the actual design or, in the case of a plant under construction or when modifications are being undertaken, the intended design or operation of the plant, which should be clearly identified as the basis for the analysis. The status of the plant can be fixed as it was on a specific date or as it will be when agreed modifications are completed. This needs to be done to provide a clear target for completion of the PSA. Later changes can be addressed in the framework of a living PSA programme, as described in paras 2.7–2.9.

2.20. For a plant in the design stage, the results of PSA should be used as part of the design process to assess the level of safety. In this case, the insights gained from PSA should be considered in combination with the insights gained from deterministic analysis to make decisions about the safety of the plant. Decisions on the safety of the plant should be the result of an iterative process aimed at ensuring that national requirements and criteria are met, the design is balanced, and the risk is as low as reasonably achievable.

2.21. In addition, the results of the PSA should be compared with the probabilistic safety goals or criteria if these have been specified in national regulations or guidelines. This should be done for all probabilistic criteria defined for the plant, including those that address system

[6] The objectives for core damage frequency in Ref. [8] are (a) 1×10^{-4} per reactor-year for existing plants and (b) 1×10^{-5} per reactor-year for future plants. It was not explicitly specified in Ref. [8] for which scope of PSA the numerical values are applicable. It is assumed that a full scope PSA is meant.

reliability, core damage frequency, fuel damage frequency, frequencies of releases of radioactive material, health effects for workers, health effects for the public and off-site consequences such as land contamination and restrictions on foodstuffs.

2.22. The PSA should set out to identify all accident sequences that not negligibly contribute to risk. and to determine weaknesses and potential improvements in the design or operation of the plant. The PSA can be used, for example, to assess the need for changes to reduce the safety significance of such weaknesses. If the analysis does not address all the significant contributions to risk (for example, if it omits external hazards or shutdown states), then conclusions drawn from the PSA about the level of risk from the plant, the balance of the safety systems features provided and the need for changes to be made to the design or operation to reduce the risk may be biased. Therefore, the utilization of full scope PSA models is recommended.

2.23. The results of the PSA should be used to identify weaknesses in the design or operation of the plant. These can be identified by considering the contributions to the risk from groups of initiating events, the importance measures of the safety systemsSSCs and the contributions of human error to the overall risk. Where the results of the PSA indicate that changes could be made to the design or operation of the plant to reduce risk, the changes should be incorporated where reasonably achievable, taking the relative costs and benefits of any modifications into account.

2.24. Section 12 provides detailed recommendations on specific applications of PSA for the regulatory body and for operating organizations.

3. PROJECT MANAGEMENT AND ORGANIZATION FOR PSA

DEFINITION OF OBJECTIVES AND SCOPE OF THE PSA PROJECT

3.1. Paragraphs 3.1 and 3.2 provide recommendations on meeting Requirement 4 of GSR Part 4[3] on the purpose of the Level 1 PSA and Requirement 14 of GSR Part 4 [3] on the scope of a Level 1 PSA. Determination of the objectives of the PSA together with its intended and potential uses is an important step to undertake prior to starting the process of performing a PSA. The scope of the PSA is defined by the analysis level (Level 1, 2 or 3), the initiating events and hazards considered, and the operating states (i.e. at power or shutdown states[7]) addressed. The scope of the PSA should be compatible with both the objectives of the study and the available resources and information, i.e. the necessary procedures and methods, personnel, expertise, funding and the time needed for the analysis. For example, if the objective of a PSA is to verify the risk arising from plant operation against specified probabilistic safety goals, thus implying a complete risk assessment, a full scope PSA comprising a comprehensive listing of initiating events and hazards and all plant operating states should be performed. Adequate resources should be provided for the analysis. In addition, other sources of radiation, particularly (e.g. the fuel in the spent fuel pool) should be analysed, depending on the formulation of the probabilistic safety goals.

3.1.

[7] PSA for low power and shutdown states is sometimes performed as part of the same study, however, it is more practical to perform low power PSA as part of PSA for power operation.

3.2. It should be recognized that the intended applications of PSA may impose additional requirements on the scope of the PSA, on the modelling approaches and on the level of detail. If such additional requirements are taken into account at the planning stage of the PSA project, it will help to avoid inconsistencies in the results and insights obtained. For instance, if it is planned to use the PSA for the development of a severe accident management programme, a Level 2 PSA should be performed. An extension ~~of~~ to Level 2 or even Level 3 PSA should be also required if it is to be used to support definition of emergency planning zones. As another example, if it is planned to use the PSA model as a basis for a risk monitor, the PSA model should be 'symmetrical' in terms of the modelling of initiating events[8]. The common simplification of modelling an initiating event as always occurring in one particular train should not be used. For example, loss of coolant accidents should be modelled for each loop with an appropriate probability that a specific loop is affected (i.e. 1/2 for a two train plant, 1/3 for a three train plant) rather than a single event in one of the loops. More details on the features of PSA necessary for various applications of PSA are provided in Section 12.

PROJECT MANAGEMENT FOR PSA

3.3. Paragraphs 3.3–3.14 provide recommendations on meeting Requirement 5 of GSR Part 4 [3] on preparation for the safety assessment for Level 1 PSA, and on meeting Requirement 22 of GSR Part 4 [3] on management of the safety assessment. Project management of the PSA depends strongly on the specific conditions in a State, namely:

(a) The organizations participating in the PSA project;
(b) The type and extent of the involvement of the participating organizations;
(c) The objectives and the scope of the PSA study.

After the objectives and the scope of the PSA have been specified, the management scheme for the PSA project should be developed, including the selection of methods and establishment of procedures, the selection of personnel and the organization of the team that will perform the PSA, the training of the team, the preparation of a PSA project schedule, the estimation and securing of the necessary funds, and the establishment of quality assurance procedures and peer review procedures.

3.4. A PSA study is normally commissioned by one of the following:

(a) The plant designer;
(b) The operating organization of the plant;
(c) The regulatory body.

The PSA can be performed by these groups or by consultants, research institutes, universities or a combination of these. In any case, the operating organization should always participate as a source of operational knowledge, as well as being a beneficiary from the insights obtained[9].

[8] Non-symmetrical modelling of initiating events could create obstacles in obtaining the realistic risk profile through risk monitor when introducing the specific changes in plant configuration.

[9] Implementation of this recommendation could be challenging for the PSA performed at the design stage of the plant. Also, if 'generic' PSA is performed for the reference plant, the participation of operating organization may be preferred to support the knowledge from their operating experiences.

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

3.6. The PSA study should consider a particular 'freeze date' for modelling the as built and as operated plant conditions. If it is known at the beginning of the PSA project that certain changes in plant design and operation will be implemented in the near term, before the PSA is finished, a decision should be taken at an early stage of the PSA as to whether these changes will be addressed in the PSA. If the decision is made to address the future changes, the freeze date should be determined accordingly, and the PSA should take account of the status of the plant after the modifications.

3.7. The documentation for the PSA should be developed in a clear, traceable, systematic and transparent manner so that it can effectively support the review of PSA, applications of PSA and future PSA upgrades.

SELECTION OF METHODS AND ESTABLISHMENT OF PROCEDURES

3.8. Appropriate working methods and procedures should be established at the outset of the project so that there is a minimum of modification to these procedures during the project. Unnecessary iterations in methods and procedures may cause delays in the PSA project. General guidance for the methodological tools and approaches to analysis is given in the following sections of this publication. Once the working methods have been selected, the various procedural steps should be interfaced with the tasks of quality assurance and training to produce a detailed plan of the tasks, including a schedule for the project.

3.9. The resources in terms of the expertise of the specialists involved, human resources, computer time, calendar time and so on that will be necessary to complete a PSA depend greatly on the scope of the PSA, which is in turn governed by the overall objectives, and on the available expertise in the PSA team. Scheduling of the activities should be carried out following the establishment of detailed procedures and should take into account the availability of personnel.

TEAM SELECTION AND ORGANIZATION

3.10. ~~A~~ The members of the team that perform the PSA can be characterized by the organization they represent and the technical expertise they provide. Once the necessary personnel have been identified, lines of communication should be set up and specific tasks should be assigned. The training necessary should be determined and planned in accordance with the activities of the PSA. The task of team formation and training is closely associated with the corresponding tasks of quality assurance.

3.11. The expertise necessary to conduct a PSA should provide two essential elements: knowledge of the plant and knowledge of PSA techniques. This expertise can vary in depth, depending on the scope of the PSA, but the participation of the plant designer and the operating organization of the plant should be foreseen, if possible. More specifically, the necessary expertise relating to knowledge of the plant should be obtained from persons with extensive

familiarity with the design and operation of the plant under operating states and accident conditions.

3.12. A team that will perform a PSA for the first time should be provided with training to acquire the expertise necessary to complete the study successfully.

ESTABLISHING QUALITY ASSURANCE PROGRAMME FOR PSA

3.13. The quality assurance[10] programme for a PSA encompasses activities that are necessary to achieve the appropriate quality of the PSA and activities that are necessary to verify that the appropriate quality is achieved. For a PSA, appropriate quality means an end product that is correct and usable and one which meets the objectives and fulfils the scope of the PSA. The quality assurance programme should provide for a disciplined approach to all activities affecting the quality of the PSA, including, where appropriate, verification that each task has been satisfactorily performed and that necessary corrective actions have been implemented.

3.14. Quality assurance of the PSA should be viewed and established as an integral part of the PSA project and the quality assurance procedures should be an integral part of the PSA procedures. The quality assurance procedures should provide for control of the constituent activities associated with a PSA in the areas of organization, technical work and documentation. In their application to the technical work, quality assurance procedures are aimed at ensuring consistency between goals, scope, methods and assumptions, as well as accuracy in the application of methods and in calculations. Quality assurance procedures should include control of the documentation of the PSA. General requirements for control of documents are established in ~~section 2 of~~ Ref. [~~7~~12].

GENERAL ASPECTS OF PSA DOCUMENTATION

Objectives and content of documentation

3.15. Paragraphs 3.15–3.22 provide general recommendations on meeting Requirement 20 of GSR Part 4 [3] on documentation for Level 1 PSA. The primary objectives of the PSA documentation should be to meet the needs of its users and be suitable for the specific applications of the PSA. Possible users of the PSA include:

(a) Operating organizations of nuclear power plants (management and operating personnel);
(b) Designers and vendors;
(c) Regulatory bodies and persons or organizations providing them with technical support;
(d) Other government bodies;
(e) The public.

Some of these users, the public for example, might use, primarily, the summary report of the PSA, while others will use the full PSA documentation, including the computer model.

3.16. PSA documentation includes work files, computer inputs and outputs, correspondence, interim reports and the final report of the PSA. The documentation of PSA should be complete, well structured, clear and easy to follow, also regarding review and update. It should be

[10] Instead of the term ‘quality assurance’, the term ‘management system’ is used in Ref. [12]. The term ‘quality assurance’ is used in this Safety Guide in order to reflect widely accepted current practices and terminology used in the area of PSA.

presented in a traceable and sequential manner, i.e. the order of appearance of analysis in the final documentation should follow, as far as possible, the order in which it was actually performed. In addition, means should be provided for possible extensions of the analysis, including integration of new topics, use of improved models, broadening of the scope of the PSA in question and its use for alternative applications. Explicit presentation of the assumptions, exclusions and limitations for extending and interpreting the PSA is also of critical importance to users.

3.17. The documentation should provide within the report (or by reference to available material) all necessary information to reconstruct the results of the study. All intermediate supporting analyses, calculations and assumptions that will not be published in any external reports should be retained as notes, working papers or computer outputs. This is very important for reconstructing and updating each detail of the analysis in the future.

Organization of documentation

3.18. The final report of the PSA study should be divided into three major parts:

(1) Summary report;
(2) Main report;
(3) Appendices to the main report.

3.19. The summary report should be designed to provide an overview of the motivations, objectives, scope, assumptions, results and conclusions of the PSA at a level that is useful to a wide audience of reactor safety specialists and that is adequate for high level review. The summary report should be designed:

(a) To support high level review of the PSA;
(b) To communicate key aspects of the study to a wide audience of interested parties;
(c) To provide a clear framework and guide for the reader or user prior to consulting the main report.

3.20. The summary report of a PSA should include a subsection on the structure of the report, which should present concise descriptions of the contents of the sections of the main report and of the individual appendices. The relation between various parts of the PSA should also be included in this subsection of the summary report.

3.21. The main report should give a clear and traceable presentation of the complete PSA study, including a description of the plant, the objectives of the study, the methods and data used, the initiating events considered, the plant modelling results and the conclusions. The main report, together with its appendices, should be designed:

(a) To support technical review of the PSA;
(b) To communicate key detailed information to interested users;
(c) To permit the efficient and varied application of the PSA models and results;
(d) To facilitate the updating of the models, data and results in order to support the continued safety management of the plant.

3.22. The appendices should contain detailed data, records of engineering computations and detailed models. The appendices should be structured so as to correspond directly to the sections and subsections of the main report, as far as possible.

3.23. In addition to the general recommendations for documentation provided in this section, specific recommendations for documentation are provided in other sections of this Safety Guide, for example, for PSA for internal initiating events, for PSA for internal fire, for PSA for internal flooding, for PSA for external hazards and for PSA for shutdown states.

4. FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION

4.1. This section provides recommendations on meeting Requirement 5 of GSR Part 4 [3] on preparation for Level 1 PSA. The PSA team should familiarize themselves with the design and operation of the plant, including the emergency procedures and the test and maintenance procedures. Information sources that may be used for familiarization with the plant include the following:

(a) The safety analysis report for the plant;
(b) Technical specifications for the plant;
(c) System descriptions;
(d) As built (as is) system drawings (piping and instrumentation diagrams);
(e) Electrical line drawings, including circuit diagrams and trip criteria for the electrical bus protection system;
(f) Control and actuation circuit drawings;
(g) Normal operating procedures, emergency procedures, test procedures and maintenance procedures;
(h) Analyses pertinent to the determinants of mission success criteria of systems;
(i) Operating experience from the plant or from similar plants in the same State or other States, and reports and analysis of incidents;
(j) Operator's logs;
(k) Discussions with operating staff;
(l) Plant operational records and reports of shutdowns;
(m) Plant databases and/or the computerized management system for maintenance, if available;
(n) Plant layout drawings;
(o) Drawings of piping location and routing;
(p) Drawings of cable location and routing;
(q) Plant walkdown reports;
(r) Regulatory requirements;
(s) Other relevant plant documents.

4.2. The plant documents containing the information necessary for the analysis should be collected and made available to the PSA team. Depending on the scope of the PSA, more specific information may be required, for example, plant layout and topography of the site and

surroundings for PSA for external hazards. Interaction with operating personnel who are not part of the PSA team might be necessary for clarification and additional information.

4.3. Currently, in many Member States, performance of a PSA is required as part of the safety analysis report. In this case, PSA documentation may refer to the corresponding sections of the safety analysis report, e.g. descriptions of systems. All references should be clearly provided so that the referred information can be easily found.

4.4. Plant familiarization is a key element of PSA for external and internal hazards. A thorough plant walkdown should be performed to verify information on hazard sources and plant features susceptible to damage due to the hazard. Specific guidance for plant familiarization for external and internal hazards should be provided.

5. LEVEL 1 PSA FOR INTERNAL INITIATING EVENTS FOR POWER OPERATION

5.1. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 [3] for Level 1 PSA for internal initiating events. In particular, it provides recommendations on the technical issues that need to be addressed in carrying out a Level 1 PSA for internal initiating events caused by random component failures and human errors occurring at power operation. The general framework for analysis is illustrated in Fig. 1.

GENERAL ASPECTS OF LEVEL 1 PSA METHODOLOGY

5.2. The first step should be to define the overall approach and methodology to be used for the Level 1 PSA. The overall approach and methodology should be capable of modelling the fault sequences that could occur, starting from an initiating event, and should be capable of identifying the combinations of ~~safety system~~ SSC failures~~, support system failures~~ and human errors that could lead to core damage.

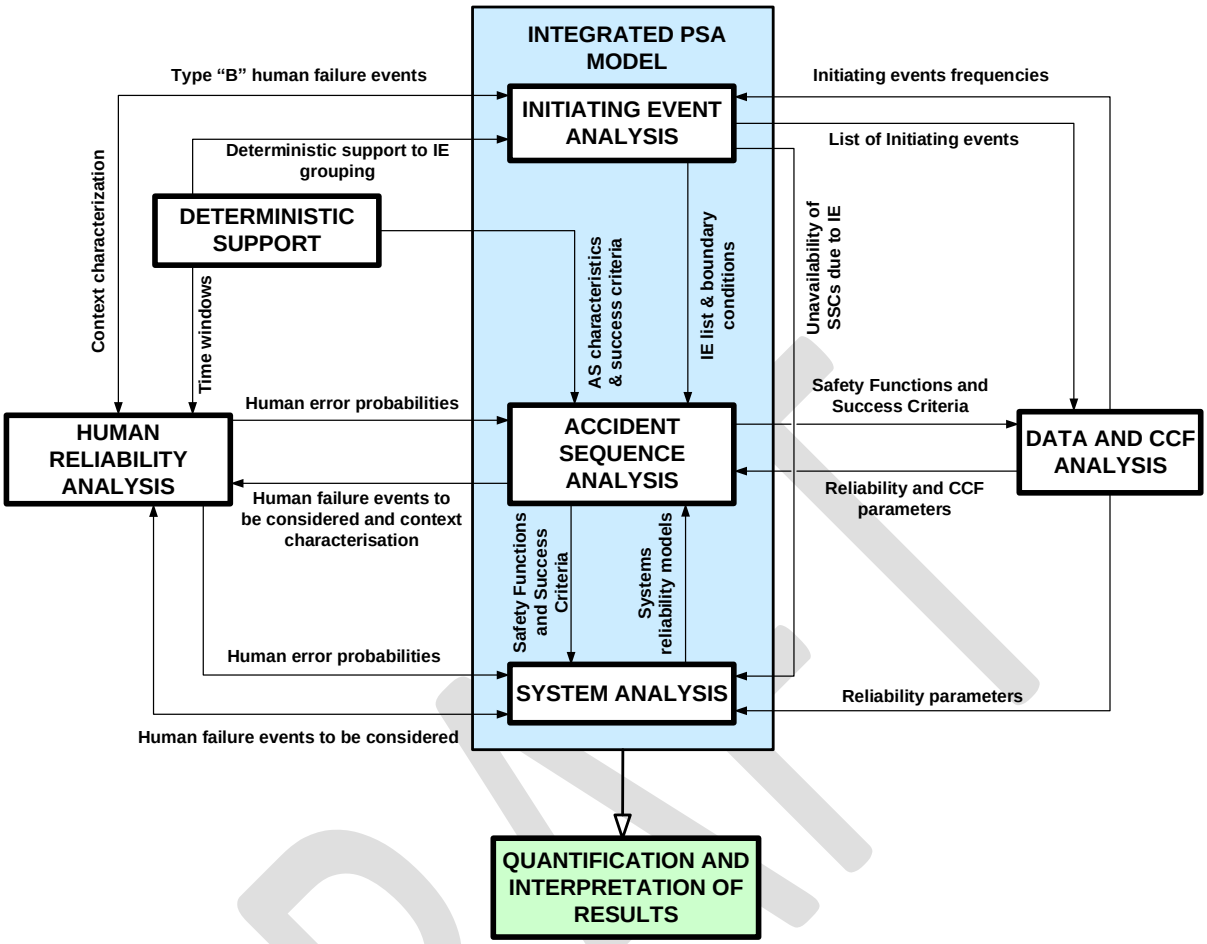

FIG. 1. General analysis framework of a Level 1 PSA for internal initiating events.

5.3. Several techniques can be used in performing a PSA. However, the usual approach is to use a combination of event trees and fault trees. The relative size (complexity) of the event trees and fault trees is largely a matter of preference of the team carrying out the analysis and also depends on the features of the software used.

5.4. One widely practised approach is to use a combination of small event trees and large fault trees often referred to as the fault tree linking approach. The event trees outline the broad characteristics of the accident sequences that start from the initiating event and, depending on the success or failure of the ~~mitigating systems~~systems credited in PSA (hereinafter referred to as 'credited systems'[11]), lead to a successful outcome or to the core damage (see paras 5.42 and 5.43), or to one of the plant damage states (used in the Level 2 PSA). The fault trees are used to model the failure of the ~~mitigating~~ credited systems to carry out their safety functions.

5.5. Another approach that is widely used is to carry out the analysis using large event trees and small fault trees. In this approach, failures of safety functions, ~~mitigating system~~credited systems and support systems are modelled in the event trees. This approach is variously referred to as the large event tree approach, the linked event tree approach, or the event tree with boundary conditions approach. It is also possible to carry out the analysis using event trees

[11] Credited systems – Systems credited in PSA, which include operating and stand-by safety and non-safety systems which operation during the accident can support prevention of the undesired end state (e.g. core damage, fuel damage)

only or fault trees only. However, in the latter case, the high level fault tree structure is usually derived from, or based on, an event tree or set of event trees.

5.6. The overall aim should be to calculate a best estimate of the core damage frequency while avoiding the introduction of excessive conservatisms wherever possible, since this may unduly bias the results. Hence, the Level 1 PSA should be based on best estimate models, assumptions and data. However, some conservatism may be necessary where there is a high level of uncertainty, in order to avoid unjustifiable optimism.

5.7. For plants with multiple units, the interactions between the units (both positive and negative from risk point of view) should be considered in Level 1 PSA from the perspective of the unit under consideration~~., whereas~~ The recommendations on multi-unit PSA aimed to quantify multi-unit risk metrics are provided in Section 11[12].

5.8. The Level 1 PSA model ~~produced~~ developed should be capable of being used for the intended applications and of being updated for possible future applications.

5.9. The analysis should be carried out using a suitable computer code that has the following capabilities:

(a) It should be capable of handling the very large and complex logic model of the nuclear power plant.
(b) It should be capable of quantifying the PSA model in a reasonably short time ~~scale~~frame.
(c) It should be capable of providing the information necessary to interpret the Level 1 PSA, such as the core damage frequency, dominant minimal cutsets, frequencies of minimal cutsets (combinations of initiating events and failures and/or human errors leading to core damage), importance measures and results of uncertainty and sensitivity analyses.

5.10. The ~~production~~ development of ~~the~~ a Level 1 PSA is an iterative process and it should be carried out until an accurate, sufficiently detailed model has been produced.

INITIATING EVENT ANALYSIS

5.11. The starting point of the Level 1 PSA is the identification of the set of initiating events. An initiating event is an event that could lead directly to core damage (e.g. reactor vessel rupture) or that challenges normal operation, and which necessitates successful mitigation using safety or non-safety systems to prevent core damage.

5.12. This section deals with the identification of internal initiating events that could arise during power operation. The general methodology for Level 1 PSA for internal and external hazards is presented in Section 6 and detailed recommendations are provided in Sections 7 and 8, respectively. Recommendations on issues specific to the identification of initiating events that could arise in shutdown states are provided in Section 9, for the spent fuel pool are provided in Section 10 and for Multi-unit PSA are provided in Section 11).~~.~~

Identification of initiating events

[12] In case of initiating events affecting the entire site the consideration of adverse effects of other facilities on site (e.g. interim dry fuel storage facilities to the reactor and spent fuel pool is considered to be important).

5.13. A systematic process should be used to identify the set of initiating events to be addressed in the Level 1 PSA. This should involve a number of different approaches including:

(a) Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for ~~all~~ plant SSCs ~~safety systems~~ to determine whether their failures, either partial or complete, could lead to an initiating event;
(b) Deductive analyses such as master logic diagrams to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an initiating event;
(c) Comparison with the lists of initiating events developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines;
(d) Identification of initiating events on the basis of the analysis of operating experience from the plant under investigation and from similar plants;
(e) Review of the deterministic design basis accident analysis and design extension conditions ~~beyond design basis accident~~ analysis and the safety analysis report.

5.14. The set of internal initiating events used as the basis for the Level 1 PSA should be as comprehensive as possible. It is recognized that it is not possible to demonstrate that all possible initiating events have been identified. However, by using a sufficiently comprehensive combination of the different approaches listed in para. 5.13, it is possible to gain confidence that the set of initiating events that has been identified for the plant is as comprehensive as possible.

5.15. In identifying initiating events, particular consideration should be given to any design features that are novel or distinctive to the plant in question as potential sources of new initiating events. This is particularly important for new nuclear power plants where there is little or no operating experience and special efforts should be made to identify unique initiating events, failure modes, accident sequences and dependencies that are particular to that design. The analytical techniques indicated in para. 5.13 (a) should be carried out for all the operating systems and standby systems to identify possible initiating events (or consequential failures that could constitute initiating events) that could arise through failure to operate, partial failure to operate or inadvertent operation.

5.16. The major categories of initiating events that are included in the Level 1 PSA are events that threaten the safety functions, such as removal of heat from the reactor core, control of the primary coolant inventory, maintaining the integrity of the primary circuit and control of the reactivity of the core.

5.17. The set of initiating events identified should include partial functional failures or partial system failures as well as complete failures, for example, reduction of feed to steam generators or loss of feed to one steam generator as well as complete loss of all feed to all steam generators. This is important since initiating events involving partial failures could make a significant contribution to the risk.

5.18. The set of initiating events identified should include those that can occur during all the permissible operating states, for example, operation with one of the coolant loops removed from service.

5.19. The set of initiating events should include events of very low frequency with potentially large consequences, for example, rupture of the reactor pressure vessel, or loss of coolant

accidents in interfacing systems. Inclusion of loss of coolant accidents in interfacing systems is particularly important if the Level 1 PSA is intended to be used as the basis for a Level 2 PSA (and possibly a Level 3 PSA).

5.20. For sites with more than one nuclear power plant unit, the set of initiating events that can affect more than one of the units at the same time should be identified, for example, loss of off-site power. In addition, events that can arise in one of the units and lead to an initiating event in another unit should be identified, for example, for a Level 1 PSA for internal hazards, an initiating event in the unit being analysed could be caused by a strike from a missile generated by disintegration of a turbine in an adjacent unit.

5.21. The set of initiating events identified for the plant should be compared with that for similar plants, as stated in para. 5.13 (c), to ensure that all the relevant initiating events have been included. Where differences are identified, additional initiating events should be included, or justification should be provided of why they are not relevant.

5.22. A review of the operating experience of the nuclear power plant (if it is already operating) and of similar nuclear power plants should be carried out to ensure that any initiating events that have actually occurred are included in the set of initiating events addressed in the Level 1 PSA.

5.23. The causes of such initiating events should be identified and should be taken into account in the analysis. For initiating events that have a number of causes or where more than one failure would be necessary for the initiating event to occur, a common approach is to use a fault tree to model the initiating event.

Transients

5.24. The Level 1 PSA should be based on a comprehensive set of transients that can occur. Examples of the types of transient that can occur include the following:

(a) Increase in reactor heat removal, e.g. opening of secondary relief valve(s) or a steam line break;
(b) Decrease in reactor heat removal, e.g. loss of main feed or a feed line break;
(c) Decrease in reactor coolant system flow rate, e.g. tripping of the reactor coolant pump, pump seizure or shaft break;
(d) Anomalies in reactivity and power distribution, e.g. uncontrolled control rod withdrawal, control rod ejection or boron dilution;
(e) Increase in reactor coolant inventory, e.g. inadvertent operation of the emergency coolant injection system;
(f) Any event causing a reactor trip or immediate shutdown of the reactor.

5.25. The set of transients should include loss of off-site power as an internal initiating event. The initiating event involving loss of off-site power should be specified in terms of the frequency of occurrence and the duration of the loss of off-site power, which should take into account the likelihood of recovery of off-site power. This should be based on details of the design and operating experience in relation to the grid connections to the plant.

5.26. When losses of off-site power that could occur due to internal hazards (such as a fire in the plant) and external hazards (such as extreme environmental conditions or an earthquake)

are modelled explicitly in a PSA for those hazards, the definition of the loss of off-site power for the model for internal initiating events should exclude these causes so as to avoid double counting in the Level 1 PSA.

5.27. The set of initiating events should also include failures of support systems, for example, electrical power systems, instrument air, cooling water systems, room cooling systems and the instrumentation and control systems. This is particularly important where the failure of a support system could lead to a reactor trip and the support system also provides a safety function after a reactor trip.

Loss of coolant accidents

5.28. A complete set of initiating events that can lead to a loss of coolant accident should be considered in Level 1 PSA.

5.29. The set of loss of coolant accidents identified should include all the different sizes and locations of breaks that can lead to a loss of primary coolant. Possible locations should be identified on the basis of the actual design and layout of the plant and the set of loss of coolant accidents should include failures of pipework and valves, in particular, relief valves.

5.30. The set of loss of coolant accidents that can result in the discharge of primary coolant outside the containment should be identified. This typically includes steam generator tube ruptures and loss of coolant accidents in interfacing systems where the primary coolant leakage from the break bypasses the containment and hence is not available for recirculation from the containment sump.

5.31. The set of loss of coolant accidents identified should be categorized and grouped in accordance with the success criteria of the ~~safety systems~~SSCs that needs to be operated to prevent core damage. For pressurized water reactors, loss of coolant accidents are usually categorized as large, medium or small, mainly on the basis of the performance required from the coolant injection systems to mitigate the loss of coolant accident. Depending on the plant design, a different set of equipment may be required to provide protection from very small loss of coolant accidents such as those involving failure of the reactor coolant pump seal.

Grouping of initiating events

5.32. In order to limit the analysis required for the Level 1 PSA to a manageable size, a grouping process should be carried out before proceeding to the accident sequence analysis.

5.33. If, in order to further limit the PSA model to a manageable size, some initiating event groups are screened from consideration for inclusion in the model, the screening criteria established should be consistent with the purpose of performing the PSA, so that significant contributors to risk are not excluded. If screening is performed, it may still need to be revisited for specific PSA applications.

5.34. Initiating events should be arranged in groups in which all of the following properties of the initiating events are the same (or very similar):

(a) The accident progression following the initiating event;
(b) The success criteria for the ~~mitigating system~~credited systems;

(c) The effect of the initiating event on the availability and operation of ~~mitigating system~~credited systems, including the presence of conditions for signals that will actuate protection actions or block actuation of systems;
(d) The response expected from operating personnel.

5.35. The success criteria for the ~~mitigating system~~credited systems used for a specific group of initiating events should be the most stringent criteria for all the individual events within the group.

5.36. Where initiating events with slightly different accident progressions and/or success criteria for the ~~mitigating system~~credited systems have been grouped together, the accident sequence analysis should provide a bound for all the potential accident sequences and consequences of these initiating events.

5.37. The grouping of initiating events should be done in such a way that undue conservatism is not introduced into the analysis.

5.38. Initiating events that could cause a containment bypass (e.g. steam generator tube rupture or loss of coolant accidents in interfacing systems) should not be grouped with other loss of coolant accidents where the containment would remain effective.

5.39. The Level 1 PSA documentation should include a list of all the initiating events that have been identified for the plant and should provide a description of each initiating event and sufficient information on the method used to identify it, e.g. hazard and operability studies, failure mode and effects analysis, master logic diagram or review of operating experience.

ACCIDENT SEQUENCE ANALYSIS

5.40. The next step in the analysis is to determine the response of the plant to each group of initiating events (as identified in accordance with the foregoing procedure) that necessitates the operation of ~~mitigating system~~credited systems to carry out the safety functions to prevent core damage. Such safety functions typically include shutting down the reactor and keeping it subcritical, and removal of heat from the reactor core (see para. 5.46).

5.41. The events that are identified in the accident sequences will relate to the success or failure of the ~~safety systems~~SSCs and human actions taken in carrying out the safety functions required for the groups of initiating events. The ~~end point~~end states of the accident sequence models will correspond either to a safe stable state where all required safety functions have been successfully fulfilled or to core damage. Criteria should be developed for what constitutes the safe stable state[13].

Core damage

5.42. A criterion (or criteria, if appropriate) should be developed for what constitutes core damage or a particular degree of core damage.[14] For example, for light water reactors, it is often

[13] Several safe stable state can be specified (e.g. the hot standby, cold shutdown)

[14] Several core damage states can be specified, depending on the degree of the damage, for example, in channel type reactors, damage to different numbers of channels is usually considered depending on the severity of the consequences (i.e. for CANDU and RBMK type reactors the criterion is severe core damage and is defined as a condition where there is extensive physical damage of multiple fuel channels due to overheating leading to loss of the core structural integrity).

assumed that core damage occurs if any of the fuel parameters (such as the clad temperature) exceeds its design basis limit or a higher limit if this can be justified.

5.43. The specification of what constitutes core damage is often done by adopting an indirect criterion. For example, for a pressurized water reactor, core damage is assumed to occur following prolonged uncovery ~~exposure~~ of the top of the core or if a maximum specified cladding temperature is exceeded. If a significantly long time interval is required to cause core damage after uncovery ~~exposure~~ of the top of the core, then this should be taken into account in framing a realistic definition of core damage.

Safety functions~~, safety systems~~ and success criteria

5.44. The accident sequence analysis should be carried out for each group of initiating events, as identified in paras 5.32–5.39.

5.45. For sequences ending in a safe stable state, the accident sequence analysis should be pursued over a time period, ended with the sequence mission time, that will allow for considering the effect of long term measures to be put in place to ensure that the risk estimate beyond the sequence mission time is negligible and that possible cliff-edge effects are appropriately captured.

5.46. The safety functions that need to be performed to prevent core damage should be identified for each initiating event group. The safety functions required will depend on the reactor type and the nature of the initiating event and will typically include:

(a) Detection of the initiating event and reactor trip;
(b) Shutdown of the reactor and maintaining subcriticality;
(c) Heat removal from the reactor core;
(d) Maintaining the integrity of the primary circuit and the containment.

5.47. The ~~mitigating system~~credited systems and actions by operating personnel that will need to be available to perform each of these safety functions should be identified, along with ~~the~~ associated success criteria ~~for the mitigating systems used in performing these safety functions~~.

5.48. The actions by operating personnel that are necessary to bring the plant to a safe, stable state should be identified on the basis of plant procedures analysis. It is a good practice to specify operator actions in a cooperative effort between plant operators, systems analysts and human reliability analysts.

5.49. The success criterion should define the minimum level of performance for ~~mitigating system~~credited systems (including the systems with supporting functions, e.g. service water system, power supply systems) necessary to fulfil the safety function, taking into account the specific features of each sequence. Where redundant trains of the ~~mitigating system~~credited system are involved, the success criteria should be defined as the number of trains that are needed to remain operable~~need operate~~. Where ~~diverse~~ multiple ~~mitigating system~~credited systems are involved, the success criteria should take into account the performance needed from each of the ~~diverse~~ different systems. This could include partial operation of each of the ~~diverse~~ systems as supported by the safety analysis with level of details sufficient to provide acceptable justification.

5.50. The success criterion for each action by operating personnel should consider the time between the moment when based on available information the action can be initiated and the last moment the ~~when~~ action even correctly performed is able to lead to the successful system function required ~~no longer effective in terms of accident progression~~ (considering the time required for diagnosis and for action performance).

5.51. The systems that would fail as a result of the initiating event should be identified and taken into account in specifying the success criteria. These consist of systems and components that are credited for the mitigation of the initiating event. Examples of such cases are where the initiating event involves the failure of a support system, for example, the electrical power and cooling water systems, or where the initiating event produces a harsh environment in an area where equipment credited for mitigation of the initiating event, is located. In either case, this can lead to failure of the required systems. Another example arises in the case of a large or intermediate loss of coolant accident in a pressurized water reactor where, if the break occurs in a cold leg, the flow would be lost from the trains of the emergency core cooling system connected to that leg; this would need to be recognized in defining the success criteria.

5.52. The success criteria should specify the system mission time so that the reactor reaches a safe, stable state and that will allow for long term measures to be put in place to maintain this state, based on the sequence mission time defined in para. 5.45. In many cases, this has been taken to be 24 or 48 h for most initiating events. For ~~new~~ designs that provide the features to delay core damage (e.g. passive systems), consideration of a longer mission time may be necessary. ~~The mission time should be defined adequately for capturing possible cliff-edge effects and assuring that the residual risk accrued after the mission time is negligible.~~

5.53. The success criteria should define the actions by operating personnel that are needed to bring the plant to a safe, stable shutdown state as defined by the plant procedures. It is a good practice to specify these actions in a cooperative effort between by operating personnel, systems analysts and human reliability analysts.

5.54. The Level 1 PSA documentation should include a list of the safety functions, ~~mitigating system~~credited systems, support systems and actions by operating personnel that are necessary for each initiating event to bring the reactor to a safe, stable shutdown state.

Analysis to support the specification of success criteria

5.55. The success criteria for the ~~safety~~ credited systems ~~and the support systems used in the Level 1 PSA~~ should be justified by supporting analysis. Supporting analysis would include the thermohydraulic analysis for decay heat removal following transients and loss of coolant accidents, and neutronics analysis for reactor shutdown and hold-down. Supporting analysis should be based on the plant specific data (whenever possible), should conform to the best practice for using the computer code and should be independently reviewed.

5.56. Wherever possible, realistic success criteria that are based on best estimate supporting analysis should be defined and used in the Level 1 PSA [5].

5.57. However, if conservative success criteria that are based on conservative design basis analyses have been used in the Level 1 PSA for some of the ~~safety~~ credited systems in any accident sequence, this should be noted and the results of the overall analysis should be reviewed carefully to ensure that such conservatism does not dominate the risk and hence obscure insights from the Level 1 PSA.

5.58. This paragraph provides recommendations on meeting Requirement 18 of GSR Part 4 [3] on use of computer codes for a Level 1 PSA. The computer codes used to justify the success criteria should be well qualified to model the transients, loss of coolant accidents and accident sequences being analysed and to obtain a best estimate prediction of the results. The computer codes should be used only within their established realm of applicability and should be used only by qualified code users. Best estimate input data and assumptions that avoid unnecessary conservatisms should be used whenever possible [5].

Modelling of accident sequences

5.59. The accident sequences that could occur following each initiating event group should be identified. This can be done by constructing an event tree for each initiating event group, which models the success or failure of the ~~mitigating system~~credited systems, support systems and human actions in carrying out the safety functions. It is considered good practice to draw detailed event sequence diagrams, including human interactions, before constructing the event tree.

5.60. The event tree for the initiating event group should address all the safety functions that need to be performed and the ~~mitigating system~~credited systems that need to be operated as specified by the success criteria. The status of the front line ~~mitigating system~~credited systems (success or failure) for the initiating event group usually forms the headings for a particular event tree; this is sometimes referred to as the 'event tree top event'. The headings may also include any actions by operating personnel that directly affect the course of an accident, particularly actions to be taken in accordance with the emergency operating procedures. Any other event with a direct and significant effect on the sequence may also be used as a heading.

5.61. The structure of the event tree should take account of the time sequence of the headings on the event tree representing actions by operating personnel or actuation of systems. The most natural way is to order them chronologically, following the time sequence of the demands made on the systems or on the operating personnel.

5.62. The event tree structure should take into account functional and physical dependencies (see para. 5.90) that may occur as a result of equipment failures and human errors. Dependencies between ~~safety~~ credited systems (usually referred to as systems interactions) should also be represented on the event tree.

5.63. The accident sequence analysis should cover all relevant combinations of success or failure of the credited ~~safety~~ systems in responding to the initiating event group and should identify all accident sequences leading either to a successful outcome, where sufficient credited ~~safety~~ systems have operated correctly so that all the required safety functions for the initiating event have been carried out, or to a core damage state.

~~End point~~End states of accident sequences and plant damage states

5.64. The accident sequence analysis will identify accident sequences where all the required safety functions have been fulfilled in a satisfactory manner so that core damage will not occur, and accident sequences where one or more of the safety functions have not been fulfilled so that core damage is assumed to occur. This distinction will generally be sufficient if the analysis is to stop at a Level 1 PSA. However, if the intent is to use the results of the Level 1 PSA as input to a Level 2 PSA, it is general practice to group the accident sequences that lead to core damage into plant damage states, which will be a starting point for forming the interface

between the Level 1 PSA and the Level 2 PSA. It is more useful if the plant damage states are specified as a part of the Level 1 PSA (rather than postponing the specification of plant damage states to the first step of the Level 2 PSA). For example, for CANDU-type reactors, the different accident sequences representing the end states of the event trees are clearly defined as fuel damage categories (FDC) (e.g. FDC1, FDC2). Examples of fuel damage categories for CANDU-type reactors could be found in [13].

5.65. If a Level 2 PSA is being pursued, then a set of plant damage states should be defined that takes account of the characteristics of each accident sequence leading to core damage that could affect the containment response or lead to a release of radioactive material to the environment. Plant damage states should be specified by means of a cooperative effort between the Level 1 PSA analysts and the Level 2 PSA analysts.

5.66. The characteristics specified for the plant damage state are generally left to the discretion of the analyst, but would typically include:

(a) The type of initiating event that has occurred (intact primary circuit or loss of coolant accident);
(b) Failures of the credited ~~safety~~ systems (in the reactor protection system, residual heat removal system or emergency core cooling system) that have occurred, leading to core damage;
(c) The state of the primary circuit pressure (high or low) at the time of core damage;
(d) The time at which core damage occurs (early or late relative to the time of reactor trip);
(e) The integrity of the containment (intact, failed, isolation failure, bypassed due to a steam generator tube rupture or a loss of coolant accident at interfacing systems);
(f) Loss of coolant accident with or without pressure suppression capability (for boiling water reactors);
(g) The state of the pool (subcooled or saturated) when core damage occurs (for boiling water reactors);
(h) The availability of the containment protection systems (containment sprays, heat removal systems and hydrogen mixing or recombiners);
(i) The availability of AC and DC power and associated recovery times;
(j) The actions by operating personnel that have been attempted and failed.

The list above is appropriate ~~only~~ for a PSA for power operation~~;~~. The additional characteristics applicable ~~for~~ for shutdown states are provided in Section 9 (see para. 9.33)~~, a different set of characteristics will be appropriate~~.

5.67. The accident sequences leading to core damage should therefore be characterized in accordance with the general physical state of the plant to which each accident sequence leads and to the possible availability of the credited ~~safety~~ systems that could prevent or mitigate a release of radioactive material.

5.68. The Level 1 PSA documentation should present the event trees that have been drawn to determine how the accident sequences progress and should give a description of the logic behind the event tree structure. This is important since the event tree diagram itself provides no reasoning, only the results of reasoning, and hence cannot be understood completely without reference to an accompanying text.

5.69. The documentation should provide explanatory information for the headings in the event tree. For example, an event tree heading may represent a simple function, or it may represent a compound event (where more than one function is included under one heading). Assumptions made in the development of the event tree and the corresponding definition of the headings should be clearly presented and justified.

5.70. The documentation should also describe the plant damage states and should give a description of how they have been specified.

SYSTEMS ANALYSIS

5.71. The next step in the analysis is to model the system failures that are identified in the accident sequence analysis. If this is done by means of fault tree analysis, then the top event of the fault tree is taken as the system failure state(s) identified by the event tree analysis. The fault trees extend the analysis down to the level of individual basic events, which typically include component failures (e.g. failures of pumps, valves, diesel generators), unavailability of components during periods of maintenance or testing, common cause failures of redundant components and human failure events that represent the impact of human errors.

5.72. The scope of the fault trees that need to be drawn depends on the size and complexity of the event tree; the fault tree will be less complex the more detailed the event tree is.[15]

Fault tree analysis

5.73. Where fault trees are used, they should be developed at a level of details sufficient to provide a logical failure model for all the ~~mitigating system~~credited system failure states identified by the event tree analysis.

5.74. The failure criterion that provides the top event of the fault tree for each safety ~~system~~ function should be the logical inverse of the accident sequence success criterion, as specified in paras 5.49–5.58. In some cases, more than one fault tree model may be necessary for the same ~~safety~~ credited system to address the success criteria specified for different initiating event groups or in different branches of the event tree, depending upon the sequence of events prior to demand for the system. This can be done by developing different fault tree models or by using logical switches (so-called ‘house events’) to disable or enable the appropriate parts of the fault tree model, depending on the success criterion.

5.75. The basic events modelled in the fault trees should be consistent with the available data on component failures. The component boundaries and component failure modes as modelled in the fault trees should be consistent with those defined in the data on the component failures. This is equally valid for both active and passive components.

5.76. The fault tree models should be developed to the level of significant failure modes of individual components (e.g. pumps, valves, diesel generators) and individual human errors and should include all the basic events that could lead, either directly or in combination with other basic events, to the top event of the fault tree. The level of the analysis is generally left to the

[15] Other techniques are possible and may be used for specific aspects of the PSA. However, the usual approach is to use a combination of event trees and fault trees and this approach is assumed to be used (see paras 5.4–5.6).

discretion of the analyst, but it should be consistent with the available data on component failures and the proposed applications of the Level 1 PSA.

5.77. The set of basic events to be modelled in the fault trees should be identified by means of systematic analysis (for example, by means of a failure mode and effects analysis that has been carried out as part of the design assessment to identify important component failure modes) and a review of actions by operating personnel supported by task analysis to identify potential human errors.

5.78. The fault tree model should include all the ~~mitigating system~~credited system components that are required to be operational, including support system components. It should also include passive components whose failure could affect the operation of the system~~lead to failure of the system~~, for example, undetected filter blockages and pipe leaks. The fault tree model should be developed in a way that ensures that the functional dependencies and component failure dependencies are taken into account explicitly. Omitting explicit modelling of these dependencies may significantly bias the results and underestimate the relative importance of the support systems.

5.79. The degree of resolution of the components in the fault tree should be sufficient to ensure that all the hardware dependencies can be modelled. For example, where the same system provides cooling water to a number of components, this cooling water system should be modelled explicitly. Available data on component reliability should also be taken into account in defining the level of resolution (reliability data may be available for a pump as a whole, but not for its constituent parts, such as rotating wheel, coupling, bearing). In addition, in defining the degree of resolution of the components in the fault tree, consideration should be given to insights required from the PSA in terms of the risk significance of plant equipment or of individual parts of equipment.

5.80. Where individual components are grouped together and a composite event is used to model their failure, it should be demonstrated that the failure modes of each component in the composite event has the same effect on the system as the composite event itself. In addition, all the composite events included in the model should be functionally independent, i.e. no individual component should appear in more than one composite event, or elsewhere as a basic event.

5.81. The fault tree models should take account of individual components or trains of equipment in the ~~safety~~ credited systems that may be taken out of service for testing, maintenance or repair in the course of the lifetime of the plant. Such components or trains of equipment should be identified and modelled explicitly in the fault tree analysis. This can be done, for example, by including basic events in the fault trees to represent component outages.

5.82. The way that the unavailability of systems due to testing and maintenance is modelled should be consistent with plant technical specifications[16] and testing and maintenance practices in the plant.

[16] In the modelling of maintenance outages, it is generally assumed that the plant is operated within the limiting conditions for operation specified in the technical specifications.

5.83. A system for uniquely coding or labelling each of the logic gates and basic events in the fault tree models should be developed and this system should be used consistently throughout the complete logic model developed for the Level 1 PSA.

5.84. The development of the model should be consistent with the proposed applications of the Level 1 PSA. For example, if the Level 1 PSA is to be used for a risk monitor application, the model should be symmetrical so that it explicitly models initiating events in all locations in which they can occur, including all primary circuit loops, all trains of the credited ~~safety~~ systems, and all running and standby trains of normally operating systems. The development of a symmetrical model will allow the importance measures calculated by the Level 1 PSA code to be used in a straightforward manner (see para. 5.178 for the examples of importance measures).

Required systems information

5.85. Functional descriptions should be produced for each of the ~~safety~~ systems credited ~~modelled~~ in the Level 1 PSA to ensure that there is a valid and auditable basis for the logic model being developed. Functional descriptions typically include the following:

(a) The function of the system;
(b) The system failure modes;
(c) The system boundaries;
(d) The interfaces with other systems;
(e) The operating state being modelled (for systems with more than one mode);
(f) The components that need to operate or change their state and their normal configuration;
(g) Whether the component operations are manual or automatic;
(h) The conditions that need to exist for automatic signals to be received by the components.

5.86. A simplified schematic diagram should be provided for each system which shows the system as modelled in the fault tree, including:

(a) All the system components modelled in the fault tree;
(b) The normal configurations of the components;
(c) The pipe segments or wiring segments connecting the components;
(d) The support system interfaces (e.g. power, electrical, cooling).

5.88. The functional descriptions and schematics provided for the credited ~~safety~~ system should provide a clear basis for development of the fault trees. The Level 1 PSA documentation should provide an explanation of how this information was used in the development of the fault trees.

ANALYSIS OF DEPENDENT FAILURES

5.89. Particular consideration should be given to the treatment of dependencies in the logic model developed for the Level 1 PSA since, in PSAs carried out in the past, dependent failures have often been found to be one of the dominant contributors to the core damage frequency.

5.90. There are four different types of dependency that can occur:

(a) Functional dependencies include dependencies resulting from plant conditions, for example, failure to depressurize leads to unavailability of low pressure injection, and

dependencies due to shared components, common actuation systems, common isolation requirements or common support systems (e.g. power, cooling, instrumentation and control, ventilation).

(b) Physical dependencies (also referred to as spatial interaction dependencies) due to an initiating event that can cause failure of ~~mitigating system~~credited system equipment. This can occur due to pipe whip, missile impact, jet impingement or environmental effects.

(c) Human interaction dependencies due to errors made by the plant staff that either contribute to, or cause, an initiating event, or lead to the unavailability or failure of one or more items of ~~mitigating system~~credited system equipment so that they do not operate when required following an initiating event.

(d) Component failure dependencies due to errors in design, manufacture or installation or errors made by plant personnel during plant operation. These are addressed by a common cause failure analysis (see paras 5.95–5.98).

5.91. A systematic review should be carried out of the design and operation of the plant to identify all the potential dependencies that could arise, leading to the unavailability of ~~mitigating system~~credited system components or a reduction in their reliability in providing protection against initiating events.

5.92. All functional and physical dependencies should be modelled explicitly in the event tree or fault tree model. Human interaction dependencies and component failure dependencies should also be modelled; these are discussed further in paras 5.99–5.124 on human reliability analysis and paras 5.95–5.98 on common cause failure analysis.

5.93. All the functional dependencies that could arise within systems should be taken account of in the fault tree model. These should be identified and modelled explicitly in the fault tree analysis. It is good practice for the analysts to tabulate all these dependencies in a matrix of system dependencies, which can be used as a basis for constructing the fault trees and which is helpful to the reviewers in checking them. Functional dependencies should not be included among the component failure dependencies in the common cause failure probabilities of the system. Rather, component failure dependencies are reserved for the more uncertain dependencies that have not been explicitly identified and that are quantified by means of beta factors and similar models.

5.94. The intersystem functional dependencies that could arise due to shared components or support systems should be identified and modelled explicitly in the fault tree analysis. In the linked event tree approach (see para. 5.5), intersystem functional dependencies can be addressed using the boundary condition method. Such dependencies could arise in separate ~~mitigating system~~credited systems that perform the same safety function or in associated support systems. These need to be included explicitly in the fault trees.

ANALYSIS OF COMMON CAUSE FAILURES

5.95. The sets of redundant equipment where component failure dependencies could arise should be identified and included in the Level 1 PSA model for the common cause failure of these components. There are a number of methods available for modelling common cause failure in a Level 1 PSA and the method chosen should be supported by the collection of data. Addressing both intra-system and inter-system common cause failure events is considered a good practice.

5.96. The common cause failures that can affect groups of redundant components should be identified and modelled using the appropriate features of the PSA software. This is often done in the fault trees. The analysis should identify all the relevant component groups and the important failure modes. Any assumptions made concerning the defences against common cause failures should be stated in the Level 1 PSA documentation.

5.97. Justification should be provided for the common cause failure probabilities used for each of the component failure modes included in the Level 1 PSA. This should take account of the level of redundancy in the system, the design aspects of the components, the layout of the system in terms of the levels of separation, segregation and equipment qualification, and the operational, testing and maintenance practices for the system.

5.98. Where possible, the common cause failure probabilities should be based on plant specific data and take account of data from the operation of similar plants and generic data. If generic common cause failure parameters are to be used for the calculation of common cause failure probabilities, the applicability of these values should be analysed and justified. The component boundaries, failure modes and failure root causes in the generic data sources to be used should be consistent with those assumed in the PSA. If expert judgement is to be used for the assignment of common cause failure parameters (when neither plant specific data nor generic data are available), an appropriate justification should be provided for the data and error factors assigned should be commensurate with the uncertainty in the process of specifying the common cause failure parameters. One case for use of only generic data could be for the design of a new nuclear power plant.

HUMAN RELIABILITY ANALYSIS

5.99. The human errors that can contribute to the failure of credited ~~safety~~ systems should be identified and included in the logic models. A structured and systematic approach should be adopted for the identification of human failure events (HFE), the incorporation of the effect of such events in the plant logic model (event trees and fault trees) and the quantification of the probabilities of such events, i.e. human error probabilities. A structured and systematic approach will provide confidence that a comprehensive analysis has been carried out to determine the contributions to the frequency of core damage from all types of HFE. Given the high degrees of redundancy, diversity and reliability of credited ~~safety~~ systems typically incorporated in the design of current nuclear power plants, fault sequences involving human failure events leading to initiating events or failure to mitigate them often make a significant contribution to the core damage frequency. A useful starting point is to check the approach applied against one of the approaches generally used to ensure that all the necessary steps for a human reliability analysis are carried out.

5.100. The recommendations provided in paras 5.99–5.124 relate to the most common methods used in a Level 1 PSA [14]. The process for human reliability analysis should consist of the following four iterative steps:

1) Identification and definition of HFEs;
2) Qualitative assessment of HFEs;
3) Quantitative assessment of HFEs;
4) Integration into PSA model.

5.101. There is a wide variety of methods available for human reliability analysis and the state of the art in this area is still evolving. The method chosen should be applied and

documented consistently and correctly. When a human reliability analysis method is used outside of its original scope or is complemented or replaced by expert judgements, this process should be clearly documented with sufficient justifications to support an appropriate human reliability analysis process.

5.102. The aim of human reliability analysis should be to generate probabilities of human errors that are both consistent with one another and consistent with the analysis carried out in other parts of the Level 1 PSA.

5.103. The human reliability analysis should be carried out in close cooperation with the plant operating and maintenance staff to ensure that the analysis reflects the design features of the plant and its operation under operating states and accident conditions. If this is not possible (for example, if the analysis is to be carried out for a plant at the design stage), the analysts should use information from other, similar plants, or should clearly state the assumptions upon which their analysis is based.

Identification and definition of human failure events

5.104. A structured and systematic procedure should be applied for the identification of the human failure events that need to be included in the Level 1 PSA. This should include all types of HFE, as indicated in paras 5.105–5.108, where failures can make a contribution to the core damage frequency.

5.105. The human reliability analysis should include human failure events occurring before the initiating event that have the potential to lead to the failure or unavailability of SSCs important to safety (usually referred to as Type A human failure events). These can occur during repair, maintenance, testing or calibration tasks. If such errors remain undetected, the component or component groups affected will be unavailable when needed after an initiating event. Particularly important are failure events that have the potential to result in the simultaneous unavailability of multiple trains of credited ~~safety~~ systems. These sources of unavailability are included in the models at component, train or system level.

5.106. A systematic review of plant procedures should be carried out to identify the repair, maintenance, testing and calibration tasks carried out by operating personnel for the systems modelled in the Level 1 PSA and thereby to identify Type A human failure events. The review should determine the potential for HFEs to occur and the effect of these potential HFEs on the unavailability or failure of credited ~~safety~~ system equipment.

5.107. A systematic review of plant procedures should be carried out to determine potential human failure events that could lead to an initiating event (Type B human failure events). As a minimum, a check should be carried out to ensure that human failure events that could cause initiating events are taken into account in the evaluation of frequencies of initiating events used in the analysis.

5.108. A systematic review of plant procedures should be carried out to identify the critical actions that will need to be carried out by operating personnel after the occurrence of an initiating event (Type C human failure events). The review should determine the potential for HFEs to occur and the effect of these potential errors on the unavailability or failure of a component or system. Type C HFEs usually provide a significant contribution to the core damage frequency and hence are often the most important HFEs identified in the Level 1 PSA.

5.109. Significant errors of commission, i.e. incorrectly performing a required task or action, or performing an extraneous task that is not required and might lead to worsening the accident progression or cause an initiating event should be considered. ~~Errors of commission~~This consideration can lead to the creation of additional accident sequences. While it is not yet general practice to include errors of commission in the base case PSA, it is ~~advantageous~~ considered to be a good practice to use information on the general causes of errors of commission to reduce their potential ~~to~~(see for example, Ref. [14]). ~~to reduce the potential for introducing changes that could increase the likelihood of, or create conditions conducive to, errors of commission.~~

5.110. Repair~~s~~ action~~s~~ (e.g. the replacement of a motor on a valve so that it can be operated) should be credited in PSA only if there is strong justification for their feasibility. Human Reliability Analysis (HRA) techniques cannot be always used for repair actions since the method of repair is case dependent. It might be possible to credit repair actions if the specific failure mode of the equipment is known for the specific sequence and (i) it is possible to quickly diagnosed the failure, (ii) the spare parts and repairing personnel are in place, and (iii) the time window is sufficiently long to credibly assume possibility for repair, including the time needed to bring spare part and repairing personal to the plant. Recovery is defined in the PSA context as a restoration of a function lost as a result of a failed SSC by overcoming or compensating for its failure. Recovery can be handled by the operating personnel as distinction from repair. The appropriateness of the recovery and repair actions should be documented.

5.111. Actions that are "heroic" (e.g. ~~if~~ operating personnel need to enter an extreme high-radiation environment to perform the action) or that are performed without any procedure guidance or are not trained on, should not be included or credited in the analysis. Exceptions may be justified, but this should not be normal practice.

5.112. Assessment of human reliability in the context of deploying portable equipment should follow the same principles as generally in human reliability analysis. If the applied human reliability analysis method does not originally address all key human performance factors relevant to deploying portable equipment, the method should be adapted and complemented in a way that these performance factors are taken into account.

Qualitative assessment of human failure events

5.113. The qualitative assessment of HFEs should include the collection, analysis and documentation of information that is relevant for analysts to understand the personnel tasks enveloped in the HFEs subject of the specific human reliability analysis.

5.114. Information collection should consider relevant sources including the following when applicable:

(a) Procedural guidance;
(b) Visits at relevant plant locations;
(c) Reviews of operating experience;
(d) Interviews, talk-throughs, and walk-throughs with operating personnel;
(e) Information on the performance of operating personnel in the plant simulator;
(f) Thermohydraulic analyses;
(g) Other parts of the PSA, typically systems analysis notebooks and accident sequence analyses.

5.115. Qualitative assessment should lead to a characterisation of human failure events so that the quantification and modelling can be performed in an adequate manner. This is usually achieved by the following main activities:

(a) Task analysis to achieve detailed understanding of the activities required to meet the success criteria associated to the HFE;
(b) Context characterisation to characterize the scenario and the performance conditions defining the personnel activities covered by the HFEs, e.g. timing constrains, procedural guidance, relevant cues;
(c) Error identification to identify the cognitive and manual activities that would result in the HFE;
(d) Error characterisation to determine, justify, and characterize the potential and mechanisms for recovering from the identified error.

These activities of the qualitative assessment are valid for all types of HFE (A, B, C) and for all areas of PSA [14].

5.116. For newly designed NPPs most of the sources for qualitative information listed in para. 5.115 might not be available. In ~~these~~ such cases, the information for similar plants should be used~~, if available~~. If this is not ~~available~~possible, then the expert judgement should be used for items listed above. In any case, later the correspondence of qualitative information to plant actual status should be verified and PSA should be updated, ~~if~~ as needed.

Quantitative assessment of human failure events

5.117. The human error probabilities derived should be scenario specific and should reflect the factors that can influence the performance of operating personnel, including the level of stress, the time available to carry out the task, the availability of operating procedures, the level of training provided, and the environmental conditions. These factors (often called 'performance shaping factors') should be identified by the qualitative assessment[17].

5.118. The method used for the derivation of the human error probabilities should be consistent with the methods generally used in PSAs or its use should be explicitly justified.

5.119. While the application of different quantification methods for different types of HFE, e.g. between types A, B and C, may be considered, the use of same human reliability analysis approach (human reliability analysis method or combination of methods) for the assessment of similar types of HFE is preferable to achieve a consistency in the analysis. If different approaches are used for the same type of HFEs the reasons for their selection should be documented.

5.120. The risk importance of HFEs should be evaluated to identify the need to perform a more detailed analysis of HFEs. Quantification of HFEs is often performed in two stages: 1) screening assessment applying a simple quantification model and 2) detailed assessment where more factors and a more detailed context characterisation is taken into account, mostly for the most risk-significant actions by operating personnel. In this approach, it should be ensured that

[17] It is recognized that the human error probabilities will also be influenced by the safety culture at the plant. However, at present there is no agreed way of taking account of safety culture in evaluating human error probabilities

the risk importance of HFEs are accurately characterized after the screening phase so that the risk significant HFEs needing more detailed assessments can be identified.

5.121. The assessment of Type C HFEs for internal and external hazards should include the following three cases:

(a) HFEs that are included in the Level 1 PSA for internal initiating events, but are also relevant for the internal or external hazard scenario. In this case, it should be checked whether there is a need to revise the assessment of performance shaping factors to consider ~~due to the fact~~ that it might be ~~harder~~ more difficult for operating personnel to implement actions than in the base case scenario (e.g. due to a higher stress level associated ~~with controlling the equipment remotely~~to the hazard context).

(b) HFEs that are relevant only for a specific hazard (e.g. firefighting using portable fire extinguishing devises). The methods to assess hazard specific HFEs may usually follow same principles as the other types of HFE.

(c) Undesired responses by operating personnel to spurious alarms and indications. ~~For the third case, m~~More information on identification and assessment of undesired actions by operating personnel can be found in Ref. [15].

Treatment of dependencies between human failure events

5.122. Identification of dependent HFEs should take place in all phases of the human reliability analysis process (identification, qualitative assessments, quantitative assessments, and integration of HFEs in the model). There are likely to be interdependencies between the individual HFEs included in the logic model. Such interdependencies could arise from the use of a common cue or procedural step, incorrect procedures, an incorrect diagnosis or an incorrect plan of action in carrying out response actions. Dependencies among human failure events in the same sequence, if any, can significantly increase the human error probability. Interdependencies between human failure events should be identified and quantified in the analysis.

5.123. All minimal cutsets or scenarios involving multiple human failure events should be identified[18]. The set of HFEs that are combined in the same minimal cutset or scenario should be reviewed to determine the degree of dependency between them; the human error probabilities used in the quantification of the model should reflect this degree of dependency.

Integration of HFEs in the PSA model

5.124. The impact of risk significant HFEs should be either incorporated as basic events in fault trees or used as event tree headings. Recovery type of HFEs may be also implemented during the post-processing phase of the quantification. The integration step should include a thorough examination of minimal cutsets to verify that HFEs have been incorporated correctly. This examination should include a step to identify combinations of HFEs which may require a dependency assessment (see paras 5.122-5.123).

OTHER MODELLING ISSUES

[18] Such minimal cutsets can be identified by setting the human error probabilities to a high value (e.g. 0.9) and recalculating the core damage frequency; the minimal cutsets involving multiple human failure events will then appear at the top of the list of minimal cutsets

Passive systems

5.125. Functional reliability assessment of passive systems being part of the safety functions (i.e., assessment of the failure probability of passive systems for performing satisfactorily their safety functions) should be considered in PSA. Paragraphs 5.125–5.131 deal with the passive systems incorporating moving fluids or expanding solid structures, direct action devices, or stored energy sources (i.e. passive systems of categories B, C, and D defined in Ref. [16]), that generally involve the use of one or more techniques such as expert judgement, validation, testing, and performance monitoring to demonstrate their reliability.

5.126. Reliability assessment of passive systems should address the specific passivity features, which can be rather different from the features of actively operating systems and components. The concepts of active and passive safety describe the manner in which engineered ~~safety systems, structures, or components~~SSCs function are distinguished from each other by determining whether there exists any reliance on external mechanical and/or electrical power, signals or forces. The absence of such reliance in passive safety means that the reliance is instead placed on natural laws, properties of materials and internally stored energy. Some potential causes of failure of active systems, such as lack of human action or power failure, do not exist when passive safety is provided. While individual processes are well understood, the combinations of these processes, which define actual performance of such systems, may vary depending on changes in the conditions of state, boundary conditions and failure or malfunctioning of components within the system, the circuit or the plant.

5.127. Assessment of reliability of passive systems should carefully consider failure mechanisms and events potentially affecting the environmental and other boundary conditions for system operation, such as the conditions that influence natural laws to effectively mitigate accident conditions, mechanical or structural degradation, including ageing effects, unique to passive systems ~~since passive safety is not synonymous with inherent safety or absolute reliability~~. For example, natural circulation may be impaired or prevented by non-condensable gases, blockage, wrong valve positions, impurities, corrosion, algae in tanks, maintenance errors or foreign objects in the system.

5.128. Assessment of reliability of passive systems should also consider the periodic testing and maintenance practices or planned procedures since such practices or procedures may have a significant influence on passive systems reliability. For instance, if it exists, the feedback from the periodic testing and maintenance may reveal any age-related material degradations or may demonstrate need to modify testing strategies.

5.129. The general approach for the reliability analysis of passive components and systems should be similar to other systems considered in PSA. The specific emphasis should be in gaining confidence that the system failure modes relevant to PSA ~~of the system~~ have been defined properly and that the associated failure probabilities have been assessed in a justifiable manner. This may require a development of a model-based approach to assess the reliability of a passive system [17] and/or use other techniques such as testing and expert judgement.

5.130. The reliability analysis of a passive system should include the following stages:

(a) System characterisation to define the mission of the system, associated accident scenarios, failure modes and success/failure criteria;

(b) System modelling to enable an evaluation of system performance in various conditions (system modelling is needed due to limited possibilities to evaluate the system performance experimentally);
(c) Validation of the system model to the extent practical;
(d) Identification of relevant parameters and sources of uncertainties in the system model and input data;
(e) Quantification of uncertainties (using available techniques to consider aleatory and epistemic uncertainties) to yield a reliability estimation for the system.

5.131. Failure of the passive component or system should be modelled in the analysis and the failure probability should be assessed. The modelling of the passive system should take into account the probability of failure to ensure its safety function and should use the standard fault tree modelling techniques to address component failures (e.g. failure of non-return or relief valves to open, pipework blockage, common cause failures), human errors in setting up the system and failure of initiation (if external initiation is required). The uncertainties in the supporting analysis should also be taken into account.

Computer based systems

5.132. Reliability assessment of computer based systems being part of the SSCs credited to ensure safety functions should be considered in PSA. Computer-based systems in this context are assumed to consider various I&C equipment with programmable modules~~,~~.

5.133. The scope and the approach for the reliability assessment of computer based systems should follow the risk ~~functional~~ importance of the systems from the PSA point of view. For instance, it ~~can~~ could be expected that if the reactor protection system and the reactor control systems or other high-risk importance systems are controlled by a computer based system, they may need a detailed analysis while the assessment of programmable components in other lower risk importance I&C systems may only require ~~be managed by treating the components~~analysis in a more simplified manner. Other acceptable simplified approaches for assessing the reliability of computer based systems could be adopted for modeling considering their architecture and their safety classification.

5.134. ~~The need to assess the reliability~~Reliability assessments of ~~the~~ operator interface systems ~~should~~usually ~~-~~consider ~~the~~other I&C system failure dependencies ~~with other I&C systems whose~~through normal PSA fault tree and event tree modelling, which cascade failures ~~are relevant for the considered actions by operating personnel. In any case,~~of systems credited earlier in a accident sequence routinely. The operator and correlated operator interface system interdependencies between different I&C systems should be considered. ~~for~~ For those programmable operator interface systems that ~~treated~~are modelled in a simplified manner, ~~a~~ justification should be provided for the ~~chosen limitation~~limitations in the analysis.

5.135. Reliability assessment of computer based systems should cover both hardware and software components of those systems. Modelling the reliability of computer based systems is a challenge, due to the fact that ~~From a PSA perspective, two specific challenges need to be considered in the reliability assessment of computer based systems. Firstly, the functional complexity of I&C systems poses challenges in defining to what extent and which level of details failures should be analysed and modelled in PSA. Secondly, a justifiable way to assess~~

~~the reliability of the~~ for the software modules ~~for which~~the standard statistical approaches have limited applicability ~~needs to be found~~.

5.136. As for any systems analysis, the first task for the reliability assessment of a programmable system should be to define the scope of the system and its PSA related tasks. Here, attention should also be paid to system tasks which, if spuriously actuated, can have adverse effects on some safety function. In addition, the interactions between the I&C systems should be analysed to define system dependencies for the considered system tasks.

5.137. The analysis of computer based systems should be sufficiently detailed to capture the functionally relevant failure modes of the systems and to capture the dependencies between systems. Both the failure mode "failure to actuate certain I&C function" and "spurious actuation" should be considered. The required level of details is dependent on the I&C architecture and the implemented fault tolerant features in the systems. Therefore, it may be necessary to perform a detailed functional analysis of failures, including common cause failures, to come to a conclusion what the sufficient level of details is. ~~Typically, with regard to the failure mode "failure to actuate certain I&C function", a simplified approach may be sufficient while for the assessment and modelling of spurious actuations quite detailed analysis may be required.~~ When more simplified models are used, they should include at a minimum, the ~~principle~~ major failure modes identified by the hazard analysis used in the development of the system [18].

5.138. In the analysis of programmable components (processors, communication modules, sensors, actuators, other devices), the starting point should be to consider both hardware and software parts of the components (modules, sub-components), and to further decompose hardware and software into smaller details if so needed and if data are available. For some components a decomposition into hardware and software is not necessary if relevant failure modes and dependencies can be covered jointly. However, such a simplified approach is not necessarily feasible when hardware and software modules have different failure modes, failure detection means, functional failure impacts or common cause failure groups. The reliability analysis of programmable components should include an assessment that provides a justification for selected level of details of components' analysis. Reference [18] provides an example failure modes taxonomy for digital I&C systems.

5.139. ~~Before a hardware or software modelling technique is chosen, t~~The analysis should confirm that dynamic interactions between a plant system and the plant's physical processes, (i.e. the value of process variable), and interactions within a computer-based system (e.g. communication between different systems, multi-tasking, multiplexing) including interaction between hardware and software have been addressed in PSA model for the programmable components. If the dynamic interactions have not been addressed a rationale for not modelling them should be provided.

5.140. The reliability of the hardware modules should be assessed using standard techniques, if these techniques can model system behaviour, failure modes and dependences identified.

5.141. The reliability assessment of software modules should include an assessment of existing operating experience (also from other NPPs or other applications) and the development process (including validation and verification process) to gain as reasonable confidence as possible for the provided reliability estimates~~. For the reliability assessment of software modules, several approaches have been developed and tried out in the literature, research and~~

~~development projects and PSA projects, e.g. statistical testing, reliability growth model, fault injection method, expert judgements based on the assessment of the quality of validation and verification process and software complexity, assessment of operating experience [19]. Depending on the type of the software module (e.g. operating system, application software) and considered failure mode, the applicability of the method varies but in practice all methods have limitations to produce a well-justifiable number as ideally expected in PSA. This should be taken into account in the use of PSA in risk-informed applications~~. For the reliability assessment of software modules, several approaches have been developed and tried out in the literature, research and development projects and PSA projects, e.g. statistical testing, reliability growth model, fault injection method, expert judgements based on the assessment of the quality of validation and verification process and software complexity, assessment of operating experience[19] [19].

5.142. ~~*Use of expert judgement may become necessary to modelling computer-based systems for software systems. Similar to other areas in PSA such as use of expert judgment is an acceptable approach. If applied, the expert judgement approach should imply proper consideration of the quality of production of the software, that is whether adequate procedures followed to minimize the likelihood of errors being made in the production of the software, whether adequate checks have been made to detect errors in the code (static analysis) and whether adequate testing has been carried out for the completed code (dynamic testing).*~~ *---removed---*

5.143. The treatment of the recovery actions taken for loss of programmable system functions, should be coordinated with HFE models of the main control room design, minimum alarms and controls inventory. If recovery actions are credited to back-up the loss of programmable system functions, possible dependencies with the loss of instrumentation should be taken into account.

5.144. The reliability analysis of programmable systems should include an assessment of intersystem common cause failures, including communications networks. This is relevant, for instance, when a control and protection system or two diverse systems carrying out the same safety function are both computer based systems, consideration should be given to whether there are any dependencies in the hardware and software of the two computer systems and, if so, this should be taken into account in the Level 1 PSA.

5.145. Uncertainties in the modelling of programmable systems and data should be addressed. It is expected that the modelling uncertainties will be significantly higher for the analysis of computer based systems than other systems, because of the lack of knowledge of detailed failure modes, system interactions and/or hardware software interactions. These modelling uncertainties should be identified and at least qualitatively addressed. Data uncertainty should also be addressed.

5.146. As stated in Ref. [20], insights gained from PSA should be considered in the design of I&C systems. Derivation of ~~Any reliability claims for~~ I&C systems reliability should be substantiated and use internationally recognised approaches. Assumptions should be

[19] Depending on the type of the software module (e.g. operating system, application software) and considered failure mode, the applicability of the method varies but in practice all methods have limitations to produce a well-justifiable number as ideally expected in PSA. Significant uncertainty in identification of failure modes, modelling dynamic interactions and data have been noted [19]. This needs to be taken into account in the use of PSA in risk-informed applications.

documented and justifiedshould be within justifiable limits. In this respect, IAEA Safety Guide SSG-39 on Design of Instrumentation and Control Systems for Nuclear Power Plants [20] points out that practices differ in Member States. Some Member States expect quantitative estimates of probability of I&C systems due to hardware and software failures. For other Member States, design errors (including software errors) and their consequences are adequately treated only by qualitative analyses of the architecture and of the design. Some Member States, that apply numerical reliability to software, have established numerical limits to software reliability claims. It may be expected that the practices of Member States will evolve over time.

DATA REQUIRED FOR A LEVEL 1 PSA

5.147. Paragraphs 5.147–5.166 provide recommendations on the data for initiating event frequencies, component failure probabilities, and component outage frequencies and durations. The data for common cause failure probabilities and human error probabilities are discussed in paras 5.95-5.98 and 5.99-5.124, respectively. The recommendations for meeting Requirement 19 of GSR Part 4 [3] on use of operating experience data are also provided in paras 5.147–5.167166.

5.148. One of the main issues that needs to be addressed is whether the available data are applicable to the design of the equipment and the operating regime of the plant in question if plant specific experience is limited or absent.

5.149. Plant specific data should be used whenever possible, supplemented by data from similar plants, if it can be shown that this is relevant, since this will provide a broader source of data. However, plant specific data will not be available for a design PSA, for new plants or for plants that have only been in operation for a relatively short time. In this case, data from similar plants should be used, and if this is not available, generic data from the operation of all types of nuclear power plant should be used.

5.150. If the available operating data do not indicate the occurrence of failures, the initiating event frequencies and component failure probabilities assigned should be justified.

5.151. Justification should be provided for the data to be used for the Level 1 PSA. In providing this justification, it is good practice to compare data from a number of different sources and determine whether any differences can be explained. In general, a judgement will need to be made in selecting the best data source.

5.152. If a combination of plant specific data and generic data from different sources is to be used, justification should be provided for the methods used for selection of the specific data or for amalgamation of data from more than one source. This can be done using a Bayesian approach or by engineering judgement.

5.153. For initiating events with a low frequency of occurrence or for equipment with a low probability of failure, the data will be sparse or non-existent, even on a generic basis, and the values to be used in the Level 1 PSA will then have to be assigned by informed judgement. The reasoning on which such judgements are based should be explained.--- removed---

Frequencies of initiating events

5.154. A frequency should be assigned to each initiating event group modelled in the Level 1 PSA. The frequency for the initiating event group should be the sum of the frequencies for all the individual initiating events assigned to that group. ~~In determining this frequency, account should be taken of all the causes identified for the initiating event.~~

5.155. In addition to the techniques mentioned in paras 5.147–5.153, another way of assessing the frequencies of initiating events is by using a fault tree that provides a logic model of all the equipment failures and human errors that can combine and lead to the initiating event. It should be checked that the predictions yielded by the fault tree are consistent with operating experience. If the results obtained from the fault tree analysis are inconsistent with operating experience, these results should be reconsidered in light of the intended applications of the Level 1 PSA.

5.156. The frequencies assigned for frequent initiating events should be consistent with the operating experience from the plant under consideration and if relevant, from similar plants.

5.157. ~~*The frequency should be calculated for the initiating event groups. The frequency for the initiating event group should be the sum of the frequencies for all the individual initiating events assigned to that group.*~~ *---removed---*

5.158. The Level 1 PSA report should give a description of each initiating event identified for the plant along with the mean value for the initiating event frequency, the justification for the numerical value assigned to it and an indication of the level of uncertainty.

Component failure probabilities

5.159. Failure probabilities should be assigned to each of the components or types of component included in the analysis. Determination of failure probabilities should be consistent with the type of component, its operating regime, the boundaries defined for the component in the Level 1 PSA model and its failure modes.

5.160. Justification should be provided for the numerical values for the component failure probabilities used in the quantification of the Level 1 PSA.

5.161. For components such as pumps that are needed to operate for some time post-trip, the mission time should be specified. Determination of component mission times should be defined on the basis of the system mission time defined through accident sequence analysis as defined in para. 5.52.

5.162. The Level 1 PSA documentation should present all the component failure data used in the quantification of the Level 1 PSA. The documentation should include a description of the component boundaries, the failure modes, the mean failure probability, the uncertainties associated with the data, the data sources used and the justification for the numerical values used.

5.163. For the parameters used in the Level 1 PSA, not only a point estimate but a full uncertainty distribution should be derived, as these are necessary for the uncertainty analysis.

Component outage frequencies and durations

5.164. The quantification of the Level 1 PSA should take account of the unavailability of components and systems for testing, maintenance or repair. The numerical values used for the

frequencies and durations for component outages should be a realistic reflection of the practices in use at, or planned for, the plant.

5.165. Wherever possible, determination of outage frequencies and durations should be based on plant specific data obtained from an analysis of the plant maintenance records and the records of component unavailability, supplemented by data from similar plants. If this is not possible, generic data or manufacturers' data can be used as long as justification can be provided that such data reflect plant operating practices.

5.166. The Level 1 PSA report should present the data on unavailability of components and should provide justification for the numerical values used.

QUANTIFICATION OF THE ANALYSIS

5.167. The logic model developed in the Level 1 PSA should be quantified using the data indicated in paras 5.147–5.166. The accident sequence frequencies are then calculated using the data for the initiating event frequencies, component failure probabilities, component outage frequencies and durations, common cause failure probabilities and human error probabilities.

5.168. For the approach using a combination of ~~small~~ event trees and a ~~large~~ fault tree (the fault tree linking approach, see paras 5.4 and~~.~~ 5.5), Boolean reduction needs to be carried out for the logic models developed using event trees and fault trees for each initiating event group. Before quantifying the Level 1 PSA, care should be taken to ensure that no logic loops exist in the model. If such loops exist, breaking the loops is a prerequisite for quantification. The Level 1 PSA report should present the manner in which, and details of how, any logic loops in the model were broken.

5.169. Paragraphs 5.170 and 5.171 provide recommendations on meeting Requirement 18 of GSR Part 4 [3] on use of computer codes for a Level 1 PSA. The quantification of the Level 1 PSA is required to be carried out using a suitable computer code that has been fully validated and verified. A number of sophisticated Level 1 PSA computer codes that can be used to carry out this analysis are available commercially or have been developed in various Member States.

5.170. The users of the codes should be adequately experienced and should understand the uses and limitations of the code.

5.171. The overall results of the quantification of the Level 1 PSA model should include:

(a) Core damage frequency (point estimates and uncertainty bounds or probability distributions);
(b) Contributions to the core damage frequency arising from each of the initiating event groups;
(c) Minimal Cutsets and minimal cutset frequencies (for the fault tree linking approach) or scenarios and scenario frequencies (for the approach using event trees with boundary conditions);
(d) Results of sensitivity studies and uncertainty analysis;
(e) Importance measures (such as the risk achievement worth and the risk reduction worth for basic events) that are used for the interpretation of the Level 1 PSA;
(f) Frequencies of the plant damage states if they are defined to provide the interface between Level 1 PSA and Level 2 PSA.

5.172. The analysts should check that the accident sequences or minimal cutsets identified by the solution of the Level 1 PSA model do indeed lead to core damage in accordance with the assumptions made in the course of the development of the PSA. This check should be carried out for a sample of the sequences, focusing on those that make a significant contribution to the risk. In addition, a check should be made to confirm that the minimal cutsets representing combinations of initiating events and component failures that are expected to lead to core damage are indeed included in the list of minimal cutsets generated.

5.173. The analyst should provide a definition of the term 'a significant contribution to the risk' as used in para. 5.172. This could take the form of an absolute criterion or a relative criterion (e.g. relative to total core damage frequency).

5.174. A check should be made that any post-processing that has been carried out on the minimal cutsets to remove mutually exclusive events or to introduce recovery actions not included explicitly in the Level 1 PSA model has indeed produced the correct results. Post-processing is commonly used for the fault tree linking approach.

5.175. The Level 1 PSA documentation should present the results of the quantification of the Level 1 PSA and should describe the most significant sequences and minimal cutsets (for the fault tree linking approach) and any post-processing that has been carried out.

5.176. The analyst should provide definitions of the terms 'significant sequence' and 'significant minimal cutset' as used in para. 5.175. These could take the form of absolute criteria or relative criteria (e.g. relative to total core damage frequency).

5.177. For quantification of the Level 1 PSA, cut-offs will need to be specified to limit the time taken for the analysis. The usual approach is to set a frequency cut-off so that minimal cutsets with a lower frequency are not included in the analysis. (It is also possible to specify an order cut-off so that minimal cutsets with an order greater than a specified level are not included in the analysis.) Justification should be provided that the cut-off has been set at a sufficiently low level that the overall result from the Level 1 PSA converges and the cut-off does not lead to a significant underestimate of the core damage frequency. The choice of cut-off may vary depending on the application of the PSA.

IMPORTANCE ANALYSIS, SENSITIVITY STUDIES AND UNCERTAINTY ANALYSIS

Importance analysis

5.178. Importance measures for basic events, groups of basic events, ~~mitigating system~~credited systems and groups of initiating events, should be calculated and used to interpret the results of the PSA. Importance values used in Level 1 PSA typically include:

(a) The Fussell–Vesely importance[20];
(b) The risk reduction worth[21];

[20] For a specific basic event, the Fussell–Vesely importance measure is the fractional contribution to the total frequency of core damage for all accident sequences containing the basic event to be evaluated.

[21] The risk reduction worth is the relative decrease in the frequency of core damage if the probability of the particular failure mode is considered to be zero. The risk reduction worth is a direct function of the reliability of the equipment and can be used to assess the contribution of the failure mode to the core damage frequency.

(c) The risk achievement worth[22];
(d) The Birnbaum importance[23].

The various importance measures provide a perspective on which basic events, contribute most to the current estimate of risk (Fussell–Vesely importance, risk reduction worth), which contribute most to maintaining the level of safety (risk achievement worth) and for which basic events the results are most sensitive (Birnbaum importance). The importance values should be used to identify the ~~components and systems~~SSCs and actions from operating personnel that significantly contribute to risk and should be considered carefully at the design level or during the operation of the plant. The importance values should be used to identify areas of the design or operation of the plant where improvements need to be considered.

Types of uncertainty

5.179. Paragraphs 5.179–5.187 provide recommendations on meeting Requirement 17 of GSR Part 4 [3] on uncertainty and sensitivity analysis for a Level 1 PSA. It is recognized that there will be uncertainties in the models developed and in the data used in the Level 1 PSA. These uncertainties should be addressed when using the results of a PSA to derive risk insights or in support of a decision. This can be done by carrying out sensitivity studies or an uncertainty analysis, as appropriate. The uncertainties in the Level 1 PSA are normally classified into three general categories as follows:

(1) **Incompleteness uncertainty**: The overall aim of a Level 1 PSA is to carry out a systematic analysis to identify all the accident sequences that contribute to the core damage frequency. However, there is no guarantee that this process can ever be complete and that all possible scenarios have been identified and properly assessed. This potential lack of completeness introduces an uncertainty in the results and conclusions of the analysis that is difficult to assess or quantify. It is not possible to address this type of uncertainty explicitly.
(2) **Modelling uncertainty**: This arises due to a lack of complete knowledge concerning the appropriateness of the methods, models, assumptions and approximations used in the analysis. It is possible to address the significance of some of them using sensitivity studies.
(3) **Parameter uncertainty**: This arises due to the uncertainties in the parameters used in the quantification of the Level 1 PSA. This is the type of uncertainty that is usually addressed by an uncertainty analysis through specifying uncertainty distributions for all the parameters and propagating them through the analysis.

5.180. Consideration needs to be given as to how to use the uncertainty information in the design evaluation and decision making process. However, probabilistic safety goal or criteria for core damage frequency often relate to point estimates[24] rather than to uncertainty

[22] The risk achievement worth is the relative increase in the frequency of core damage if the failure of the particular item of equipment is considered to be certain. The risk achievement worth is a measure of the importance of the function performed by the equipment. It identifies the equipment playing a major role with regard to safety, even if the failure rate of such equipment is very low.
[23] The Birnbaum importance measure is a measure of the increase in risk when a component is failed compared with when the component is operating.
[24] In this context, a point estimate is meant to be either a point estimate usually calculated by a PSA computer code or another parameter or quantile of the probability distribution, such as the mean or median.

distributions. The way that the Level 1 PSA is used for the identification of weaknesses also relates to point estimates rather than to uncertainty distributions.

Sensitivity studies

5.181. Studies should be carried out to determine the sensitivity of the results of the Level 1 PSA to the assumptions made and the data used.

5.182. The sensitivity studies should be carried out for the assumptions and data that have a significant level of uncertainty and which are likely to have a significant impact on the results of the Level 1 PSA. The sensitivity studies should be carried out by requantifying the analysis using alternative assumptions or by using a range of numerical values for the data that reflect the level of uncertainty.

5.183. The analyst should provide a definition of the term 'significant impact on the results of the Level 1 PSA' as used in para. 5.182. This could take the form of a numerical criterion in an absolute or a relative form (see para. 5.173), a qualitative criterion (e.g. introduction of a new accident sequence), or a combination of both quantitative and qualitative criteria (e.g. introduction of a new significant accident sequence).

5.184. The results of the sensitivity studies should be used to indicate the level of confidence that may be placed in the insights obtained from the PSA, that is, whether the core damage criterion or target has been met, whether the design is balanced and whether there are possible weaknesses in the design and operation of the plant that have not been highlighted in the base case Level 1 PSA with which the sensitivity cases are compared.

5.185. It should be noted that sensitivity studies are usually carried out for one assumption or one parameter at a time and that the results of the sensitivity studies have no statistical significance. The sensitivity of relevant combinations of assumptions can also be analysed.

Uncertainty analysis

5.186. An uncertainty analysis should be carried out to determine the uncertainty in the results of the Level 1 PSA that arises from the data that have been used to quantify the Level 1 PSA.

5.187. Uncertainty distributions should be specified for the parameters used in the quantification of the Level 1 PSA. This should be done as part of the data analysis. These uncertainty distributions should be propagated through the analysis to determine the uncertainties ~~in frequencies of occurrence of initiating event groups, and~~ in the core damage frequency. These uncertainties should be used to provide an indication of the level of confidence that the risk criterion or target has been met.

~~5.187.~~5.188. Failure rate coupling should be considered in uncertainty analysis. This is to address the correlation of the data which have been derived from the same source and can be done by means of parameter sampling.

6. GENERAL METHODOLOGY FOR LEVEL 1 PSA FOR INTERNAL HAZARDS AND EXTERNAL HAZARDS

INTRODUCTION

6.1. Apart from random component failures and human errors (as discussed in Section 5) that may lead to internal initiating events, fault sequences may be caused by the damage imposed by other hazards. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 [3] for Level 1 PSA for other hazards, which can be categorized as follows:

(a) **Internal hazards** originating from within the site boundary and are associated with failures of facilities and activities that are under the control of the operating organization~~originating from sources located on the site of the nuclear power plant, both inside and outside plant buildings~~. The hazards caused by (or occurring at) different facilities at the same site are also considered to be internal hazards. Examples of internal hazards are internal fires, internal floods, internal explosions, ~~turbine~~ internal missiles (e.g. turbine), drop of heavy loads, ~~–~~on-site transportation accidents and releases of hazardous ~~toxic~~ substances from on-site storage facilities.

(b) **External hazards** include natural or human induced events that are originating outside the site boundary and outside the activities that are under the control of the operating organization, for which the operating organization has very little or no control. ~~originating from sources located outside the site of the nuclear power plant.~~ Examples of natural external hazards are seismic hazards, ~~external fires (e.g. fires affecting the site and originating from nearby forest fires),~~ external floods, high winds or severe weather conditions, examples for human induced hazards are aircraft crash, ~~and wind induced missiles,~~ off-site transportation accidents, releases of hazardous substances from outside the nuclear power plant site~~toxic substances from off-site storage facilities and severe weather conditions~~.

~~Such h~~Hazards including combined ones can damage the plant ~~components~~ SSCs and thus generate accident sequences that might lead to core damage (or to other undesired end states as appropriate, if these are to be considered in the Level 1 PSA). Often, ~~these~~ hazards have the potential to affect many ~~different pieces of equipment~~SSCs simultaneously and adversely impact plant personnel. Both internal and external hazards including their combinations should be included in the Level 1 PSA.[25]

Combinations of hazards cover combinations of external with other external hazards, external with internal hazards and internal with internal hazards. Combinations of hazards might have a significantly higher impact on plant safety than each individual hazard considered separately, and the occurrence frequency of hazards combinations may be comparable to that of the individual hazards, e.g. a severe storm may cause important ~~causes~~ precipitation together with simultaneous ~~and~~ dam failure ~~simultaneously~~ resulting in ~~extremely~~ high water level on the plant platform.

ANALYSIS PROCESS

[25] This Safety Guide does not provide recommendations relating to events originating from the impact of war or acts of sabotage or terrorism. However, consideration should be given to incidental hazards posed by military facilities or peacetime activities (e.g. crash of a military aircraft).

6.2. A consistent approach should be applied to the identification of internal and external hazards and the analysis of their contribution to core damage frequency. The main stages of the analysis of internal and external hazards typically include:

(1) Collection of initial information on internal and external hazards;
(2) Hazard identification, including single and combined hazards;
(3) Hazard screening analysis, both quantitative and qualitative;
(4) Bounding assessment;
(5) Detailed analysis.

The overall analysis approach is illustrated in Fig. 2.

6.3. While the stages of hazard identification and screening are similar for internal and external hazards, the bounding assessment and detailed analysis for each hazard may involve tasks that may be unique for the hazard considered, for example, fire propagation will need to be analysed in the case of internal fires. This section addresses the tasks of identification and screening of hazards, which are similar for internal and external hazards; specific recommendations on the bounding assessment and detailed analysis for specific hazards are provided in Section 7 for internal hazards and in Section 8 for external hazards.

6.4. All potential internal and external hazards that may affect the plant are required to be considered and should be subjected to screening analysis, bounding assessment or detailed analysis, as appropriate: see IAEA Safety Standards Series No. SSR-1, Site Evaluation for Nuclear Installations [21].

6.5. As explained in para. 5.168, in Level 1 PSA for internal initiating events, in order to eliminate logic loops, reduced fault tree models are developed by removing submodels representing random failures of components. For example, to eliminate the logic loop between service water and power supply, the links to fault trees of specific buses are removed. Dependent failures of these components (whose random failures have been eliminated from the logic model) resulting from damage due to internal and external hazards should be incorporated in the Level 1 PSA models for internal and external hazards.

COLLECTION OF INITIAL INFORMATION

6.6. At the starting point of Level 1 PSA for internal and external hazards, all available information specifically relating to the internal and external hazards should be collected. This information should include, at a minimum:

(a) Design information relating to internal and external hazards as considered in the safety analysis report;
(b) List and layout of plant buildings and SSCs;
(c) Plant layout and topography of the site and surroundings;
~~(c)~~(d) Environmental conditions, such as climate zone, meteorological characteristics;
~~(d)~~(e) Information on the location of pipelines, transportation routes (air, water, rail, road) and on-site and off-site storage facilities for hazardous (e.g. combustible, toxic, asphyxiant, explosive, corrosive) materials;
~~(e)~~(f) Location of industrial and military facilities in the vicinity of the site;

~~(f)~~(g) Historical information on the occurrence of any internal and external hazards at the site and in the region.

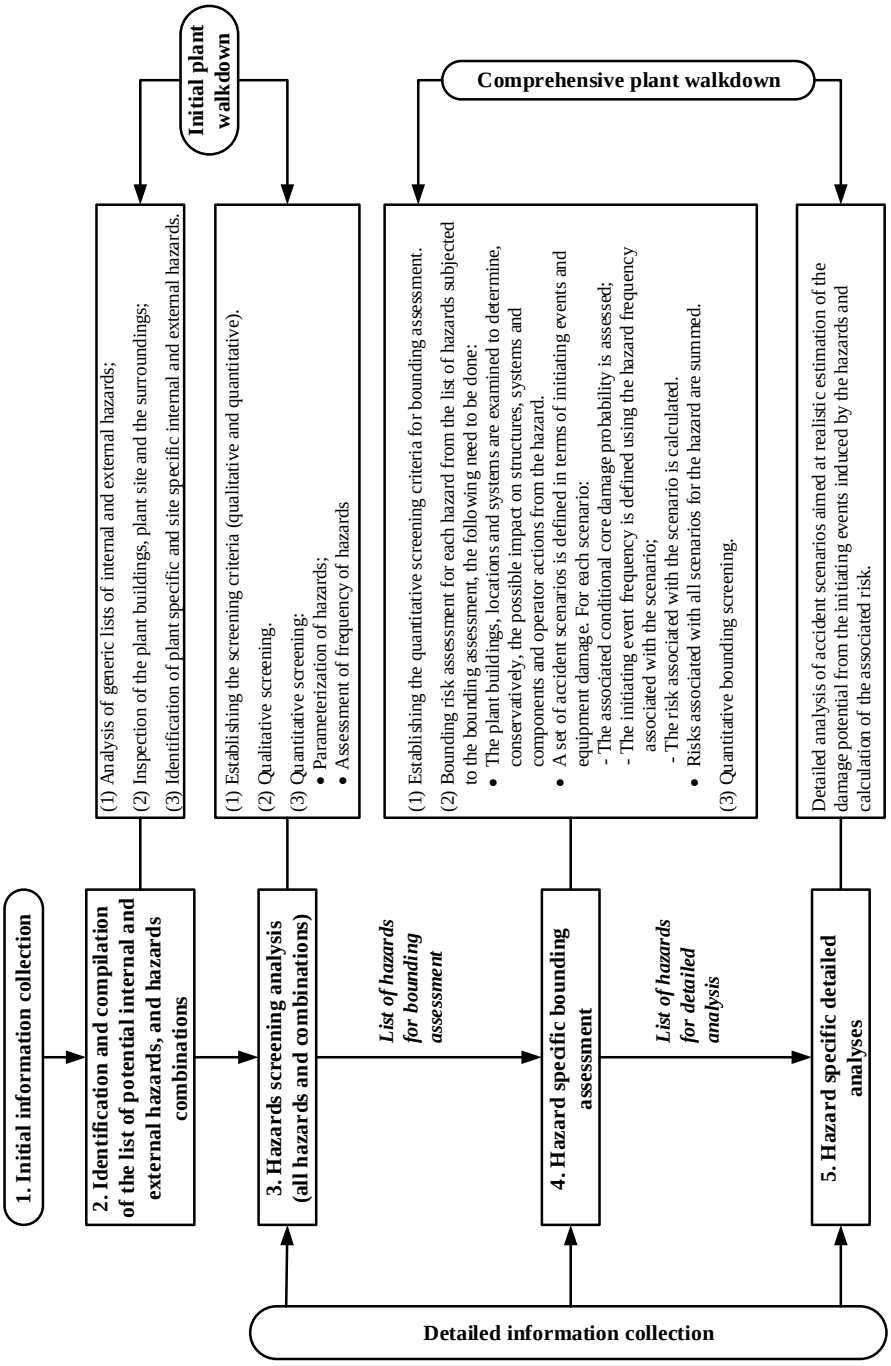

FIG. 2. Overall analysis approach for Level 1 PSA for internal and external hazards.

6.7. The initial information should be updated and expanded in the course of the internal and external hazards Level 1 PSA, depending on the necessary level of detail for the screening analysis, bounding assessment or detailed analysis for each hazard.

IDENTIFICATION OF HAZARDS

6.8. The task of hazard identification should aim to generate a comprehensive and traceable list of potential internal and external hazards. Examples of specific hazards and hazard groups are (see Refs [7, 21-25]):

Internal hazards ~~inside plant buildings~~:

(a) Internal fires;
~~(a)~~
(b) Internal explosions;
(c) Internal missiles;
(d) Pipe whip and jet effects
~~(b)~~(e) Internal floods;
(f) Heavy load drops;~~.~~
(g) High energy arcing fault;
(h) Electromagnetic interference;
(i) Release of hazardous substances inside the plant.
~~(c)~~(a) ~~Internal missiles;~~
~~Internal explosions;~~
~~(d)~~(a) ~~Heavy load drops.~~

External natural hazards:

(a) Seismic hazards;
(b) External fires;
(c) External floods[26] and other hydrological hazards;
(d) High winds[27];
(e) Biological phenomena[28]
(f) Extreme meteorological conditions[29]
(g) Extraterrestric phenomena;
(h) Geological phenomena;~~.~~
~~(f)~~(i) Solar storms.

[26] External floods is a hazard group that includes multiple hazards such as dam failure, tsunami, riverine flood, storm surge
[27] High winds is a hazard group that includes hazards such as tornado, hurricane/typhoon and straight wind.
[28] One example of biological phenomena is abnormal fish population in the cooling pond.
[29] According to Ref. [29], extreme meteorological conditions include extreme temperature, extreme atmospheric moisture, snow precipitation (also blizzards) and ice pack, and lightning. Other hazards may be connected to these, such as frazil ice, frost and hail.

External human-induced hazards:

(a) Aircraft crashes (accidental).
(b) Off-site explosions;
(c) Offsite transportation accidents;
~~(a)~~(d) Offsite industrial storage accidents;
(e) Accidental releases of hazardous substances~~Off-site toxic substance releases~~;
~~(b)~~(f) Off-site human-induced fires
~~(a) Aircraft crashes.~~

6.9. As a starting point, the hazards listed in various publications (e.g. see Refs [26-28] and Annex I) and examined in past studies should be included in the list and systematically reviewed in terms of their applicability to the site. Annex I provides an example of a generic list of potential internal and external hazards.

6.10. The generic list should be complemented by additional site or plant specific hazards, if any exist. The identification of these site or plant specific hazards should be performed in a systematic, structured framework to ensure completeness. For existing plants, an integral part of the process of identification of internal and external hazards should be a dedicated site survey and plant/site walkdown.

6.11. A list of potential combined hazards that may be significant for risk should be developed. In this context, combined hazards ~~are defined as follows~~includes three types of hazard combinations described in [6]: consequential (subsequent), correlated and unrelated (independent), see [6] for more detailed description~~:~~.

~~(a)~~ For consequential hazards combinations the assessment of consequences of hazards should be part of the assessment of the primary hazard. ~~Consequential Hazards (i.e. causally connected hazards): The case when one of the hazards (i.e. the primary hazard), may result in one or more consequential, or secondary hazards (which may be internal or external), due to a direct relationship between the primary and secondary hazard(s) are to be specifically addressed in the assessment for the primary hazard. For example, the following hazards are not considered combined hazards but need to be addressed explicitly as an additional plant impact from primary hazard in PSA model (see Section 8):~~
~~An earthquake could result in a tsunami;~~
~~An earthquake could result in a seismically-induced internal fire or internal flood;~~
~~high winds can generate missiles.~~

~~(b) Correlated Hazards: External hazards occurring as a consequence of a single underlying cause, in which case they can be assumed to be correlated. The underlying cause could be either internal or external. In this case the degree of correlation may range from low to high and needs to be identified on a case by case basis. For example:~~
~~high sea water levels and transportation accidents caused by high wind;~~
~~extreme rain and lightning triggered by extreme meteorological conditions;~~
~~extreme low temperatures and heavy snow load caused by winter meteorological conditions.~~

~~(c) Coincidental Hazards: External hazards occurring simultaneously without a common mechanism as combination of independent phenomena. For example:~~
~~a seismic event during extreme cold weather conditions;~~

~~— high winds occurring during extended flooding conditions at the site.~~

6.12. ~~Consequential hazards should be included in the assessment of the primary hazard, while c~~Correlated and ~~coincidental~~ unrelated ~~external~~ hazards combinations should be included in the hazard identification process for combined hazards.

6.13. Combinations of ~~Coincidental~~ unrelated ~~external~~ hazards ~~combination~~ should consider the duration of the impact of individual hazard~~s~~s in the combination (e.g. a seismic event during a long drought period, a plant internal fire during a long-lasting external flooding). ~~Combined coincidental hazards are normally limited to two.~~

6.14. The potential combined hazards should be identified starting from the list of individual internal and external hazards applicable to the site. The entire list of applicable hazards should be used for this purpose before any screening analysis is carried out [30]. ~~Usually, combined hazards involve only natural hazards (e.g. a combination of high wind and high sea water level). However, combinations of natural hazards and/or human-induced hazards are also possible and cannot be excluded a priori (e.g. an increased risk of ship accidents during severe weather conditions).~~

6.15. The combination of mutually exclusive hazards should be excluded.

SCREENING OF HAZARDS AND HAZARD COMBINATIONS

6.16. A successive screening process is generally established to minimize the emphasis on internal, external hazards and hazard combinations identified in accordance with para. 6.11-6.13 whose significance to risk is low, and to focus the analysis on hazards that are risk significant. The successive screening process should be based on clearly defined screening criteria and consistently applied to ensure~~s~~ that none of the significant risk contributors from any internal, external hazard and hazard combinations relevant to the plant and the site are omitted. The screening criteria and the screening process should be included in the documentation of the Level 1 PSA along with the results from the screening process.

6.17. When qualitative screening criteria are used, either individually or in combination, for single or combined hazards it should be confirmed that:

(a) The hazard will not lead to an initiating event. For external hazards, this criterion is generally applied when the hazard cannot occur close enough to the plant to affect it, or when critical components are not impacted (e.g. an ~~internal~~ external flooding scenario that does not generate an initiating event). Satisfaction of this criterion will also depend on the magnitude of the hazard.
(b) The hazard will be slow to develop, and it can be demonstrated with high confidence that there will be sufficient time to eliminate the source of the threat or to provide a reliable and adequate response.
(c) The hazard is included within the definition of another hazard or the hazard combination is included in the definition of the more severe hazard.

[30] Usually, combined hazards involve only natural hazards (e.g. a combination of high wind and high sea water level). However, combinations of natural hazards and/or human-induced hazards are also possible and cannot be excluded a priori (e.g. an increased risk of ship accidents during severe weather conditions).

(d) ~~The hazard has a significantly lower mean frequency of occurrence than other hazards with similar character and will not result in consequences that are worse than those from other such hazards. The uncertainty in the frequency estimate for a hazard screened out in this manner and cumulative impact of all screened out hazards are judged as not significantly influencing the total risk.~~

(e) The impact of the combined hazard is not more severe than the effect of the more severe hazard in the combination.

6.18. Quantitative screening criteria applied to hazards should depend on the overall objective of the Level 1 PSA and should correlate with the overall core damage frequency (typically obtained based on full scope PSA). Hazards of very low frequency but with potentially severe consequences in terms of releases of radioactive material should be considered for the purposes of a Level 2 PSA.

6.19. ~~None of the criteria listed in para. 6.17 are applicable to internal hazards that originate inside plant buildings. These hazards should not be screened out as an entire hazard category and should always be the subject of either bounding or detailed analysis.~~ --- *removed* ---

6.20. The most important parameters relating to the damage potential of the internal and external hazards should be specified. Several parameters should be specified if the damage potential of a hazard cannot be limited to consideration of a single parameter. All parameters specified for the hazards should be taken into account in performing the screening analysis (e.g. water level and pressure from the flow).

6.21. The following external hazards should not be screened out as an entire hazard ~~category~~class:

(a) Seismic hazards;
(b) Wind hazards;
(c) External floods;
~~(c)~~(d) Human induced hazards.

6.22. In order to eliminate specific hazards from ~~the high wind~~ a given hazard class~~category~~, it should be proven that the ~~climatic~~ conditions specific to the location of the plant (topographic, geographic, meteorological, biologic) support the assumption that these hazards are not sufficient to damage the plant (e.g. hurricanes in a non-coastal area).

6.23. External hazards ~~Wind hazards~~ with a certain potential for damage should be screened out only when it is demonstrated that the frequency of exceedance of a particular ~~wind velocity~~ magnitude is negligible or when uncertainties in hazard frequency are so large that they prevent any valuable insight to be driven. ~~The combination of wind with other hazards, such as rainfall or flooding, should be considered. When screening is performed, it is necessary to include in the analysis the possibility of objects being picked up by the wind (mainly in the case of tornadoes and hurricanes) and turned into missiles.~~

~~*6.24. For* --- *removed* --- *the screening process for external flood hazards, the following should be taken into consideration:*~~

~~*6.25. The location of the nuclear power plant with respect to distance to a river, sea or lake, and the possibility of any flood reaching the site.*~~

~~*6.26. The warning time[31]:*~~

~~*6.27. This can be long enough to allow shut-off operations in plants located at river sites (e.g. more than one day in advance).*~~

~~*6.28. For plants located at coastal sites, in general, the warning time is shorter and may sometimes be only a matter of hours or minutes in the case of a local tsunami.*~~

~~*6.29. In addition to the warning time, the time dependent likelihoods of success in receiving the warning and of the success of potential preventive actions should also be considered.*~~

~~*6.30. The type of structure in place for retaining water.*~~

~~6.31.~~6.24. ~~*It is possible that other, adjacent areas will be inundated as the flooding occurs and that the flood level will be higher than expected. A plant at the edge of a narrow flood plain is more likely to be flooded than a plant located in a wide delta area.*~~

~~6.32.~~6.25. For each ~~internal hazard originating outside the plant buildings and for each external~~ individual hazard, an approximate maximum impact that could occur, given pessimistic assumptions about events subsequent to the initiating accident, should be determined and should be used in the screening process.

~~6.33.~~6.26. When the screening criteria cannot be applied to the hazard as a whole, but can be applied to the hazard with a certain magnitude, the hazard as a whole should be divided into ~~subcategories~~ subclasses and screening criteria applied to each ~~subcategory~~subclasses, so as to avoid screening out hazards with low frequency but high potential for damage.

~~6.34.~~6.27. Initiating events occurring at the plant may be the result of the impact of a single hazard or a combination of two or more hazards. While using the screening criteria, it should be justified that hazards whose combined impact can result in significant consequences are not excluded from further consideration, even though each of them, considered independently, would make a negligible contribution to risk.

~~6.35.~~6.28. A periodic review of the actual status of the plant and the surroundings should be performed while applying screening criteria, in order to verify that changes in the original design conditions are not significant or are taken into account in the PSA. In particular, changes that have the potential to cause new hazards or to lead to an increased frequency of hazards of a certain magnitude should be thoroughly investigated.[32]

~~[31] The warning time is the period necessary for a possible flood to travel from the main source (river, upstream basin, dam) to the site, and is therefore also directly related to the accuracy of prediction.~~

[32] The following examples of changes are for the purposes of illustration:

(a) Changes in military and industrial facilities within a 30 km radius around the site or changes in nearby transport routes (i.e. railways, aircraft, roads and rivers) leading to changes in the range and magnitude of human-induced external hazards.

(b) Changes in dam construction on rivers above the plant site leading to an increase in the damage potential of the external flood hazard.

(c) Changes in environmental conditions (average annual wind speed and maximum annual wind speed, water level, temperature, local precipitation) leading to an increase in the frequency of natural external hazards with higher damage potential.

7. SPECIFICS OF LEVEL 1 PSA FOR INTERNAL HAZARDS

INTRODUCTION

7.1. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 [3] for a Level 1 PSA for internal hazards (see typical internal hazards in para 6.8). Specific recommendations are provided for Level 1 PSA relating to the ~~following~~ internal hazards for nuclear power plants (other internal hazards are not explicitly covered in this Safety Guide, but may be addressed using similar approaches):

~~(a) Internal fires;~~
~~(b) Internal floods;~~
~~(c) Heavy load drop;~~
~~(d) Turbine missiles;~~
~~Internal explosions.~~

A BOUNDING ASSESSMENT AND DETAILED ANALYSIS FOR LEVEL 1 PSA FOR INTERNAL HAZARDS

7.2. Internal ~~H~~hazards (see paras 6.1 and 6.8) ~~that can occur inside plant buildings~~ should be considered in the frame of a bounding assessment and/or detailed analysis; a conservative screening analysis is usually omitted (it has been demonstrated in many studies that such internal hazards are often significant contributors to the overall risk). A consistent approach should be applied for the bounding assessment and detailed analysis for Level 1 PSA for internal hazards. It typically includes the following tasks:

(a) Collection of site and plant information supported, when feasible, by plant walkdowns.
(b) Hazard characterization: identification of hazards, calculation of hazard frequency and analysis of the impact of hazards.
(c) Derivation ~~Integration~~ of the Level 1 PSA for internal hazards ~~with~~ from the Level 1 PSA for internal initiating events:
    (i) Determination of initiating events induced by the internal hazards**;**
    (ii) Identification of necessary revisions to the existing event trees and fault trees of the Level 1 PSA for internal initiating events;
    (iii) Analysis of specific dependencies and common cause failures;
    (iv) Analysis of specific data;
    (v) Analysis of specific human reliability aspects.
(d) Qualitative and/or quantitative screening.
(e) Quantification of the contribution of internal hazards to core damage frequency (analysis of results, sensitivity studies, and uncertainty and importance analyses).
(f) Documentation (with particular consideration given to assumptions and references used in the analysis, including quality assurance).

7.3. ~~Some~~ Most internal hazards (e.g. internal explosions, internal fire~~s~~, internal ~~floods~~flooding) can occur in a variety of different locations in the plant (rooms, inside or outside buildings ~~or elsewhere on the site~~). In such cases, the hazard characterization should specify:

(a) First, a global plant analysis boundary so that all locations that could contribute to the hazard risk are considered;

(b) Second, enclosed plant areas, assuming that the existing protection features (e.g. physical separation, barriers, isolation equipment) in the plant design will effectively contain the damage inside the ~~areas~~area where it initiated.

7.4. Contributions to the core damage frequency from the internal hazards that remain following the screening process should be determined using a Level 1 PSA for those hazards. A Level 1 PSA for internal hazards should rely on the model of plant response developed for the Level 1 PSA for internal initiating events, both for at power and shutdown states. The availability of a Level 1 PSA for internal initiating events should be a prerequisite for development of a Level 1 PSA for internal hazards. The results of the hazards analysis may yield further initiating events in addition to those found by carrying out the Level 1 PSA for internal initiating events (e.g. the loss of all information in the main control room in the event of fire). In such cases, new accident sequences should be developed and integrated into the Level 1 PSA.

7.5. For the purposes of quantitative simplified assessments of the risk resulting from a specific internal hazard or for the screening of enclosed plant areas as specified in para. 7.3, the core damage frequency can be estimated without a detailed Level 1 PSA model for internal hazards. In this case, the general formula for calculating the cumulative contribution to core damage frequency from the specific internal hazard is:

$$f_{\text{hazard core damage}} = \sum_{i} f_{\text{hazard in plant area } i} \times \text{CCDP}_i$$

where:

$f_{\text{hazard core damage}}$ is the contribution from the specific internal hazard in the plant area to the core damage frequency;

$f_{\text{hazard in plant area } i}$ is the frequency of occurrence of the specific internal hazard in plant area '*i*';

CCDP_i is the conditional core damage probability for plant area '*i*', estimated using the Level 1 PSA for internal initiating events, adapted with conservative assumptions in accordance with the effect in the plant area '*i*' of the internal hazard.

7.6. The impact analysis should consider the effect of hazard induced component failures on initiating events included in the PSA and on associated mitigatory safety functions. Detailed analysis based on physical studies (e.g. simulations of fire scenarios or flooding propagation scenarios) should be carried out to reduce undue conservatism leading to overestimation of the risk posed by the hazard.

7.7. The potential failure of the protection features such as barriers or physical separation that could lead to the propagation of the damage to other areas should be addressed by means of a specific detailed hazard analysis.

7.8. Basic site and plant information should be obtained from drawings or databases. For operating plants, such information should be verified and completed by using plant walkdowns.

7.9. Since information from plant walkdowns may be significant input to the Level 1 PSA for internal hazards, such walkdowns should be well planned, organized and thoroughly documented.

7.10. Plant walkdowns should preferably be performed at the beginning of the process of developing the Level 1 PSA for internal hazards, but some tasks (i.e. detailed analysis for selected hazards) could require dedicated plant walkdowns.

7.11. The combination of the probabilities of hazard induced failures of SSCs important to safety and independent failures in the Level 1 PSA model will yield the hazard induced core damage frequency.

ANALYSIS OF INTERNAL FIRE

General

7.12. A Level 1 PSA for internal fire is the probabilistic analysis of fire events occurring on the site of a nuclear power plant and their potential impact on safety. Using probabilistic models, the Level 1 PSA for internal fire should take into account [42]:

(a) The possibility of a fire at any location in the plant.
(b) The potential spread of fire to other locations.
(c) Fire detection, fire suppression and confinement of fire.
(d) The possibility of damage to equipment due to actuation of fire suppression systems (e.g. spray and flood caused by fire suppression systems) may damage equipment that would otherwise survive a fire, or the failure mode of such equipment may be altered).
(e) The effects of fire on ~~pieces of equipment~~SSCs including ~~(components as well as~~ their associated ~~instrumentation and control and power~~ cables~~)~~. The effects considered should include new failure modes resulting from spurious actuation of equipment caused by 'hot shorts'.
(f) The possibility of damage to ~~such equipment~~SSCs and ~~, in the case of severe fires,~~ to the integrity of the civil structures of the plant (walls, ceilings, columns, roof beams).
(g) The impact of random equipment failures and human errors.
(h) ~~The e~~Effects of the fire, both direct (e.g. the need to evacuate the control room) and indirect (e.g. confusing information resulting from spurious indications), on actions by operating personnel and credited SSCs.

7.13. The physical separation (fire barriers) between redundant trains of SSCs important to safety may limit the extent of fire damage. Therefore, quantification of the contribution of fire to the core damage frequency with the Level 1 PSA model for internal fire should generally include probabilities of random failures of equipment not affected by the fire and the likelihood of a test or maintenance outage.

7.14. In particular, the impact of smoke should be considered in a Level 1 PSA for internal fire with regard to the following:

(a) Smoke may cause electric and/or electronic devices to fail and in particular when accompanied by high temperature.

(b) The human error probability may be higher due to unusual environmental conditions (smoke, which may be toxic as well as merely irritating, and heat) imposed by the fire event.
(c) The presence of smoke may necessitate evacuation of the main control room.

7.15. For a Level 1 PSA for internal fire for shutdown states, the following specific aspects should be considered:

(a) The specific items of the methodology for a Level 1 PSA for internal initiating events for shutdown conditions, as presented in Section 9.
(b) The screening should be performed separately to take account of the greater potentially higher and additional fire loads and different and/or additional ~~higher number of~~ potential ignition sources, particularly transient combustibles associated with maintenance ~~operations~~ activities performed during shutdown states.
(c) The fire protection means availability.
(d) The potential for further paths for fire propagation (e.g. some doors may be open during shutdown states).
(e) The increased occupancy of different plant locations during outages may improve the fire detection capabilities but may also create additional fire sources.
(f) The fire related plant operating and configuration changes that are implemented to control combustibles and those that are performed to provide compensatory measures for system or component outages.

7.16. Deterministic fire hazard analysis carried out during the design (see [6]) and the operation (see NS-G-2.1 [30]) of the plant should be used to provide an important input to the Level 1 PSA for internal fire, for example, the list of components and cables and their locations, the partitioning of the plant into fire compartments taking into account functional and detailed fire impact analyses performed for designing the fire protection features.

7.17. The approach to the Level 1 PSA for internal fire should be based on a systematic analysis of all locations within the plant boundary [42]. To facilitate this examination, the plant should be subdivided into distinct physical units ('fire compartments'[33]), which are then scrutinized individually. The plant partitioning carried out in the design may be useful as an initial point for division of these physical areas. Criteria applied for specifying fire compartments should be justified and documented. ~~Some flexibility may be exercised by the analyst in defining fire compartments for use in Level 1 PSA. For instance, the analyst may prefer to consider several fire compartments as one compartment, if this facilitates the screening analysis. Division of the plant into a large number of small locations may not be necessary, at least at the early stage of the PSA analysis.~~

7.18. The process for development of a Level 1 PSA for internal fire typically includes the tasks shown in Fig. 3 and presented in paras 7.19–7.68. For the purpose of this Safety Guide, a fire scenario is defined in terms of the fire ignition source and the extent of fire damage within a compartment. In accordance with to the level of detail of the analysis for the Level 1 PSA for

[33] In Safety Guide [6], a fire compartment is a building or part of a building that is completely surrounded by fire resistant barriers: all walls, the floor and the ceiling. In contrast to this, in the context of a PSA for internal fires, a fire compartment could be a well-enclosed room that is not necessarily surrounded by fire resistant barriers.

internal fire, the frequency associated with a particular fire scenario depends on the ignition frequency and the probability of fire suppression.

Data collection

7.19. The task of data collection and assessment in the Level 1 PSA for internal fire is aimed at preparing the necessary data. The task should be focused on collecting the plant specific data necessary for modelling the fire risk. However, some data used in the Level 1 PSA for internal initiating events will have to be reassessed to take into account fire induced conditions.

7.20. The plant specific data for the Level 1 PSA for internal fire should include the following:

(a) Cable routes of the plant, including raceways, conduits, trays and barriers;
(b) The physical characteristics of the fire compartments and their inventories (see para. 7.22);
(c) Data on fire events;
(d) Compartment specific information on components regarding their potential to be a source of fire ignition (i.e. component failures that could cause fire and transient combustible materials);
(e) Estimates of the reliability of fire detection and the means for suppression of fire;
(f) Human actions in the event of a fire and human error probabilities;
(g) Fire brigade availability and capability;
(h) Features of fire suppression systems (the timing of system actuation, fire suppression agents that may cause equipment damage or prevent operating personnel from entering the fire compartment);
(i) Equipment failure modes induced by fire and fire damage criteria.

7.21. Due to the amount and the nature of information collected and to be maintained for a Level 1 PSA for internal fire, the development of a database as a support tool should be considered.

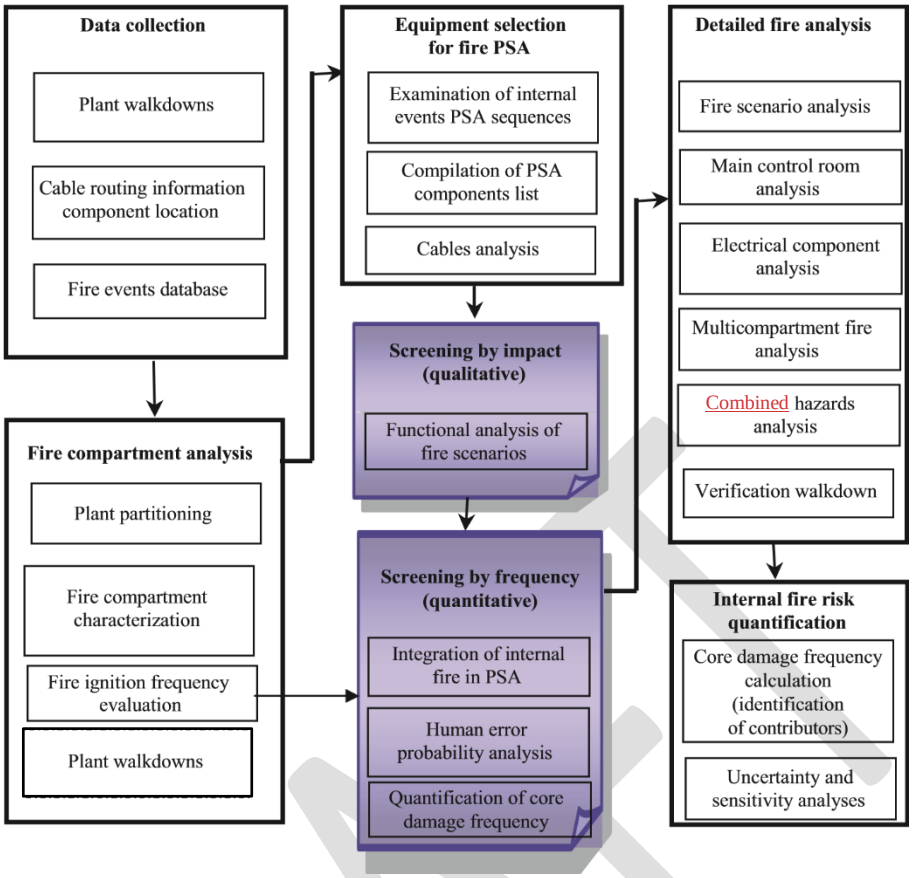

FIG. 3. Process for development of a Level 1 PSA for internal fire.

Analysis of fire compartments

7.22. For the purposes of the PSA for internal fire, all buildings and structures included in the analysis should be partitioned into distinct fire compartments, which are examined individually (see para. 7.17). Fire compartments should be characterized at least by the following:

(a) Their physical boundaries (e.g. walls, doors, dampers, penetrations);
(b) The fire protection features;
(c) The fire resistance (fire rating) of the barriers surrounding the compartment;
(d) The components and cables located inside the fire compartment;
(e) Adjacent fire compartments and the connections to these;
(f) Ventilation paths (ducts) that connect the fire compartment to be analysed with non-adjacent fire compartments;
(g) The fire load (e.g. type, amount, whether protected or unprotected, location, local distribution and whether permanent or temporary);
(h) Potential ignition sources (e.g. type, amount, location);
(i) Procedures for control of combustible material;
(j) Occupancy level (i.e. the possibility of detection of the fire by personnel);
(k) Accessibility of the location (e.g. for the fire brigade).

7.23. Either for data collection or for specification of fire compartments, the information obtained from plant documentation should be verified during plant walkdowns by visual inspection of each fire compartment throughout the entire plant to the extent possible. This verification should be such as to ensure that the data represent the actual and current condition of the plant.

7.24. Estimation of the frequency of ignition of fires for fire compartments is an important part of the Level 1 PSA for internal fire and should be performed either before screening for all fire compartments, or at the beginning of the quantitative screening process for the most important fire compartments that survive the qualitative screening process (see para. 7.44).

7.25. The frequency of ignition associated with fire ignition sources should be evaluated as far as feasible using plant specific data. When plant specific data are insufficient, generic data should be used for estimation of the fire ignition frequency along with the available plant specific data, adjusted in respect of the actual sources of fire ignition (including sources resulting from hot work), and the amounts of permanent and temporary combustible material in the fire compartments.

7.26. Estimation of the fire ignition frequency should take into account potential human errors causing fire during specific operating states (e.g. human-induced fires include transient fires and welding cutting, or other 'hot work' fires in different plant operating states).

7.27. Fire frequencies should be estimated as a mean with statistical uncertainty intervals ~~for~~ after identification and qualitative screening of fire scenarios ~~forall unscreened fire scenarios~~.

Selection of equipment for Level 1 PSA for internal fire

7.28. On the basis of the examination of plant components considered in the Level 1 PSA for internal initiating events, a list of equipment to be modelled in the internal fire Level 1 PSA should be established. The list should include equipment whose fire induced failure might result in one or more of the following:

(a) The failure might lead to an initiating event;
(b) The failure might affect the ability of safety functions to mitigate an initiating event (frontline systems and support systems);
(c) The failure might affect actions by operating personnel after the occurrence of an initiating event induced by fire (type C human interactions);
(d) The failure might lead to spurious actuation of functions that could induce other unsafe effects on the plant, both during at-power operation and during plant shutdown.

Such failures might result from failure of motive power or control power, or from hot shorts resulting in spurious operation or erroneous output from plant monitoring instrumentation and alarms. The depth of the analysis of spurious actuation of equipment should be adapted to the scope of the PSA and should focus on equipment or failure modes not already considered in the Level 1 PSA.

7.29. The plant components and all the related elements of the model important to Level 1 PSA for internal fire should be identified. The underlying basis for screening or subsuming component failure modes in the PSA model for internal initiating events should be systematically re-examined to determine the validity of the assumptions made in the context of

fire induced faults, and where necessary, the model for internal initiating events should be expanded. Passive components could be also affected by fire and the vulnerable parts of passive components should be considered.

7.30. Identification of all related cables and circuits associated with the components specified in paras 7.28 and 7.29 and analysis of cable routes should be an integral part of this examination. In addition, non-electrical circuits such as instrument air control lines should be considered for potential damage due to fire.

7.31. A list of Level 1 PSA related equipment for each fire compartment should be drawn up. At a later stage of the detailed analysis, it will be necessary to more accurately determine the locations of components within the fire compartment.

Screening by impact

7.32. Screening by impact should be used to eliminate non-significant fire scenarios on the basis of qualitative ('impact oriented') criteria. The screening starts with identifying critical fire compartments and areas, followed by specifying potential single and multicompartment fire scenarios using pessimistic assumptions. The impact oriented criteria used for screening out particular fire scenarios should take into account the characteristics of those fire compartments involved in the scenario considered.

7.33. A fire compartment may be screened out on the basis of negligible potential impact on plant safety if one or more of the following apply:

(a) The fire load density is below a specified accepted threshold and the potential for propagation is very low; or
(b) All of the following conditions hold:
    (i) No equipment is present in the compartment that can cause an initiating event or necessitate manual shutdown;
    (ii) Neither safety relevant systems (i.e. systems that are necessary for safe shutdown of the plant), nor their cables or support systems are located in the compartment;
    (iii) The potential for spreading of fire effects to other fire compartments containing SSCs important to safety is very low.

7.34. For the purposes of screening, all components and cables exposed to fire should be assumed failed, that is the pessimistic assumption is usually made that the fire detection and extinguishing features are either ineffective or not available. Other protective measures, such as fire shields, protective coatings or enclosures are not usually taken into account.

7.35. Screening by impact should also cover multicompartment fire scenarios developed under pessimistic assumptions for fire spreading. For each fire compartment, complexes of compartments where fire could propagate are defined by adding to that compartment all adjacent compartments (in all directions) and by adding all connected compartments that share ventilation without their necessarily being adjacent to the compartment. Then, all possible combinations of fire compartments should be analysed with regard to the potential for spread of fire to adjacent (or connected) fire compartments. To limit the number of combinations that need to be considered, general assumptions could be made regarding the reliability and effectiveness of fire barrier elements, based on relevant qualification programmes, industry and past facility performance data.

7.36. Fire with the potential to spread from outside the plant buildings to fire compartments located inside should be considered in the analysis (e.g. potential spreading of fire from the transformer yard into the turbine hall).

7.37. For a multi-unit site, the potential spreading of a fire from one unit to a fire compartment of another unit should be considered in the analysis. Also, the possibility of fires in common areas (e.g. swing diesels (i.e. diesels shared between units), switchyard) should be considered.

Screening by contribution to core damage frequency

Integration of internal fire in the Level 1 PSA for internal initiating events

7.38. Screening of fire compartments by their contribution to the core damage frequency, on the basis of quantitative criteria, is aimed at further elimination of fire compartments or complexes of multiple fire compartments remaining after the first step of qualitative screening by impact.

7.39. At this step, the contribution of fire to the core damage frequency should be calculated using a probabilistic model developed on the basis of the existing Level 1 PSA model for internal initiating events. Such a model is typically used to calculate the conditional core damage probability for specific fire scenarios. At this stage, for evaluating the frequencies of occurrence of fire scenarios and the associated conditional unavailability of the necessary safety functions due to fire, pessimistic assumptions should be made regarding the growth and propagation of fire, the effects of fire on equipment and the associated human actions (i.e. action for reducing fire effects): all equipment inside the fire compartment itself is pessimistically considered unavailable and the means of detecting and extinguishing fires are not credited. Human error probabilities for Type C HFEs are penalized to consider fire context as described in para 5.121(a).

7.40. With these assumptions, for each remaining fire compartment, the model for the Level 1 PSA for internal initiating events should be modified in order to map the fire effects inside the compartment and the associated initiating events and equipment failure modes. This will allow the conditional core damage probability for each fire compartment to be calculated, from which the global contribution of fire to the core damage frequency may be calculated using the formula given in para. 7.5.

Human error probability analysis

7.41. Probabilities relating to recoveries and post-trip human errors should be revised in order to assess the impact of the fire on the credited recoveries and human actions modelled in the Level 1 PSA for internal initiating events. The assessment of Type C HFEs for fire PSAs should include the following three cases:

(a) HFEs that are included in the Level 1 PSA model for internal initiating events, but are also relevant for the fire hazard scenario. In this case, it should be checked whether there is a need to revise the assessment of performance shaping factors due to the possibility that it might be harder for operating personnel to implement actions than in the base case.
(b) HFEs that are relevant only for fire. In this case the methods to assess fire specific HFEs usually follow same principles as the other types of HFE.
(c) Undesired responses by operating personnel to fire-induced spurious alarms and indications [15].

7.42. When applying the approach to human reliability analysis presented in Section 5, performance shaping factors should be analysed, considering specific fire impacts such as additional stress, the potential existence of contradictory signals, smoke, loss of lighting, and difficulty in entering or passing through the area affected by the fire.

7.43. If human actions for recovery are credited in the Level 1 PSA model for internal initiating events, the feasibility of carrying out the actions should be checked. For example, it might be difficult to carry out a particular recovery action in a room that is affected by fire. Possible secondary effects of the fire on the control room air quality and on human error probability should be checked.

Quantification of the contribution of fire to the core damage frequency for screening

7.44. For quantitative screening, the contribution of fire to the core damage frequency should be assessed for each fire compartment, considering the corresponding frequency of the fire scenario, in accordance with the general formula given in para. 7.5 and potential for fire propagation.

7.45. Quantitative screening should be based on a pessimistic estimate of the conditional core damage probability or the absolute contribution of fire to the core damage frequency. Two criteria for quantitative screening of fire compartments could be defined as follows:

(a) The cumulative contribution of fire to the core damage frequency for all fire compartments screened out should be under a specified threshold. This threshold may be defined as a specific absolute value or be given in relative terms (e.g. the contribution of internal initiating events to the core damage frequency).
(b) The criterion for screening individual fire compartments should be set to a value high enough to allow some screening, but sufficiently low as to retain all risk significant fire scenarios.

7.46. Screening by considering the contribution of fire to the core damage frequency should consider the frequency of damage to multiple fire compartments as the product of the frequency of ignition in one fire compartment and the conditional probability of fire spreading to other compartments.

7.47. The result of the entire screening process (by impact and by frequency) should be as follows:

(a) A list of fire scenarios or fire compartments that cannot represent significant contributors to risk, and which can be screened out from detailed analyses. The estimated risk associated with screened out scenarios or fire compartments should remain in the overall fire PSA results.

(b) A list of fire scenarios associated with fire compartments that may represent significant contributors to risk, and which need further consideration. For each fire scenario on this list, a quantitative Level 1 PSA model for internal fire should be developed for further analysis.

Detailed analysis of fire

Analysis of fire scenarios

7.48. Detailed fire analysis should aim at reducing the level of conservatism in the fire scenarios identified so far in the screening process. The effect of fire barriers inside the compartment and other means of protection from fire, the location of SSCs important to safety and firefighting equipment in the fire compartment and other aspects such as growth and propagation of fire should be taken into account. All the effects of fire, including flame, plume, ceiling jet, radiant heat from hot gases, high energy arcing and smoke should be considered and assessed. Generally, dedicated walkdowns should be performed in carrying out the Level 1 PSA for internal fire to gather supporting information for verification of the detailed analysis.

7.49. More realistic models should be applied for assessing human actions for reducing the probability of equipment damage, growth and propagation of fire, and the effects of fire on the equipment and cables.

7.50. The effects of fire and of possible spreading of smoke and toxic gases on human performance should be assessed. It should also be noted that overpressure resulting from fire may prevent the opening of doors necessary to access recovery locations.

7.51. The choice of specific modelling tools for the analysis of growth and propagation of fire (e.g. fire simulation codes) should be justified and documented.

7.52. Fire scenarios should describe the time dependent course of a fire that is initiated in a selected compartment and any subsequent component and cable failures. A fire scenario should be represented in the Level 1 PSA model for internal fire, for example, by fire propagation event trees (see example in Annex II), where all important features affecting fire development are modelled (design and quality of fire barriers, fire growth and propagation model, criterion for damage of equipment at risk, including cables, fire protection and suppression features). The recommendations in Section 5 should be applied for determining such fire propagation event trees.

7.53. For the fire scenarios to be analysed, human reliability for manual actions and component reliability of detection and suppression systems should be assessed using the same methodology as presented in Section 5 for PSA for internal initiating events.

7.54. Pathways that may be relevant for propagation of fire (e.g. ventilation or cable gutters, failed fire barriers) should be taken into account in the fire scenarios.

7.55. For fire compartments considered in the detailed fire analysis, data on the frequency of occurrence of a fire scenario should be complemented with additional data specific to the fire compartment, such as non-permanent ignition sources, ignitability, and the possible presence of fire load.

7.56. The specified effectiveness and response times of automatic and manual capabilities for fire detection and suppression should be substantiated for specific fire scenarios, together with the specified probability of non-suppression of fire.

Analysis of fire in the main and supplementary control rooms

7.57. The Level 1 PSA model for internal fire in the main and supplementary control rooms should take into account the specific features associated with ~~this~~ these locations, such as the widespread effect of a fire in the ~~main~~ control rooms across all ~~mitigating system~~credited

systems, the potential for spurious actuation of systems and the impact of fire in ~~the main~~ control rooms on actions by operating personnel. The latter should include:

(a) The effects of fire and smoke on the availability of instrumentation and related equipment;

(b) The capability of features for fire detection and suppression, including the potential adverse impact of flooding;

(c) The use of an alternative location for safe shutdown, taking into account aspects of accessibility, interdependencies and other possible limitations;

~~(c)~~(d) The potential fire-induced failure modes affecting both main and supplementary control rooms simultaneously (e.g. fire in supplementary control room leading to the overtaking the control from the main control room due to the spurious activation)

~~(d)~~(e) The effects of the spreading of smoke and toxic gases.

In addition, intracavity fire propagation should be taken into account, including the presence of physical barriers as well as spatial separation of redundant components.

Analysis of fire in the electrical component room

7.58. The electrical component rooms, switchgear rooms, cable spreading rooms and other rooms containing control equipment tend to become natural centres of convergence for equipment and wiring. They contain electrical equipment and cables that may belong to more than one ~~safety system~~ train of the credited system. Therefore, the potential impact of fire on redundant equipment for safe shutdown and on other Level 1 PSA related equipment is likely to be greater than the impact of fire in other plant locations and this should be considered.

7.59. There is also a higher probability for single or multiple spurious actuations of electrical components because of fire induced electrical shorts in these locations. In the analysis of spurious actuation of electrical components, the particular fire induced circuit failures should be identified and associated conditional probabilities assessed.

Multicompartment fire analysis

7.60. Multicompartment fire analysis aims to identify the potential fire scenarios significant to risk that involve more than one fire compartment. It should be assumed that fire may spread from one compartment to another through shared barriers or via ventilation ducts that connect the compartments. Compared with the analysis performed during the screening process, multicompartment detailed fire analysis should be based on a fire growth model, a model for analysis of fire propagation and a model for fire suppression.

7.61. As for single fire compartments, the detailed analysis for multicompartment fire should consider the depth of propagation of the fire, the spread of combustion products and/or the transfer of heat to adjacent (or connected) fire compartments.

Analysis of combined hazards

7.62. The potential for occurrence of other fire-induced consequential internal hazards (e.g. flooding caused by actuation of a fire extinguishing system discharging a large amount of

water, explosion of hazardous material caused by fire, fire caused by explosion) should be identified and should be considered in the Level 1 PSA for internal fire. The multiple independent fires could typically be screened out based on low frequency of occurrence.

7.63. A qualitative analysis of internal fires induced by other hazards (e.g. seismicity, lightning, external fire, airplane crash) should be performed. Fire compartments where the combined impact of other hazards and fire could be important for safety should be analysed. Ignition sources induced by hazards, spurious actuation or degradation of fire suppression systems, and difficulties in carrying out manual firefighting actions, are examples of impacts to be considered (see the recommendations on Level 1 PSA for external hazards provided in Section 8).

7.64. The following effects of internal fire induced by other hazards on the performance shaping factors of operating personnel should be taken into account:

(a) Accessibility of the compartments of interest after initiation of the fire;
(b) Increased stress level;
(c) Failures of indication or false indication;
(d) Combined effects of fire on the behaviour of operating personnel.

Quantification of risk of internal fire

7.65. The specific models developed for the detailed analysis of the Level 1 PSA for internal fire (e.g. model for a fire in the main control room or model to assess the impact of single or multiple spurious actuations of components induced by fire) should be included in the complete Level 1 PSA model.

7.66. The final quantification of the contribution of internal fire to the core damage frequency should be performed for the fire compartments remaining after the screening, considering the results of the detailed analysis. The results and the model used for quantitatively screening out fire compartments by frequency should be included in the Level 1 PSA for internal fire. The results of the Level 1 PSA for internal fire should be interpreted by identifying the main contributors to core damage frequency (e.g. fire compartments, fire scenarios, human actions). Assumptions relating to screening should be reviewed at this final stage to consider whether contributors to the core damage frequency that were screened out need to be added to the detailed model.

7.67. The quantification of the Level 1 PSA model for internal fire, the uncertainty analysis, the importance analysis and the sensitivity analysis should all follow the recommendations presented in Section 5. An uncertainty analysis should be performed to identify the sources of uncertainty and to evaluate them. Sensitivity studies and importance analysis should be performed to identify the elements of the Level 1 PSA for internal fire that are significant to risk. Sensitivity studies should also be performed for the important assumptions and data. The relative importance of various contributors to the calculated results should be determined.

Documentation for Level 1 PSA for internal fire

7.68. This paragraph provides recommendations on meeting Requirement 20 of GSR Part 4 [3] on the documentation for Level 1 PSA for internal fire. The Level 1 PSA for internal fire should be documented in a manner that facilitates review, applications and updating of the Level 1 PSA. In particular, the following information should be included in the documentation:

(a) A description of the fire protection features specific to the plant, including passive and active mitigation features of the plant as well as partitioning of the plant into fire compartments;
(b) A description of the specific methods and data used for assessing the fire hazard;
(c) A description of the changes made in the Level 1 PSA model for internal initiating events to take into account the effects of internal fire;
(d) A characterization of fire compartments;
(e) Justification for the screening of particular fire compartments from the analysis;
(f) The results of the specific analyses for detailed fire scenarios, for example for the main control room, the electrical component room, multicompartment fire and multiple hazards;
(g) The final results of the Level 1 PSA for internal fire in terms of core damage frequency as well as selected intermediate results;

(h) The report of the plant walkdown in support of fire analysis.

ANALYSIS OF INTERNAL FLOODING

General

7.69. A Level 1 PSA for internal flooding is the probabilistic analysis of events relating to release of liquids (usually water) occurring inside plant buildings and the potential impact of such releases on safety. The process of development of a Level 1 PSA for internal flooding typically includes the tasks shown in Fig. 4 and presented in paras 7.69–7.98. For a Level 1 PSA for internal flooding for shutdown states, the aspects listed in para. 7.15 should be considered.

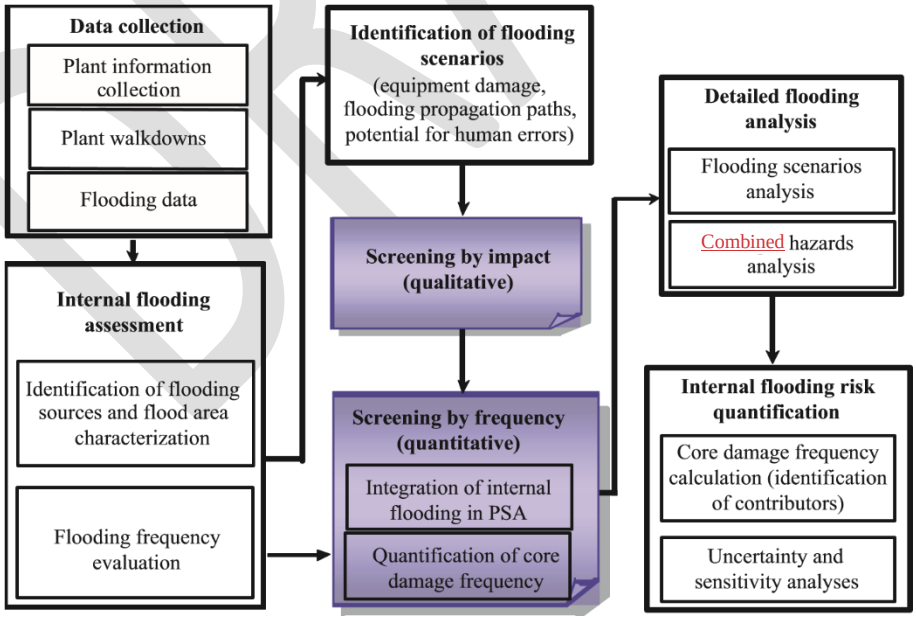

FIG. 4. Process of development of a Level 1 PSA for internal flooding

Data collection and assessment of potential for internal flooding

7.70. For operating nuclear power plants, plant walkdowns specifically oriented towards assessment of internal flooding should be performed to verify the accuracy of information obtained from drawings and other sources of plant information and to obtain necessary information on spatial interactions for analysis of the damage effects from each potential source of internal flooding.

7.71. Possible internal flooding events should be identified and characterized (see [6] for general considerations on flooding in the design of nuclear power plants). In carrying out this task, consideration should be given to the following:

(a) Possible sources of flooding: pipes, internal tanks, pools, valves, heat exchangers, connections to open-ended sources (e.g. sea, lake, river), multi-unit shared systems or structures.
(b) Possible flooding mechanisms: breaks, leaks, rupture, spurious or desired actuation of a spray system (e.g. the containment spray system or the fire extinguishing system) or human error during operation or during maintenance related activities (e.g. wrong positioning or inadvertent opening of a valve).
(c) Characteristics of the flood: capacity (depending on whether the source of flooding is a closed or open system), flow rate, temperature and pressure, presence or possible production of steam.
(d) Flooding related alarms, leak detection systems, capacity of draining systems and flooding related protection for components (such as equipment trip signals).
(e) Critical flooding heights of components relevant to PSA and room dimensions in the flooding areas.

7.72. When identifying potential flooding events, particular consideration should be given to plant shutdown conditions, as water pathways are frequently manually reconfigured at such times.

7.73. Plant areas that can be affected by internal flooding should be determined and possible propagation paths for the water should be identified. In doing this, consideration should be given to multi-unit aspects and account should be taken of the potential for failure of flood barriers due to accumulated water.

7.74. The plant should be divided into physically separate ‘flooding areas’, where one flooding area is viewed as generally independent of other areas in terms of the potential effects of internal flooding and the potential for flood propagation.

7.75. Plant specific data should be used as far as feasible for the estimation of frequencies of internal flooding events. When plant specific data are insufficient, it is possible to use generic data or expert judgement with appropriate justifications.

7.76. The main data for evaluation of the frequency of internal flooding events are estimates of pipe failure rates and rupture frequencies with associated uncertainties. Data should be selected for piping systems that represent significant sources of internal flooding.

7.77. The frequency and severity of flooding events caused by human error should be also evaluated, considering plant specific maintenance procedures and experience as well as spurious actuation of water-based firefighting systems.

7.78. Flood frequencies should be estimated as a mean with statistical uncertainty intervals after identification and qualitative screening of flood scenarios~~for all unscreened flood areas~~.

Identification of internal flooding scenarios

7.79. For each flooding area, SSCs that could be affected by the flooding occurring inside should be identified. Depending on the scope of the analysis, the following flooding effects on equipment could be relevant: submersion, temperature, pressure, spray, steam, pipe whip or jet impingement as a consequence of a break in high energy piping or valve binding. It should be ensured that the analysis is, as far as possible, complete.

7.80. Consideration of components affected by internal flooding should take into account elevations, barriers, doors and drains. The potential for drain blockages should be considered.

7.81. The possibility of floodwater spreading from one area to another should be assessed, including consideration of barrier failure.

7.82. All possible routes for the propagation of floodwater should be taken into consideration, for example, equipment drains, and the possibility of normally closed doors or hatches being left open.

7.83. The location, including the elevation, of cabinets, terminal boxes for cables for SSCs important to safety and other sensitive equipment should be identified. In this way, the vulnerability of components with respect to flooding of certain rooms can be identified.

7.84. The potential impact of flooding on plant operation should be assessed. Analysis of the potential impact of flooding on plant operation should include spurious actuation of components or systems due to flooding effects, which could initiate particular accident sequences.

Screening by impact

7.85. Screening of internal flooding scenarios by their impact should be performed. Critical flooding areas can be selected by screening out flooding areas on the basis of negligible potential impact on plant safety. Flooding area may be screened out from the analysis by their impact if one or more of the following apply:

(a) Both of the following conditions hold:
  (i) The flooding area contains no equipment that can cause an initiating event;
  (ii) Neither systems necessary for safe shutdown of the plant nor their support systems are located in the compartment of flood origin or in the flood propagation zone; or
(b) The compartment does not contain any sources of flooding, including in-leakage from other compartments, sufficient to cause failure of equipment.

Screening by contribution to core damage frequency

Integration of internal flooding in the Level 1 PSA for internal initiating events

7.86. Internal flooding events could be further screened for their contribution to the core damage frequency. Therefore, the Level 1 PSA for internal initiating events should be modified to take into account flooding phenomena (both system models and actions by operating personnel).

7.87. A complete review of the human reliability analysis in the Level 1 PSA for internal initiating events should be performed. When applying the approach to human reliability analysis presented in Section 5, performance shaping factors should be analysed, with consideration given to the specifics of the flood initiator. Reassessment and readjustment of human error probabilities should be performed, taking into account specific procedures for mitigation of flooding. At a minimum, the following flood induced effects on the performance shaping factors of operating personnel should be taken into account:

(a) Accessibility of the compartments of interest after flooding and/or the impact of adverse environmental conditions due to flooding or the presence of steam or spray;
(b) Potential increased stress level;
(c) Failures of indication or false indication;
(d) Other effects of flooding on the behaviour of operating personnel.

Quantification of the contribution of internal flooding to the core damage frequency for screening

7.88. For the quantitative screening task, a conservative approach should be used, which assumes that all components in the compartment being affected by the flooding will fail. If this assumption does not give rise to a significant contribution to the core damage frequency (calculated by using the formula given in para. 7.5), the flooding area can be screened out.

7.89. Quantitative criteria for screening in accordance with contribution to the core damage frequency should be defined for Level 1 PSA for internal flooding. Examples of such criteria could be as follows:

(a) The cumulative contribution of flooding to the core damage frequency for all flooding areas screened out should be under a specified threshold. This threshold may be defined as a specific absolute value or be given in relative terms (e.g. the contribution of internal initiating events to the core damage frequency).
(b) A list of flooding scenarios associated with fire compartments that may represent significant contributors to risk, and which need further consideration. For each flooding scenario on this list, a quantitative Level 1 PSA model for internal flooding should be developed for further analysis.

~~(b) The contribution of flooding for individual flooding area to the core damage frequency is sufficiently low to bound all risk significant fire scenarios. The threshold for screening may be defined in the same way as for the previous criteria, but should be at least an order of magnitude lower.~~

7.90. The result of the entire screening process (by impact and by frequency) should be as follows:

(a) A list of flooding scenarios or areas that cannot represent significant contributors to risk, and which can be screened out from detailed analyses. Estimated risk associated with screened out scenarios or flooding areas should remain in the overall internal flooding PSA results.

(b) A list of flooding scenarios associated with flooding compartments that may represent significant contributors to risk, and which need further consideration. For each flooding scenario on this list, a quantitative Level 1 PSA model for internal flooding should be developed for further analysis.

Detailed analysis of flooding

Analysis of flooding scenarios

7.91. The quantitative, detailed flooding analysis should address the following issues:

(a) Timing calculations (rate of change of flood levels) for recovery;
(b) Human reliability analysis for the additional human actions necessary to mitigate the flooding sequences;
(c) Development of event tree or fault tree models for each flooding scenario (based on the Level 1 PSA for internal initiating events (see Section 5 or new models when appropriate));
(d) Quantification of the corresponding event tree or fault tree with equipment failed due to the flood and analysis of results, including sensitivity studies and uncertainty analysis.

7.92. All potentially contributory initiating events should be analysed in terms of the means of detecting and controlling them. The means of detection and control should then be considered in estimating the probabilities of non-detection and non-isolation.

7.93. Internal flooding scenarios should describe the time dependent course of a flood originating in a selected plant area and the subsequent component failures (see para. 7.79). A flooding scenario can be represented by event trees for flooding where all important features affecting flood development (design of flood barriers, flood detection and isolation of flooding sources) and probabilities of component failures are modelled. Generally, dedicated walkdowns should be performed in carrying out the Level 1 PSA for internal flooding in order to gather supporting information for verification of the detailed flooding analysis.

7.94. Probabilities relating to recoveries and post-trip human errors should be revised in order to assess the impact of the internal flooding on the credited recoveries and human actions modelled in the Level 1 PSA for internal initiating events. The assessment of Type C HFEs for internal flooding should include the following three cases:

(a) HFEs that are included in the Level 1 PSA for internal initiating events, but are also relevant for the flooding scenario. In this case, it should be checked whether there is a need to revise the assessment of performance shaping factors due to the possibility that it might be harder for operating personnel to implement actions than in the base case.
(b) HFEs that are relevant only for flooding (e.g. these include, for example, isolation and subsequent restoration of the electrical power supplies). In this case the methods to assess flood specific HFEs may usually follow same principles as the other types of HFE.
(c) Undesired responses by operating personnel to flood-induced spurious alarms and indications.

Analysis of combined hazards

~~7.95. Flooding and damage to SSCs due to high energy pipe breaks should be treated in the Level 1 PSA for internal flooding. if it has not been included as part of the Level 1 PSA model for internal initiating events.~~

7.95. ~~Flooding caused by actuation of a fire extinguishing system discharging a large amount of water should be addressed in the context of the Level 1 PSA for internal fire (see para. 7.62).~~A qualitative analysis of internal flooding induced by other hazards (e.g. seismicity) should be performed. Flooding compartments where the combined impact of other hazards and flooding could be important for safety should be analysed. Flooding sources induced by hazards and difficulties in carrying out manual flooding protection actions, are examples of impacts to be considered (see the recommendations on Level 1 PSA for external hazards provided in Section 8). In addition, ~~F~~flooding caused by actuation of a fire extinguishing system discharging a large amount of water should be addressed in the context of the Level 1 PSA for internal fire (see para. 7.62).

7.96. The following effects of internal floods induced by other hazards on the performance shaping factors of operating personnel should be taken into account:

(a) Accessibility of the compartments of interest after initiation of the flood;
(b) Increased stress level;
(c) Failures of indication or false indication;
(d) Combined effects of flooding on the behaviour of operating personnel.

~~7.96.~~

Quantification of risk of internal flooding

7.97. The results and the model used for quantitatively screening out flooding scenarios by frequency and the specific models developed for the detailed analysis of the Level 1 PSA for internal flooding should be included in the complete Level 1 PSA model. Then, the final quantification of the contribution of flooding to the core damage frequency should be performed, including identification of the main contributors (e.g. flooding sources, flooding scenarios) and review of assumptions relating to screening, uncertainty and sensitivity analyses. The recommendations in Section 5 should be followed.

Documentation for Level 1 PSA for internal flooding

7.98. This paragraph provides recommendations on meeting Requirement 20 of GSR Part 4 [3] on documentation for Level 1 PSA for internal flooding. The Level 1 PSA for internal flooding should be documented in a manner that facilitates review, applications and updating of the Level 1 PSA. In particular, the following information should be included in the documentation:

(a) A description of the specific methods and data used to assess the internal flooding hazard;
(b) A description of the changes made to the Level 1 PSA model for internal initiating events aimed at accounting for the effects of internal flooding;
(c) Justification for the screening of particular flooding scenarios from the analysis;
(d) The results of the detailed analysis for flooding scenarios, including description of the scenarios, and significant assumptions made in the analysis;

(e) The final results of the Level 1 PSA for internal flooding in terms of core damage frequency, qualitative insights and recommendations;
(f) The report of the plant walkdown in support of flooding analysis.

OTHER INTERNAL HAZARDS

Analysis of heavy load drops

7.99. PSAs normally focus on the failure to cool the core inside the reactor vessel or the fuel stored in the spent fuel pool. However, other, more direct damage can occur, for example, by heavy load drops onto the vessel, spent fuel pool or systems required to perform critical safety functions. Potential drops of heavy loads (e.g. the confinement dome, the reactor pressure vessel head, the spent fuel cask, concrete shielding blocks) should be analysed in respect of their potential to damage SSCs needed to perform safety functions or in respect of their potential to result directly in mechanical damage to fuel assemblies.

7.100. If the pathway along which a load is transported is located neither above the fuel nor above the regions containing SSCs important to safety, screening out of individual initiators of heavy load drops may be possible.

7.101. The probabilistic analysis should consider locations in addition to the reactor refuelling floor where heavy loads are handled. For example, some plants have open areas in the turbine hall where decay heat removal systems are located, and which are vulnerable to heavy load drops (e.g. testing devices may drop down and destroy pipes connected to the vessel).

7.102. The contribution of heavy load drops to the core damage frequency should be calculated, unless the event can be discarded on a probabilistic basis.

7.103. The Level 1 PSA for heavy load drops should be consistent with the plant response model developed for the Level 1 PSA for internal initiating events for shutdown states (see para. 9.12).

7.104. All permanent lifting equipment in the plant should be considered. Areas where a dropped load could adversely affect SSCs important to safety should be identified and examined in detail. A plant walkdown should be performed for that purpose.

7.105. Loading operations should be identified and analysed on the basis of work procedures during shutdown.

7.106. The frequencies of initiating events should be calculated in accordance with the recommendations in Sections 5 and 9. Calculations should consider failure of mechanical equipment, human error and possible unavailability of automatic protection functions. If not considered in the Level 1 PSA for external hazards, external phenomena such as earthquakes or impacts of aircraft should be addressed in the initiating event analysis.

7.107. For each heavy load drop event, it should be conservatively assumed that the maximum load is dropped and, if necessary, the nature of the dropped object and the cause of its dropping should be analysed. The possible direction, size, shape and energy of the missile or missiles generated by the dropped load should be characterized and the effects on the building structure and on the plant should be assessed.

7.108. If a Level 2 PSA if foreseen, each heavy load drop event should be considered in order to determine the potential radiological consequences and the contribution to the frequency (if any) of a plant damage state.

Analysis of turbine missiles

7.109. The contribution of turbine disintegration (e.g. failure of turbine rotor) to the core damage frequency should be calculated, unless the event can be discarded on a probabilistic basis. The impact of a fire due to ignition of hydrogen or due to oil combustion on components relevant to PSA should be considered in the context of the analysis of the impact of turbine missiles.

7.110. The analysis of turbine disintegration should include both normal speed values and overspeed values.

7.111. The distribution of missiles following turbine disintegration should be determined and hence the probability of such missiles impacting buildings, given the orientation and the location of the turbine, should be evaluated.

7.112. The resulting failure probabilities of SSCs important to safety within buildings should be determined, taking into account the proportion of missiles with sufficient kinetic energy to penetrate the buildings.

7.113. In the first stage, only equipment credited in the accident sequences identified previously in the Level 1 PSA should be considered.

7.114. Failure probabilities resulting from missile impact, together with the probabilities of random failure of the surviving SSCs important to safety and the frequency of turbine disintegration, should be used to calculate the frequencies of faults which lead to associated core damage states or large releases.

7.115. A plant walkdown should be performed to confirm the assumptions in the analysis regarding protection of structures, buildings and the selected equipment against turbine missiles.

Analysis of internal explosion

7.116. The general process for conducting Level 1 PSA for internal hazards should be adapted for a Level 1 PSA for internal explosion, considering that nuclear power plants are basically designed so as to minimize the likelihood and effects of internal explosions. Analysis of internal explosions induced by or inducing internal fires should be considered in the Level 1 PSA for internal fire.

7.117. The design of the nuclear plant building includes the prevention and mitigation of explosions (see [6]). For design purposes, systematic analysis of explosions is used to characterize the potential sources of explosions (nature and quantity of the explosive materials, localization), the potential impacts of deflagrations or detonations on the plant (overpressure, impulse or drag loads, fire or heat) and prevention features. The Level 1 PSA for internal explosion should rely mainly on the information and data collected during these analyses to allow the qualitative screening out of explosion scenarios.

7.118. A plant walkdown should be performed for identification of potential explosion sources and for verification purposes.

7.119. ~~For the remaining explosion scenarios, t~~The frequency of explosion events should be evaluated using the recommendations in Section 5. The quantification should consider the amount of explosive materials located within the plant, human activities that can be at the origin of the explosion and the effectiveness of the means of prevention (e.g. hydrogen detection equipment, leakage of explosive liquid or gas detectors, ventilations).

7.120. The contribution of internal explosion to the core damage frequency should be calculated, unless the event can be discarded on a probabilistic basis.

8. SPECIFIC ASPECTS OF LEVEL 1 PSA FOR EXTERNAL HAZARDS

INTRODUCTION

8.1. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 [3] for Level 1 PSA for external hazards. Specific recommendations are given only for selected external hazards that cannot be screened out in many cases, as follows:

(a) Seismic hazards;
(b) ~~Wind hazards~~High winds;
(c) External floods;
(d) Human-induced hazards.

BOUNDING ANALYSIS FOR EXTERNAL HAZARDS

General aspects

8.2. The bounding analysis is performed with the aim of reducing the list of external hazards subject to detailed analysis, thereby focusing on the most significant accident scenarios. The bounding analysis should be performed in such a way that it provides assurance that the core damage associated with the specific external hazard is insignificant compared with other hazards.

8.3. In the bounding analysis, all potential impacts of each non-screened external hazard on the nuclear power plant should be considered.[34]

8.4. The cumulative contribution of the external hazards subject to the bounding analysis should be calculated and retained in the final results of the Level 1 PSA.

[34] Examples of impact categories include loss of off-site power or station blackout; degradation or loss of ultimate heat sink; explosion or release of hazardous material; and degraded or isolated plant ventilation (owing to risk of toxic impact).

8.5. A set of scenarios for the specific hazard should be developed unless all the impacts of the hazard on the plant can be bounded by a single scenario, which is typically not the case.

8.6. In the bounding analysis, applicable combinations of external hazards identified as described in para. 6.11 should also be considered.

8.7. The bounding estimations should be based on models and data that are realistic but demonstratively conservative. Such models and data include the following:

(a) Assessment of the frequency of hazards (i.e. estimations of the frequency of exceedance of particular intensities);
(b) Analysis of the impact of hazards on the plant (i.e. loads associated with the hazard);
(c) Analysis of the plant response (i.e. fragilities);
(d) Level 1 PSA models and data for the plant.

Seismic hazards

8.8. Seismic hazards are important contributors to core damage frequency in many Level 1 PSAs; consequently, a detailed analysis should be performed. However, in order to limit the effort required for Level 1 PSA for seismic hazards, it is possible to perform a simplified analysis with conservative assumptions. The secondary effects of seismic hazards (e.g. seismically induced fires and floods) should also be considered at this stage. Additional details are provided in Refs [7, 25, 29, 31].

High winds

8.9. Several types of high wind should be considered and subjected to bounding analysis or detailed analysis, depending on the location of the site, as follows:

(a) Winds and other effects associated with tornados;
(b) Winds associated with tropical cyclones (cyclones, hurricanes, typhoons);
(c) Extratropical high winds (e.g. thunderstorms, squall lines, weather fronts).

The applicable combinations of high winds with other hazard phenomena identified as described in para. 6.11 should be considered, with account taken of possible dependencies (e.g. high winds and high water levels).

External floods

8.10. The following flood related hazards should be considered in the Level 1 PSA:

(a) High river water or lake water;
(b) High tides;
(c) Wind driven storms;
(d) Extreme precipitation;
(e) Tsunamis;
(f) Seiches;
(g) Flooding caused by landslides;
(h) Human-induced floods (e.g. failures of dams, levees, dykes).

The applicable combinations of external floods with other hazard phenomena identified as described in para. 6.11 should be considered, with account taken of possible dependencies (e.g. high water level, consequential dam failures).

8.11. The consequences of heavy rain and other flooding, such as water collecting on rooftops and in low lying plant areas, should be included in the scope of the analysis.

Other natural hazards

8.12. A comprehensive list of potential natural hazards (other than seismic hazards, high winds and external floods) should be considered in the bounding analysis. The list of natural hazards presented in Annex I and the list of natural hazards considered in the safety analysis reports for the plant should be used as a basis for identification of hazards. Site specific natural hazards should also be considered if applicable.

8.13. The applicable combinations of natural hazards with other hazard phenomena identified as described in para. 6.11 should be considered, with account taken of possible dependencies (e.g. severe weather conditions and transportation accidents).

Human-induced hazards

8.14. The following sources of human-induced hazards should be considered at a minimum:

(a) Fire spreading from nearby plant units or facilities;
(b) Explosions of solid substances or gas clouds from nearby facilities or due to a transportation or pipeline accident;
(c) Releases of chemical materials from nearby facilities or due to a transportation or pipeline accident;
(d) Aircraft crash;
(e) Collisions of ships with water intake structures.

The following sources could also be considered as human-induced hazards:

(f) Missiles from other plants on the site;
(g) Excavation work outside and inside the site area;
(h) Electromagnetic interference (e.g. magnetic or electrical fields generated by radar, radio or mobile phones).

PARAMETERIZATION OF EXTERNAL HAZARDS

General aspects

8.15. The most important parameters relating to the damage potential of the external hazards should be defined. Several parameters should be defined if the damage potential of the hazard cannot be characterized by a single parameter.

Seismic hazards

8.16. Seismic hazards are characterized by following main parameters [7, 25]:

(a) The peak ground motion (e.g. acceleration, velocity, displacement).
(b) The frequency content, which is generally represented by spectral accelerations associated with the ground response spectrum.

When a single parameter is used in a simplified way in Level 1 PSA to characterize seismic damage potential (e.g. peak ground motion acceleration), other parameters should also be considered when specific impacts of seismic hazards are to be assessed, as follows:

(a) The frequency content is essential for the consideration of relay 'chattering' and for determining the response and fragility of structures and components, and stress factors for human errors.
(b) The local geology and geotechnical conditions should be taken into consideration in relation to secondary hazards such as liquefaction of soil, subsidence, slope instability, collapse, surface faulting or fracturing.

8.17. Vibratory ground motion caused by earthquakes should not be eliminated from consideration (i.e. seismic waves can reach any point on the Earth's surface).

8.18. Earthquake ground motion should not be screened out.

High winds

8.19. Different parameters should be considered depending on the wind type, as follows:

(a) The dynamic load from gusts and the load from the wind averaged over a specified time period (e.g. 10 minutes) are essential parameters for the characterization of continuous translational winds.
(b) The rotation velocity, pressure differential and path area of tornadoes and the impact potential (i.e. size and velocity) of tornado-borne missiles are essential parameters for the characterization of tornadoes.

External floods

8.20. The damage potential of external floods can be characterized by the discharge, velocity, water level, duration and contribution of wave action. Some or all of these parameters should be estimated for the characterization of external floods (SSG-18 [24]). For floods, the following parameters are commonly used:

(a) River: water level, water discharge/velocity and duration of flood.
(b) Sea or lake: water level, duration of flood and velocity.
(c) Wave: height, length, period, wind speed and direction.
(d) Wave run-up: height, quantity of water overtopping and quantity per second.
(e) Seiche: frequency of oscillation and wave height.
(f) Ice: thickness and stream velocity.

8.21. The speed, direction and duration of wind, which can occur simultaneously with a flood, should be taken into account as a potential combined hazard.

Other natural hazards

8.22. A wide variety of natural hazards could be applicable to a specific site. For each specific hazard, parameters should be specified that bound all potential effects associated with the hazard.

8.23. The parameters for each hazard should be selected in a way that provides the possibility for analysis of the combined effects of the hazards.

Human-induced hazards

8.24. For each human-induced hazard, the parameters should be defined on the basis of their specific challenge to SSCs important to safety, for example as follows:

(a) For many transportation related hazards, the actual danger is from an explosion or a release of a hazardous material. The key parameter is the amount of material being carried or the maximum amount that could be released in an accident.
(b) For releases from nearby industrial facilities, the nature of the hazardous material and the maximum amount that could be released in an accident are appropriate parameters.
(c) For a collision, the key parameter should be related to the impact, e.g. the mass and the velocity of the impacting object (e.g. a barge colliding with a water intake, or an aircraft colliding with a structure).
(d) If a human-induced hazard is caused by explosion after direct impact (e.g. an aircraft crash), the key parameters should involve some combination of the amount of fuel onboard and the mass of heavy items such as engines that could damage a structure.
(e) For hazards such as pipeline accidents, the inventory of materials that could be released and the nature and pressure of the materials are appropriate parameters.

8.25. Each human-induced hazard may result in a combination of various impact factors that have to be considered. For example, an aircraft crash may cause direct damage, explosion, fire and vibration. Similarly, a pipeline accident may result in a blast (impulsive load resulting from deflagration or detonation), fire and vibration. It may also produce missiles that can affect different parts of the plant. In the characterization of human-induced hazards, all primary and secondary effects should be taken into account. Regardless of the origin of the initiator, the effect should be expressed in terms of the following parameters:

(a) Impact load;
(b) Thermal load;
(c) Vibratory load;
(d) Propagation of toxic gases.

8.26. For explosion of gas clouds, the potential drift from their point of origin to the plant should be taken into account.

8.27. The applicable combinations of the human-induced hazard with other hazard phenomena identified as described in para. 6.11 should also be considered, with account taken of possible dependencies (e.g. chemical release, wind speed and direction).

DETAILED ANALYSIS OF EXTERNAL HAZARDS

8.28. A detailed analysis should be performed for all hazards ~~that~~ for which the simplified analysis with conservative assumptions has demonstrated that the risk coming from the hazard might be significant.

8.29. The availability of the Level 1 PSA model for internal initiating events is a prerequisite for carrying out the detailed analysis of the external events PSA.

8.30. The detailed analysis should be based on realistic models and data, including a comprehensive Level 1 PSA model that provides the possibility of modelling all phenomena associated with the external hazard under consideration.

8.31. While performing detailed analysis, the combined impact of external hazards should be considered when they have a common origin (e.g. high winds, lightning) or other dependencies (e.g. high level water due to precipitation, dam failure).

FREQUENCY ASSESSMENT FOR EXTERNAL HAZARDS

General aspects

8.32. Paragraph 4.20 of SSR-1 [21] states:

> "The site evaluation for a nuclear installation shall consider the frequency and severity of natural and human induced external events, and potential combinations of such events, that could affect the safety of the nuclear installation."

Thus, the output of the hazard evaluation should include the frequency and the severity of the hazard and should properly consider uncertainties.

8.33. External hazards are characterized by multiple output parameters, some of which may be probabilistically dependent. For simplicity, the hazard curve is generally described in terms of a limited number of parameters (typically one). The other parameters that would be needed for a more complete description of the hazard are typically considered in the response analysis and fragility evaluation.

8.34. The hazard analysis (the estimation of the frequency of exceedance of a particular severity) should be based on a probabilistic evaluation specific to the site.

8.35. Analysis of time trends (e.g. variation of meteorological and hydrological parameters in time due to climate change) should be performed to confirm the absence of trends towards increased frequency of the hazards. Recent, short term trends to decreasing hazard frequencies should not be accounted for unless they are well understood as being caused by processes having a non-random nature.[35]

8.36. When the hazard frequencies are developed on a regional or generic basis, an assessment should be performed with the aim of understanding the extent to which these data are applicable to the specific site and are up to date. The uncertainties associated with the use of regional and generic data should be reflected in the family of hazard curves, if provided (see para. 8.36).

[35] For example, an observed diversity in a river bed can be used for justification of a decreased frequency of associated transportation accidents.

8.37. When expert elicitation or another expert based process is to be used in developing the hazard curves, a procedure for the process should be established and followed. Recommendations on the hazard assessment methodology are provided in NS-G-3.1 [22], SSG-9 [23], SSG-18 [24] and SSG-21 [32].

8.38. When combined ~~coincidental~~ unrelated hazards are evaluated, the joint occurrence frequency should consider the individual hazard frequency, the duration of the individual hazards that are combined and the probability of conditions (e.g. seasonality) that allow the hazards to occur simultaneously.

8.39. When combined correlated hazards are evaluated, the level of correlation used in the joint occurrence frequency estimate should be justified if full correlation is not assumed.

8.40. When combined consequential hazards are evaluated, a conditional probability of the secondary hazard (e.g. water elevation due to a seismic-induced tsunami) to occur following the primary hazard of specific parameter (e.g. PGA or spectral acceleration for the seismic hazard) should be developed to allow for the quantification of the combined hazard effect.

Seismic hazards

8.41. The occurrence frequency of earthquake ground motions~~s~~ at the site should be based on a site specific probabilistic seismic hazards assessment (see Refs [7, 25, 31]).

8.42. Probabilistic seismic hazard assessment should be conducted in accordance with the recommendations provided in SSG-9 [23].

8.43. The range of parameters used to characterize the seismic hazards should cover the acceleration range of interest, e.g. from ‘no failure’ to the ‘screening limit’, in order to accurately estimate the seismic risk.

8.44. For the lower bound parameter value for use in the hazard analysis, it should be demonstrated that seismic events with any lower parameter value will not cause any damage to structures and components, including those off the site, such as power lines and pipework carrying hazardous material.

High winds

8.45. The model used for the calculation of frequencies and intensities for high winds should be based on site specific data that reflect recent available regional and site specific information. The analysis should incorporate at least the worst weather conditions experienced at the site. Thus, recent, short term trends in decreasing frequencies of high winds should not dominate in the assessment of wind frequencies.

8.46. Wind hazard assessment should be conducted in accordance with the recommendations provided in SSG-18 [24].

8.47. The range of parameters used to characterize the wind hazard should cover the range of interest, e.g. from ‘no failure’ to the ‘screening limit’, in order to accurately estimate the wind risk.

8.48. The high wind hazard assessment should consider the relevant time trends (e.g. climate change).

8.49. For the evaluation of extratropical windstorms and other phenomena involving high straight winds, the recorded wind speed data appropriate to the site should be used. Uncertainties that arise from a lack of weather stations should be accounted for conservatively in developing the hazard curve for high winds.

External floods

8.50. Calculation of the frequency and consequences of external floods at the site should be based on a probabilistic analysis that reflects recent, available, site specific information. When data for the site are only available for a short period, regional data on floods should be used with confirmation of the applicability of these data (i.e. correlation analysis could be used to confirm the applicability of the regional data for the site).

8.51. External flood hazard assessment should be conducted in accordance with the recommendations provided in SSG-18 [24].

8.52. The uncertainties in the models and parameter values should be properly accounted for and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived. The analysis of frequencies and consequences for extreme river floods should include floods due to single or cascade dam failures.

8.53. Calculation of the frequency and consequences of extreme ocean floods should be based on a probabilistic analysis that reflects recent, available, site specific information. These data should be supported by data for a longer period for other coastal areas, with proper account made for the topography of the area, both within the adjusted coastal area and on the land. The combination of high waves and high winds should always be considered.

8.54. Calculation of the frequency and consequences of extreme lake floods should be based on a probabilistic analysis that reflects recent, available, site specific information. The effects of the wind induced waves should always be considered, including any potential tornado induced water displacement.

8.55. Calculation of the frequency and consequences of tsunamis should be based on reliable regional data supported by engineering analysis. The uncertainties associated with the frequency and consequences of tsunamis should be taken into account.

8.56. The external flood hazard assessment should consider the relevant time trends (e.g. climate change).

Other natural hazards

8.57. A comprehensive database should be developed and used to support the frequency assessment for specific natural hazards. The database should include all relevant information necessary to support realistic and valid estimations of hazard curves. In particular, historical information on the occurrence of hazards in the vicinity of the site and in the region should be included in the database for the available data period.

8.58. The frequency of specific natural hazards should be estimated using both site specific and regional data. Correlation analysis should be employed in support of the use of regional data.

8.59. In particular cases, when neither site specific nor regional data are available, worldwide data could be used. In using the worldwide data, the applicability of these data to the site under consideration should be investigated and all assumptions applied for the analyses should be documented.

Human-induced hazards

8.60. Human-induced hazard assessment should be conducted in accordance with the recommendations provided in NS-G-3.1 [22].

8.61. Appropriate information (preferably in the form of a database) should be collected and used to support the frequency assessment for specific human-induced hazards. This information should include, at a minimum, the following data necessary to support realistic and valid estimations of the frequencies of hazards:

(a) Qualitative and quantitative information regarding the composition of explosive, hazardous or toxic material stored on the site and off the site within a predetermined radius of the nuclear power plant, as follows:
   (i). Potential hazard sources (within a predetermined radius of the nuclear power plant):
      • Off the site:
         — Oil storage station;
         — Gas or oil transportation line;
         — Vehicular transportation;
         — Railway transportation;
         —River and sea transportation;
         — Air transportation;
         — Other facilities.
      • On the site:
         — Storehouse (e.g. acids, hydrazine).
   (ii). Distance (in kilometres) of potential hazard sources to the nuclear power plant:
      • To the structures;
      • To buildings housing safety significant equipment;
      • To ventilation intakes.

(b) Locations of military or training facilities whose activities may affect the plant and a description of the frequency of training exercises.

(c) The potential for, and frequency of, accidents and their potential consequences (explosive capability).

FRAGILITY ANALYSIS FOR STRUCTURES AND COMPONENTS

General aspects

8.62. The fragility[36] of structures and components should be evaluated using plant specific information when available and to the extent necessary for the purpose of the analysis

[36] Fragility is the conditional probability of failure of a system, structure or component for a given hazard input level.

(bounding analysis or detailed analysis) and accepted engineering methods. Findings from plant walkdowns should be considered in these analyses.

8.63. The fragility analysis should not be limited to on-site structures but should include off-site structures such as power lines and pipework carrying hazardous materials, as failures involving such off-site structures may result in initiating events, such as loss of off-site power or a blast. Such failures may be highly correlated if the fragilities are low.

8.64. The fragility should be expressed as a function of the hazard parameter. The fragility analysis should include uncertainties in the underlying information, in particular when data other than plant specific data are used (i.e. generic data).

8.65. When combined hazards are considered, all the hazards-specific failure mechanisms resulting in SSC failure modes should be added in the Level 1 PSA model. If the combined hazards have different failure mechanisms, the failures should be represented by the individual hazard fragilities~~,~~. ~~i~~If the combined hazard has similar failure mechanism, the compounded fragility should be considered.

Seismic hazards

8.66. The initial list of structures and components for seismic fragility analysis should include all structures and components that are included in the Level 1 PSA model for internal initiating events. The list should be expanded to include all structures and components and their combinations that, if failed, could contribute to core damage frequency or large release frequencies; the latter is important for Level 2 PSA considerations.

8.67. The seismic equipment list (SEL) should be supplemented by any structure, system or component associated with any combined hazard identified as described in para. 6.11 and retained in the analysis. Depending on the retained combined hazard this may include dams, tsunami walls, internal flood*ing* source*s* or internal fire sources identified systematically. Details on the development of the SEL are provided in [31].

8.68. All realistic failure modes of structures and components that interfere with the operability of the equipment during and after an earthquake should be identified through a review of the plant design documents and a plant walkdown.

8.69. Fragilities should be evaluated for all relevant failure modes of structures (e.g. sliding, overturning, yielding, excessive drifts), equipment (e.g. anchorage failure, impact with adjacent equipment or structures, bracing failures, functional failures, pressure boundary breach for flooding and spray considerations) and soil (e.g. liquefaction, slope instability, excessive differential settlement) that are found to be important. Details of seismic fragility analysis are provided in [25] and [31].

8.70. The limiting fragility for a component should be used as a surrogate for the fragility associated with the fire ignition failure mode. Conditional ignition probabilities should be used to relate the functional failure to the fire ignition. See Ref. [33] for an example.

8.71. The fragility analyses should be supported by a plant walkdown. The walkdown should focus on the anchorage and lateral seismic support.

8.72. The potential for seismic interaction (e.g. possibility that structure, system or component could fall on to a~~n~~ seismic equipment list item), including the potential for additional interactions with fires and floods should also be included in the focus of the walkdown.

8.73. Calculations of parameters relating to seismic fragility (e.g. median seismic capacity of structures and its variability) should be based on plant specific data supplemented by data from actual earthquakes, data from fragility tests and data from generic qualification tests.

8.74. When structures and components of a low fragility are to be screened out on the basis of generic data, it should be proven that the generic data are used in a conservative manner and that no relevant plant and site specific features are neglected.

8.75. The seismic responses of structures and components at their failure level should be estimated on the basis of site specific earthquake response spectra anchored to a ground motion parameter (e.g. averaged spectral acceleration).

8.76. Uncertainties in the input ground motion and structural and soil properties should be taken into account in developing joint probability distributions for the responses of structures and components located in different buildings.

8.77. For all structures and components that appear in dominant accident sequences, it should be ensured that the associated site specific fragility parameters are derived on the basis of plant specific information. This is essential to avoid distortion of the contribution of seismic hazards in the results of, and insights from, the Level 1 PSA.

High winds

8.78. In assessing the impact of high winds, consideration should be given to specific features of exterior barriers (i.e. walls and roofs) surrounding SSCs important to safety, any weather exposed SSCs, or combinations thereof, and the consequences of damage from impact of windborne missiles that may result in an initiating event. A survey of the plant buildings and their surroundings should be made to assess the number and types of object that could be picked up by high winds and which could become missiles. Probabilities of missile strike should also be developed on the basis of state of the art methodologies.

8.79. An evaluation should be performed to estimate plant specific, realistic fragilities in respect of high winds for those SSCs, or combinations thereof, whose failure may lead to an initiating event.

8.80. In evaluating wind related fragilities of structures and components, plant specific data should be used. In the assessment, any structures that could fall into or onto structures that are important to safety, thereby causing damage, should be considered. In this assessment, findings from plant walkdowns should be used as an important source of information.

8.81. A family of fragility curves corresponding to a particular failure mode for each structure or component should be constructed and expressed in terms of median wind speed capacity and uncertainty characteristics (e.g. logarithmic standard deviations), representing randomness in capacity and uncertainty in median capacity of structures or components. More details on fragility analysis for high winds are presented in Section 5.2 of [28].

External floods

8.82. An analysis of dam failures should be performed for conditions corresponding to the high flood level in the river and associated frequencies should be determined.[37]

8.83. In evaluation of fragilities of structures and components in respect of external floods, plant specific data should be used. In the assessment, any structures that could fall into or onto structures important to safety, thereby causing damage, should be considered. In this assessment, findings from plant walkdowns should be used as an important source of information. All structures located at low levels, in particular intakes and ultimate heat sinks, should be included in the consideration.

8.84. The fragility analysis should include immersion, dynamic loads on structures and components from waves, and foundation failures (soil erosion). More details on fragility analysis for external floods are presented in Section 5.3 of [28].

Other natural hazards

8.85. The general aspects and recommendations for the fragility analysis of seismic hazards, high winds and external floods should be followed for other natural hazards as applicable.

Human-induced hazards

8.86. The general aspects and recommendations for the fragility analysis of seismic hazards, high winds and external floods should be followed for human-induced hazards as applicable. More details on fragility/capacity analysis for aircraft impact are presented in Section 5.4 of [28]. More details on fragility/capacity analysis ~~and~~ for explosions and hazardous releases are presented in Section 5.5 of [28].

INTEGRATION OF EXTERNAL HAZARDS IN THE LEVEL 1 PSA MODEL

General aspects

8.87. The Level 1 PSA model for internal initiating events is almost always used as a basis for the Level 1 PSA model for external hazards. The Level 1 PSA model should be adapted from the Level 1 PSA model for internal initiating events to incorporate aspects that are different, owing to the impact of external hazards. The major impacts of the hazard that could lead to different classes of internal initiating event (e.g. large loss of coolant accident, small loss of coolant accident, transient) or which could lead directly to core damage should be assessed in the selection of the appropriate event tree from the PSA model for internal initiating events (e.g. by use of a hazard event tree). Annex II presents an example of a seismic event tree for seismic hazards. The appropriate hazard curves for, and fragilities of, SSCs important to safety should be incorporated in the Level 1 PSA model for external hazards. All important dependencies, correlations and uncertainties associated with the specific hazard should be accounted for in the Level 1 PSA model for external hazards.

8.88. Probabilities relating to recoveries and post-trip human errors should be revised in order to assess the impact of the external hazards on the credited recoveries and human actions modelled in the Level 1 PSA for internal initiating events.

[37] The probability of dam failures should be calculated for different levels in the river. It is typical to assume dam failure for a river level above the dam failure design level.

8.89. The assessment of Type C HFEs for external hazards should include the following three cases:

(a) HFEs that are included in the Level 1 PSA for internal initiating events, but are also relevant for the hazard scenario. In this case, it should be checked whether there is a need to revise the assessment of performance shaping factors due to the possibility that it might be harder for operating personnel to implement actions than in the base case.
(b) HFEs that are relevant only for a specific external hazard (e.g. relay reset after seismic events). In this case the methods to assess external hazard specific HFEs may usually follow same principles as the other types of HFE.
(c) Undesired responses by operating personnel to spurious alarms and indications.

8.90. The Level 1 PSA model for external hazards should reflect the as built and as operated plant conditions.

Seismic hazards

8.91. The Level 1 PSA model for internal initiating events should be adapted to incorporate seismic specific aspects that are different from the corresponding aspects of the Level 1 PSA model for internal initiating events. Details of integration of seismic events in PSA model are provided in [25] and [31].

8.92. At many plants, plant manual shutdown is initiated for a seismic hazard over a certain magnitude (e.g. 50% of the design basis earthquake). A Level 1 PSA model for seismic hazards should reflect this, even for cases where the power conversion system has a high seismic capacity and where automatic reactor scram can be avoided.

8.93. The Level 1 PSA model for seismic hazards should include all important seismically induced initiating events that can lead to core damage. In particular, initiating events leading to scenarios of the following type should be modelled:

(a) Failures of large components (e.g. reactor pressure vessel, steam generators, pressurizer).
(b) Loss of coolant accidents of various sizes and locations. Seismically induced very small loss of coolant accidents due to ruptures of small lines (e.g. impulse lines) should also be considered in the Level 1 PSA model for seismic hazards as an additional failure mode.
(c) Loss of off-site power.
(d) Transients (with and without failure of the power conversion system), including losses of various support systems.

8.94. The models for specific accident sequences should be added to those from the Level 1 PSA for internal initiating events when seismically induced initiating events lead to specific accident scenarios not considered in the Level 1 PSA model for internal initiating events. The Level 1 PSA model for internal initiating events should be expanded for the purpose of including seismic hazards in the Level 1 PSA in order to incorporate failures of a wider scope of components or component failure modes, such as failure of passive components (e.g. structures, buildings, distribution systems, cable trays, relay chattering). The effects on reactor internals, in particular the sticking of a control rod due to the impact of a seismic event on the reactor core, should be considered.

8.95. All SSCs modelled in the Level 1 PSA for internal initiating events and those SSCs for which seismically induced damage can have an effect on accident sequences should be incorporated into the Level 1 PSA model for seismic hazards.

8.96. The Level 1 PSA model for seismic hazards should include all non-seismic related failures, unavailabilities and human errors that can contribute measurably to the core damage frequency.

8.97. The model for seismically induced damage of SSCs should thoroughly take into account all dependent failures of the equipment located in the building after damage of the building due to a seismic event. If dependencies of this type are to be eliminated from the model or if their significance in the model is to be decreased, this should be justified.

8.98. The seismic hazard assessment, seismic fragilities, dependencies between SSCs, non-seismically-induced failures, unavailabilities and human errors should be appropriately integrated into the Level 1 PSA model for seismic hazards.

8.99. As discussed in para. 8.89, a thorough check and associated adjustment should be performed in relation to recovery actions and probabilities of human errors. Recovery actions that cannot be performed due to the impact of seismic events of certain magnitude should be removed from the Level 1 PSA model; alternatively, probabilities of failure whilst performing the action should be increased. All post-initiator human errors that could occur in response to the initiating event, as modelled in the Level 1 PSA for internal initiating events, should be revised and adjusted for the specific seismic conditions. At a minimum, the following seismically induced effects on the performance shaping factors for operating personnel should be taken into account:

(a) Availability of pathways to specific SSCs after a seismic event;
(b) Increased stress levels;
(c) Failures of indication or false indication;
(d) Failure of communication systems;
(e) Scenarios with consequential fire and flood;
(f) Other applicable factors impacting the behaviour of operating personnel.

8.100. Seismically induced fires and floods should be included in the Level 1 PSA model for seismic hazards, unless it is clearly justified that other seismic damage bounds additional effects from seismically induced fire and floods. Plant impacts associated with induced fires and floods scenarios should be consistent with the fire and flood scenarios discussed in paras 7.48–7.64 and 7.79–7.84, respectively[38].

8.101. In quantifying the core damage frequency, key information about each accident sequence and the minimal cutset should be available as the result of model quantification, in addition to the integrated results.

8.102. Integration and quantification of the Level 1 PSA model for seismic hazards should be performed so that uncertainties from each seismic input into the Level 1 PSA (i.e. frequencies of seismic hazards, seismic fragilities, dependencies and aspects relating to system

[38] Multiple independent fires and floods could be typically screened out based on low frequency of occurrence. However, multiple fire and flood risk may come up if multiple equipment are damaged simultaneously.

analysis) are properly propagated through the model for obtaining correct uncertainty characteristics of the core damage frequency.

High winds

8.103. The Level 1 PSA model should include all initiating events caused by high winds and should be as complete as necessary to model all wind related effects.

8.104. The consideration of accident sequences initiated by high winds should include site specific hazard curves and the fragilities of all structures for which damage may lead to the disabling of the equipment modelled in the Level 1 PSA. Other factors to be considered should include unavailabilities or failures of the equipment and human errors that are not related to high winds. Probabilities of human errors should be adjusted to take into account the effects of wind on performance shaping factors as discussed in para. 8.89.

External floods

8.105. The consideration of accident sequences initiated by external floods should include the site specific hazard curves and the fragilities of all SSCs for which damage may lead to the disabling of the equipment modelled in the Level 1 PSA. Other factors to be considered should include unavailabilities or failures of the equipment and human errors that are not related to external floods. Probabilities of human errors should be adjusted to take into account flood effects on performance shaping factors (in particular, the accessibility of the equipment) as discussed in para. 8.89.

8.106. Uncertainties, dependencies and correlations should be thoroughly accounted for in developing accident sequence models for initiating events induced by external floods.

Other natural hazards

8.107. The general aspects and recommendations for model integration of seismic hazards, high winds and external floods should be followed.

Human-induced hazards

8.108. The general aspects and recommendations for model integration of seismic hazards, high winds and external floods should be followed.

DOCUMENTATION AND PRESENTATION OF RESULTS

General aspects

8.109. Paragraphs 8.109–8.119 provide recommendations on meeting Requirement 20 of GSR Part 4 [3] on documentation for Level 1 PSA for external hazards. The screening analysis, bounding analysis and detailed analysis for Level 1 PSA for external hazards should be documented in a manner that facilitates peer review, as well as future upgrades and applications of the Level 1 PSA, as follows:

(a) The screening of each specific external hazard should be documented in a manner that describes the processes that were used and provides details of the methods used, assumptions made and their bases.

(b) A description of the methods used for determining the hazard curves for each external hazard should be provided, including the following:
  (i). The data used for the determination of the hazard curves;
  (ii). The technical interpretations that are the basis for inputs and results;
  (iii). The underlying assumptions and associated uncertainties.
(c) A detailed list of SSCs subjected to the fragility analysis should be provided, together with the following:
  (i). The location of each SSC;
  (ii). The key assumptions and methods used for the fragility analysis;
  (iii). The dominant failure modes for each SSC;
  (iv). The sources of information for the analysis.
(d) Those SSCs that are not subjected to fragility analysis should also be discussed and the basis for their screening out from the Level 1 PSA model should be provided.
(e) The specific adaptations made to the Level 1 PSA model for internal initiating events should be thoroughly documented, with an indication of the motivation for each adaptation.
(f) The final results of the bounding analysis and detailed analysis should be documented in terms of core damage frequencies, significant minimal cutsets and significant accident sequences for each scenario associated with external hazards. The general recommendations for documentation presented in paras 3.15–3.23 should be also followed.

8.110. Major outputs of the Level 1 PSA for external hazards should be presented, as follows:

(a) Core damage frequencies and their uncertainty distributions;
(b) Results of sensitivity studies;
(c) Lists of significant accident sequences and significant minimal cutsets;
(d) Discussion of the technical basis for the significant sequences and significant minimal cutsets;
(e) Description of major contributors to the uncertainties. Contributors to both epistemic and aleatory uncertainties should be discussed.

Seismic hazards

8.111. A description of the specific methods used for the characterization of seismic sources and of the selected parameters should be provided. In particular, the specific interpretations that are the basis for the modelling inputs and results should be thoroughly documented.

8.112. The following information should be included in the seismic Level 1 PSA model documentation:

(a) A list of SSCs considered in the Level 1 PSA for seismic hazards;
(b) The fragility characterization and the technical bases for this for each SSC;
(c) Quantified probabilities of damage for the range of seismic hazards modelled in the Level 1 PSA;
(d) Significant failure modes for SSCs and the location of each SSC
(e) Specific adaptations made in the Level 1 PSA model for internal initiating events to take into account the impact of seismic events;

(f) Comprehensive information on the dependencies (in particular, spatial interactions) modelled in the Level 1 PSA for seismic hazards, as well as any assumptions applied to eliminate or decrease the impact of the dependencies.

8.113. The basis for screening out any structure, system or component should be described fully.

8.114. The methodology and procedures used to quantify seismic fragilities should be documented. This should include the following different aspects of seismic fragility analysis:

(a) Seismic response analysis;
(b) Steps involved in screening;
(c) Plant walkdown;
(d) Review of design documents;
(e) Identification of critical failure modes for each SSC;
(f) Calculations of fragilities for each SSC.

8.115. The procedures for plant walkdowns, the compositions of walkdown teams, and the observations and conclusions made from the walkdown should be fully documented.

High winds

8.116. The Level 1 PSA for high winds should be documented in a manner that facilitates the review, application and updating of the Level 1 PSA. In particular, the following information should be included in the documentation:

(a) A description of the specific methods and data used for determining the hazard curves for high winds;
(b) A description of changes made in the Level 1 PSA model to take into account effects relating to high winds;
(c) A list of all SSCs considered in the analysis, together with the justification for the SSCs that are screened out from the analysis;
(d) The methodology and data used to derive wind fragilities for all SSCs modelled in the Level 1 PSA;
(e) The final results of the Level 1 PSA in terms of core damage as well as useful intermediate results.

External floods

8.117. The Level 1 PSA for external floods should be documented in a manner that facilitates the review, application and updating of the Level 1 PSA. In particular, the following information should be included in the documentation:

(a) A description of the specific methods and data used for determining the hazard curves for external floods;
(b) A description of changes made in the Level 1 PSA model to take into account effects relating to external floods;
(c) A list of all SSCs considered in the analysis along with justification for the SSCs that are screened out from the analysis;
(d) The methodology and data used to derive flood fragilities for all SSCs modelled in the Level 1 PSA;

(e) The final results of the Level 1 PSA in terms of core damage as well as selected useful results.

Other natural hazards

8.118. The recommendations for documenting and presenting results in paras 8.109–8.117 should be followed, as applicable.

Human-induced hazards

8.119. The recommendations for documenting and presenting results in paras 8.109–8.117 should be followed, as applicable.

9. LEVEL 1 PSA FOR SHUTDOWN STATES

GENERAL ASPECTS OF LEVEL 1 PSA FOR SHUTDOWN STATES

9.1. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 [3] for a Level 1 PSA for shutdown states[39] for fuel in the reactor core and during fuel handling. The recommendations for Level 1 PSA for fuel in the spent fuel pool are provided in Section 10. In principle, the Level 1 PSA for shutdown states for internal initiating events is based on the same methodology as the Level 1 PSA for power operating states outlined in Section 5. Therefore, the structure of this section corresponds largely to that of Section 5 and the general framework for analysis depicted in Fig. 1, unless otherwise advocated by the specifics of shutdown states. Repetition of contents has been avoided and instead reference is made to earlier sections in this Safety Guide, unless approaches and conditions for shutdown states necessitate specific descriptions. However, it should be noted that the objective of the analysis is not necessarily the determination of a core damage frequency, since fuel damage frequency and inadvertent criticality may also be risk metrics of interest.

9.2. Internal and external hazards can be as important for shutdown states, as for power operating states. The approaches discussed in Sections 6–8 of this Safety Guide apply, but have to be modified in accordance with the specific characteristics of shutdown states. The scope of initiating events is, in principle, identical, but screening of events might lead to a different pattern. This is primarily the case in situations where the duration of shutdown states is much shorter compared with the duration of power operation. Obviously, the probability of occurrence of an external hazard is then much smaller in the shutdown state. On the other hand, the consequences can be very different for shutdown states. For example, in the handling of heavy equipment, careful consideration may need to be given to seismic events or external explosions and external floods could also lead to different accident sequences in the plant.

9.3. During shutdown, the following main activities are typically performed in a light water reactor :

(a) Achieving shutdown from power operation;
(b) Operation of the residual heat removal system;

[39] For low power operation all recommendations provided in Sections 2-9 are applicable with due account being taken of the potential reduced power level and different interlocks and system configurations compared to power operation.

(c) Opening of the reactor pressure vessel, flooding of the cavity;
(d) Refuelling;
(e) Maintenance and testing;
(f) Shutdown of the residual heat removal system and return to power operation.

For other types of reactor, the list of activities can be different, for example, opening of the reactor pressure vessel and flooding of the cavity will not be relevant for channel type reactors. In Annex III, examples of outage profiles of a pressurized water reactor and a boiling water reactor and examples of plant operating states are provided. The examples of typical operating states for CANDU-type reactors are presented in Ref. [13].

SPECIFICATION OF OUTAGE TYPES AND PLANT OPERATING STATES

9.4. In contrast to power operation, in shutdown states the operating configuration of the plant and conditions at the plant change significantly. Generally (for plants where refuelling is carried out off-line), there are three different types of outage, as follows:

(a) Regular refuelling outages with partial or complete relocation of the fuel from the reactor[40], during which major maintenance activities are also carried out;
(b) Planned outages, during which only specific maintenance activities are carried out;
(c) Unplanned outages that follow a disturbance during power operation with and without drainage of the reactor vessel and fuel reloading.

This is reflected in the plant's technical specifications, which are usually divided in accordance with different plant operating states, each having its own operability requirements on plant equipment.

9.5. It is considered good practice to analyse all types of outage mentioned in para. 9.4. The risks associated with refuelling outages should be assessed in full. It is essential that analysis of sequences following a disturbance be carried through until a safe and stable state is reached. Termination of the analysis at a fixed pre-defined sequence mission time may prevent meaningful results from being obtained. In many cases, as a first step, a typical outage is analysed. For reactors in operation, such an outage should be derived by starting from a recent outage and adding elements derived from the documentation of additional recent outages and from discussions with the personnel responsible for planning them. If necessary, certain elements of outages that are expected to contribute to risk should be evaluated separately. For example, in the cases of outages planned specifically for certain maintenance activities, a comparison of the risk associated with the planned outage with the risk associated with continued operation can be an important input to decision making.

9.6. Foreseeable changes to outage procedures should be incorporated in the analysis if one of the objectives of the PSA is to evaluate risks associated with future operation.

9.7. During shutdown, a large number and variety of plant configurations exist that would, if handled individually, lead to an excessive number of scenarios needing to be analysed. For

[40] For plant ~~operational~~ operating states with refuelling outages, when fuel is completely relocated into the spent fuel pool the recommendations provided in Section 10 should be applied.

dealing with the variety of plant configurations during shutdown, a limited number of plant operating states should be specified for which the plant status and configuration are sufficiently stable and representative.

9.8. To limit the number of combinations of plant operating states to a manageable size, some grouping of similar states will be necessary. Such grouping should take into account the following physical and technical aspects of the plant:

(a) Reactor criticality (and/or shutdown margin);
(b) The level of decay heat;
(c) Temperature and pressure in the reactor coolant system;
(d) Water level in the primary system;
(e) Open or closed reactor coolant system;
(f) Operability status of loops in the reactor coolant system;
(g) Location of the fuel;
(h) Availability of ~~mitigating system~~credited systems including support systems, including consideration of whether they are controlled automatically or by manual actions;
(i) System alignments;
(j) Status of the containment integrity.

9.9. For a Level 1 PSA for shutdown states, the plant operating states should be specified on the basis of actual operating experience and in accordance with current practices and procedures. Depending on the selection of the outage type performed in the previous step (see para. 9.5), an appropriate number of outages should be analysed in detail to determine the actual status of all parameters of interest at all times during the outage. Sources of information to be used for this purpose generally include the following:

(a) Shutdown and startup procedures;
(b) Outage plan for a specific outage or outages;
(c) General plant practice for outages;
(d) Technical specifications for outages;
(e) Guidelines for configuration control;
(f) Other documents providing information on outages (e.g. logbooks detailing boron concentration);
(g) Maintenance records (specifying duration of maintenance on specific components);
(h) Interviews with operating personnel and shift supervisors;
(i) Interviews with outage planners.

From such sources, all the information relevant for characterizing the plant operating states should be extracted and documented, especially the availability of safety functions and other relevant functions. An example for the selection of plant operating states is included in Annex III, in which 11 different plant operating states have been differentiated. It is emphasized, however, that for Level 1 PSA for shutdown, the analysis should be based on a substantially larger number of plant operating states, depending on the particular application of the PSA, e.g. for risk monitor applications.

9.10. For nuclear power plants at the design stage, information from analogous or reference plants should be used as much as possible. For completely new designs, a thorough assessment

of time needed for different operations for different types of outage should be performed. This information should be verified and updated at commissioning stage and during the first years of plant operation.

9.11. To ensure that the whole operating cycle is covered and in order to avoid missing contributors to risk from certain plant operating states, or to avoid double counting, the points of interface between plant shutdown operating states (including power operation) should be clearly specified in terms of the duration, power level and system configuration of each plant operating state, the frequency (per calendar year) of entry into each plant operating state and the initiating events. Data on operating history should be used for this purpose.

INITIATING EVENTS ANALYSIS

9.12. In principle, the identification of initiating events follows the same approach as described in paras 5.11–5.39. Therefore, loss of coolant accidents and transients should be addressed, as well as initiating events that are identified in the analyses of internal and external hazards. As a starting point, a generic list can be compiled from the analysis of power operation. This list will need to be modified and extended in accordance with the steps described in paras 9.13–9.23.

9.13. In para. 5.11, initiating events ~~is~~ are defined with relation to the core damage. As indicated in paras 9.4–9.8, the core can be in very different configurations in different shutdown states. Fuel stored in ~~a~~ a spent fuel pool~~s~~ both internal ~~and~~ or external to the reactor building is covered separately in this Safety Guide as part of the PSA for spent fuel pool (see Section 10)~~s~~. Therefore, a number of initiating events are unique to shutdown conditions and these will be different from those identified in the Level 1 PSA for power operation (see examples in Annex III). In addition, many initiating events relating to maintenance activities or operating procedures may be human-induced. The major categories of initiating events that are of interest for a Level 1 PSA for shutdown states are events that threaten safety functions such as heat removal, primary circuit inventory or integrity and reactivity control. This implies that, as well as core damage, damage to fuel outside the reactor pressure vessel might be an ~~end point~~end state of the accident sequences in a Level 1 PSA for shutdown states; such ~~end point~~end states are often termed fuel damage states and criticality events. Examples of initiating events in a shutdown PSA for CANDU-type reactors are provided in Ref. [13]. It is necessary to decide which of these ~~end point~~end states need to be included in the analysis. This decision should be correlated with the probabilistic safety goals or criteria to be verified, if specified in national regulations or guidelines~~based on national targets for risk~~. The characteristics of such ~~end point~~end states are highly specific to the reactor type and therefore cannot be addressed here in depth. In most cases, a Level 1 PSA for shutdown states considers the events that can lead to the following ~~end point~~end states:

(a) Damage to fuel due to loss of cooling to the fuel;
(b) Damage to fuel during handling;
(c) Damage to fuel due to dropping of heavy loads;
(d) Damage to fuel in criticality event due to changes in fuel configuration (part of the fuel can be in spent fuel).

9.14. Care should be exercised to identify clearly the initiating events of interest. To complement the generic list obtained in accordance with para. 9.12, systematic techniques should be used for the identification of initiating events. In addition to the methods

recommended in para. 5.13–5.23, a systematic examination of plant procedures for changing the configuration of the reactor coolant system and of procedures for equipment testing and maintenance should be performed. The ~~end point~~end states of the accident sequences for initiating events in shutdown states could differ from core damage states.

9.15. Identification of potential human errors during the execution of plant procedures for shutdown states for different types of outage is one of the key objectives of this process and it should incorporate knowledge of plant procedures and plant walkdowns to familiarize PSA specialists with working practices in the plant.

9.16. To ensure adequate completeness of the list of initiating events for the Level 1 PSA for shutdown states, the following sources of information should be reviewed in addition to the list from the PSA for power operation:

(a) Level 1 PSAs for shutdown states from other similar plants;
(b) Plant operating history;
(c) Experience at similar plants;
(d) Generic data from operation in shutdown states.

Some publicly available sources of such information are as follows:

(a) Generic studies (e.g. information on boron dilution events caused by inadvertent pumping of unborated water through the core);
(b) Event reports from licensees;
(c) Event reports from international organizations and plant owners' groups.

9.17. Initiating events should be grouped in a way that all initiating events in the group can be analysed using the same event tree and fault tree model (see paras 5.32–5.39). In addition to the criteria listed in paras 5.32–5.39 the basis for grouping initiating events in shutdown states should include ~~the following~~that all initiating events in the group:

(a) ~~All initiating events in the group~~ have a similar effect on the availability and operation of ~~safety systems and support systems~~credited SSCs.
(b) ~~All initiating events in the group~~ have similar success criteria for ~~safety systems, support systems and other systems necessary for mitigating the event~~credited systems.
(c) ~~All initiating events in the group~~ place similar requirements ~~on~~ for the operator actions.

Similar initiating event can occur in different plant operating states (see Annex III), but as availability of systems and success criteria are in general different for the different plant operating states, grouping across plant operating states is not feasible in most cases.

9.18. The characteristics for the group should be defined on the basis of the most restrictive events within the group (see para. 5.35).

9.19. As in the case of PSA for power operation, quantification of the frequencies of initiating events should follow standard Level 1 PSA practices, as described in paras 5.154–5.158. However, the quantification of initiating event frequencies for shutdown states should take into account the higher possibility of initiating events caused by HFEs and therefore human reliability analysis methods should be also used when applicable. In addition, plant specific

items such as equipment configuration and availability, technical specifications and outage management, including refuelling operations, should be taken into account.

9.20. In a Level 1 PSA for shutdown states, the frequency of initiating events can be first defined in terms of the expected hourly rate of occurrence in a specific plant operating state and then recalculated with the actual state duration taken into account. However, the frequencies should not be defined in this way if the initiating event has arisen due to events relating to the occurrence of the plant operating state, rather than its duration (e.g. some initiating events may be related to testing or transition activities and the frequencies of such events would not scale in accordance with the duration of a plant operating state).

9.21. There are basically three approaches to quantifying the frequencies of initiating events occurring in a given plant operating state (see paras 5.154–5.158), as follows:

(a) Direct estimation from operating experience (from the plant being analysed, other plants of similar design, or generic type of reactor);
(b) Estimation from frequencies determined in Level 1 PSA for power operation, with supplementary analysis (i.e. reassessment of the frequencies of loss of cooling accidents for a depressurized or opened reactor);
(c) Use of a logic model, including all the foreseen inputs leading to the initiating event.

9.22. To account correctly for dependencies between an error that results in an initiating event (e.g. an error resulting in a loss of the decay heat removal function) and an error made in responding to that event (e.g. failure to recover the decay heat removal function), the errors that result in an initiating event should be modelled explicitly.

9.23. The overall results of assigning initiating events to plant operating states should be presented in the form of a table or other type of overview. An example is presented in Annex III.

ACCIDENT SEQUENCE ANALYSIS

Safety functions~~, safety systems~~ and success criteria

9.24. Recommendations on the general approach to accident sequence analysis are provided in paras 5.40–5.70. Although decay heat levels during shutdown are generally much lower than immediately following shutdown from power operation, the characteristics of the possible plant configurations may still give rise to events that challenge the fulfilment of safety functions. The analysis should take account of the following aspects:

(a) Owing to the disabling of automatic actuation of ~~safety~~ credited systems in shutdown, the availability of safety equipment might be reduced and the dependence on actions by operating personnel might be increased.
(b) The integrity of the primary cooling system might be compromised and additional bypass of the containment might be possible.
(c) The performance of a front line system will depend in general on the particular initiating event, the characteristics of the plant operating state and the decay heat level.
~~(c)~~(d) The number of available redundant trains or components for a certain safety function which should be defined taking into account the minimum requirements of operational limits and conditions as well as operational experience.

9.25. Functional performance criteria should be used to specify success criteria for the various systems, which may differ from the success criteria specified for a Level 1 PSA for power operation.

Analysis to support the specification of success criteria

9.26. The fault tree models constructed for the Level 1 PSA for power operation should be revised as appropriate. Even if the logic and the response of the system remain basically the same as at power operation, possible changes in the conditional availabilities of components or systems should be taken into account.

9.27. To ensure that core cooling assumptions are correct, thermohydraulic calculations should be performed to determine realistic success criteria. The level of detail of the thermohydraulic analyses should correspond to the requirements of the systems analyses and the primary system configuration. For transitional operating states (during shutdown and startup) and under hot shutdown conditions, the configuration and conditions of the primary systems are in some cases similar to those for transients initiated from power operation, and models designed for thermohydraulic calculations for power operation will be applicable. In other cases, the applicability has to be demonstrated. For other plant operating states, a comparison of the primary system characteristics and the model capabilities should be carried out to assess the applicability of a particular code. For example, for light water reactors, the thermohydraulic analyses to support the specification of success criteria should, as a minimum, take into account the following factors:

(a) The status of the primary circuit pressure boundary;
(b) Vessel head removed or de-tensioned;
(c) Safety valve removed or primary system vent open;
(d) Loops isolated or nozzle dams installed;
(e) Water level in steam generators;
(f) Primary circuit parameters (temperature, pressure, presence of non-condensable gas, shutdown margin);
(g) Water level in the primary system;
(h) Residual heat level;
(i) Isolation status of the containment;
~~(i)~~(j) Availability of protection systems for actuation of safety functions.

9.28. When performing thermohydraulic calculations, the violation of criteria for a particular fuel damage state should be assessed. These criteria and time to damage might be very different depending on whether the reactor is closed or opened.

Modelling of accident sequences

9.29. Event trees (see paras 5.59–5.63) or equivalent presentations should be used to model the response of the plant and operating personnel to initiating events. It is considered good practice to draw detailed event sequence diagrams, including human interactions, before modelling the accident sequences.

9.30. In the accident sequence analysis, the possibility of actions by operating personnel aimed at recovering reactor core cooling as well as water supply into the reactor from alternative sources should be considered as mitigation actions at a minimum.

9.31. Accident sequence modelling should be done by a multidisciplinary team, which should include specialists in human reliability analysis, from the beginning of the process of analysis.

Accident sequence ~~end point~~end states and plant damage states

9.32. As for power operation, the accident sequences should be grouped into plant damage states in order to reduce the number of possible distinct outcomes of the Level 1 PSA to a manageable number for further analysis (Level 2 PSA or Level 3 PSA) and for concise presentation of the study results. The expected accident progression (beyond core damage), including challenges to containment integrity and radionuclide transport, for all accident sequences that are grouped under a particular plant damage state should be qualitatively similar. On the other hand, there are modern analytical tools offering the possibility of modelling the accident sequences up to release categories. Such approaches do not involve such a grouping of plant damage states for the Level 1 PSA. Appropriate sequence mission times should be specified (see para. 5.52), taking into account the specific features and timing of the processes taking place.

9.33. The process of selecting the plant damage states for a Level 1 PSA for shutdown states should take account of the plant damage states specified for the Level 1 PSA for power operation (see para. 5.66). However, for a Level 1 PSA for shutdown states, additional plant damage states different from those for a Level 1 PSA for power operation should be identified. For example, additional plant damage states may be necessary for conditions unique to certain shutdown states such as those with the reactor vessel head removed or with the containment equipment hatch open.

The following additional accident sequence characteristics should be considered in specifying the plant damage states:

(a) Decay heat level (time since shutdown from power operation);
(b) Containment state — especially ~~where~~ when the containment is open;
(c) Conditions that determine the time to restore containment isolation and the potentially reduced effectiveness (leaktightness) of the containment during such time;
(d) The integrity of the primary system pressure boundary with vessel head removed, nozzle dams installed, safety valves removed, primary system vent open;
(e) The water inventory ~~of water~~ in the primary circuit.

9.34. Appropriate specification of the plant damage state will be decisive for results and their interpretation.

SYSTEMS ANALYSIS

9.35. As for Level 1 PSA for power operation, the objective of systems analysis for Level 1 PSA for shutdown states is to carry out detailed modelling of the system failures necessary for quantification of accident sequences. Fault tree analysis is the most widely used method for system modelling. Fault tree models constructed for power operation (see paras 5.73–5.94) may be utilized and adapted as far as possible. However, revisions to the existing models should be made if necessary, or new models may need to be developed, particularly in the following situations:

(a) Existing system models are not suitable for describing specific system behaviour in different plant operating states, for example, the system may be configured differently to accommodate maintenance or specific alignment of the system may change system success criteria (e.g. when one safety train is in scheduled maintenance).
(b) A particular system that was on standby during power operation is operating during shutdown.
(c) Actuation of a system is performed manually during shutdown, whereas in power operation actuation was automatic.
(d) The required mission time for systems may be significantly different.
(e) Success criteria change for different plant operating states.
(f) The number of trains initially available is different for each plant operating state.
(g) Time 'windows' and plant conditions are significantly different, which could influence the probability of success of recovery actions and allows repair activity to be credited.
(h) A particular system was not modelled as this was not necessary for power operation.
(i) Interconnection of particular systems is necessary to establish a configuration for a safety function that is used just in shutdown states, for example, using the spent fuel cooling system for core cooling; account should be taken of the procedure for this connection.
(j) A particular system was not modelled as this would only be necessary for the Level 2 PSA for power operation.

Examples of specific requirements for system modelling are given in Annex III.

ANALYSIS OF DEPENDENT FAILURES

9.36. As described in paras 5.89–5.94 for power operation, the objective of this analysis is to identify dependencies that may influence the logic and quantification of the accident sequences and system models. The main types of dependency in this regard are: functional dependence on supply systems and support systems; hardware sharing between systems or process coupling; physical dependence, including dependencies caused directly or indirectly by initiating events; dependencies on human interactions; and common cause failures. These dependencies should be included in the analysis.

9.37. As a point of departure from the conditions at power operation, the different support and front line systems as well as their interdependencies should be reviewed and checked regarding their applicability for the specific plant operating states. Testing and maintenance activities may create new sources of dependencies, such as coincident repairs or maintenance of redundant components that should be accounted for. Examples are presented in Annex III.

9.38. Revisions to the dependency models for power operation should be implemented as necessary, especially if the success criteria are different for shutdown or conditions are different for support systems, e.g. requirements for ventilation systems and power supply systems.

9.39. The alignment of systems and component outages should also be reviewed.

9.40. The various common cause failure mechanisms and the potential impact of maintenance and other activities specific to shutdown conditions on their occurrence should be identified.

HUMAN RELIABILITY ANALYSIS

9.41. In paras 5.99–5.121, the key aspects of human reliability analysis are explained; these aspects also apply to shutdown . The analysis of human failure events during shutdown is complex. Therefore, human reliability analysis should be performed in a structured and logical manner. As with other analysis tasks, the process of human reliability analysis should be thoroughly documented in a traceable way. Human reliability analysis should aim to generate failure probabilities which are both consistent with one another and consistent with the analysis carried out in other portions of the Level 1 PSA.

9.42. In accordance with para. 5.117, typical aspects conditions during shutdown, such as extensive use of external maintenance staff from external organizations, frequent overtime work and increased control room work need adequate consideration in the analysis. Account should also be taken of difficulties in work supervision and pressures due to tight schedules.

9.43. For human reliability analysis, close interaction between the HRA analyst and ~~with~~ plant operating personnel and maintenance personnel should be practised in order to ensure that plant design and operating features during shutdown are properly reflected in the analysis. If this is not possible, for example, for a plant in the design stage or construction stage, the analyst should attempt to gain knowledge based on practical experience gained from the operation of similar plants.

Type A human failure events — pre-initiator HFEs

9.44. Type A human failure events (see para. 5.105) consist of actions associated with testing, maintenance, repair and calibration that, if not carried out correctly, could lead to equipment unavailability. The process of identification and quantification of type A human failure events is similar to that for Level 1 PSA for power operation, but should take into account particular shutdown features, especially the following:

(a) Functional testing performed close to the end of the outage might be subject to difficult time constraints and therefore could have a high potential for human errors.
(b) Reduced availability of automatic realignment functions (e.g. no automatic closure signal for a valve that can be left open after a test).

Type B human failure events — HFEs that may cause an initiating event

9.45. Owing to the great variety of different maintenance measures, tests and changes of configuration, it cannot be expected that all possible human errors will have been observed in relation to the frequencies of initiating events specific to shutdown (e.g. drain down due to adverse valve alignment) . Therefore, the potential for human failure to contribute to initiating events should be assessed explicitly. This is also important for addressing the dependency with respect to response actions (type C actions). This assessment may result in identification of human failures that lead to unavailability of components, either immediately or as latent faults in the case of a demand modelled in the fault tree of an initiator. For the analysis, the following sources of information can be used:

(a) Written procedures for startup and shutdown of operation;
(b) Operating experience;
(c) Documents on outage planning, including technical specifications and testing and maintenance procedures.

Screening may be necessary for the analysis of type B human failure events to decide which failures can be screened out on the basis of a qualitative evaluation and for which a quantitative estimate or even detailed analysis is necessary. A possible approach is outlined in Annex III. The derivation of human error probabilities can be carried out as set out in paras 5.117–5.121.

Type C human failure events — post-initiator HFEs

9.46. Type C human failure events (see para. 5.105) are particularly important during shutdown because of the reduced level of plant automation. They tend to be significant contributors to core damage frequency in many Level 1 PSA studies for shutdown conditions. Thus, thorough consideration should be given to a realistic assessment of the failure probabilities of such interactions.

9.47. The methodology selected should take into account specific aspects relevant for modelling and quantifying type C human failure events in the framework of a Level 1 PSA for shutdown conditions in a systematic manner. Certain aspects may differ from the PSA for power operation, for example, as follows:

(a) More frequent actuation of alarms and standing alarms;
(b) Quality of procedural guidance;
(c) Status of training of operating personnel;
(d) Duration of time windows for response;
(e) Quality of interfaces that facilitate human actions in shutdownstates.

9.48. Care should be taken that values generated by the use of time reliability correlations specific to power operation are not uncritically accepted, since the time windows in shutdown states may be well outside the applicable ranges of such correlations.

9.49. The potential for errors in the diagnosis of the causes of initiating events should be addressed especially when event based procedures are to be used.

9.50. As in a Level 1 PSA for power operation, dependencies between human interactions in the same accident sequence should be taken into account (see paras 5.122 and 5.123). However, in the PSA model for shutdown states, it is particularly important to address the dependencies between type B and type C human failure events. If an initiating event such as a loss of decay heat removal is caused by a human error, the circumstances that led to the individual making the error will likely complicate the recovery of the decay heat removal function and may lead to increased failure probability compared with the case where loss of function was a result of mechanical failure.

DATA ASSESSMENT

9.51. The data necessary for quantification of the Level 1 PSA for shutdown conditions includes the following:

(a) Initiating event frequencies;
(b) Data relating to human error probabilities;
(c) Duration of plant operating states;
(d) Allowed outage times;
(e) Component reliability data;

(f) Maintenance unavailabilities, including overlapping maintenance based on operating history;
(g) Assessment of common cause failures;
(h) Other data needs.

The basic needs and approaches for data acquisition that have been described in Section 5 also apply to shutdown states. Data for the quantification of component reliability parameters that are specific for shutdown are less widely available than for power operation. Thus, a widely used approach has been to adapt data from power operation. This should not be done without transparent justification as regards the applicability of such data.

9.52. A major part of testing during planned outages serves to verify the function of the components that were previously undergoing maintenance, i.e. such tests are functional tests before equipment is put back into operation. Determination of unavailability should be related to the average test duration and to the duration of the plant operating state during which the component is tested.

9.53. Possible human interactions and probability of human errors in overriding alignments resulting from test and maintenance activities should be assessed.

9.54. The possibility of repair should be considered because it can significantly increase availability of credited ~~safety~~ systems in plant operating states for shutdown conditions. Neglecting repair may, in many cases, lead to an overestimation of risk, especially in post-initiator scenarios, crediting in the analysis the probability of recognizing the possibility of a specific repair option that would enhance the realistic consideration. 'Repair' here includes cases of short term recovery sufficient to fulfil the demands of the accident sequence under consideration. It should, however, be restricted to cases in which plant experience shows that there are good possibilities for recovery or the probability of success can be supported by engineering judgement and/or established repair procedures valid under the conditions of the accident sequence.

9.55. Dependency of repair times on the plant operating state should be taken into account. Such dependencies may be due to the accessibility of systems and equipment, the availability of staff to undertake repair, the availability of spare parts and, for some accident sequences, the level of radiation in the surroundings of the component to be repaired.

9.56. An appropriate reliability model should be selected in shutdown states to take into account that the components that are on standby during power operation might be in operation during an outage.

9.57. Components mission times are used in models to calculate the probability that operating equipment used to ensure some safety function to attain and/or maintain a stable shutdown state following an initiator fails to continue to operate. Components mission times can have a significant impact on the calculated probabilities of system failure. Assumptions regarding the mission time of components should be consistent with the modelling of accident sequences i.e. sequence mission time and system mission times, as well as with reliability data, as these may reveal a sensitivity to operation time.

9.58. If foreseeable changes in outage procedures are to be incorporated in the analysis, this might have implications on data acquisition. The changes might be such that the available

information on operating experience either cannot provide the necessary data or can only provide the necessary data after adaptation by analysis or engineering judgement.

QUANTIFICATION OF ACCIDENT SEQUENCES

9.59. For Level 1 PSA for shutdown states, quantification of accident sequences should be performed using the same techniques as for a Level 1 PSA for power operation. Use of other techniques, such as Markovian techniques instead of standard fault tree and event tree evaluation methods may have the potential to yield more realistic results for shutdown states in which long sequence mission times enable to credit recovery actions.

9.60. When reviewing the results of the quantification, as in the case of a Level 1 PSA for power operation, a careful review of the minimal cutsets obtained should be carried out. In a Level 1 PSA for shutdown states, the system models may have to be modified to represent the conditions of the different plant operating states. If system models are modified, cross-checking should be performed for the minimal cutsets obtained for similar accident sequences or systems in different plant operating states to ensure that any differences in these indeed reflect different plant operating states or sequence characteristics and do not stem from modelling errors.

IMPORTANCE ANALYSIS, SENSITIVITY STUDIES AND UNCERTAINTY ANALYSIS

9.61. For the uncertainty analysis, the same techniques should be used as for a Level 1 PSA for power operation (see paras 5.183 and 5.184).

9.62. Importance analysis and sensitivity studies should be performed using the same techniques as for a Level 1 PSA for power operation (see paras 5.178–5.185).

9.63. Sensitivity studies are an important part of the analysis in Level 1 PSA for shutdown states; they are aimed at analysing the potential impact of many factors specific to PSA for shutdown states. For example, the specific conditions that were selected to characterize a plant operating state may represent a wider range of conditions that can actually occur during the plant operating state. Compared with PSA for power operation, there may be different combinations of systems that are unavailable; some combinations may result from more conservative analysis and some from less conservative analysis. The plant operating state may have a longer or shorter duration. Times available for human action can vary considerably depending on the time of the plant operating state relative to plant shutdown. Success criteria can also vary depending on decay heat levels. These variations should be investigated, especially for cases where the assumptions used to model the plant operating state result in a dominant contribution to risk.

DOCUMENTATION AND PRESENTATION OF RESULTS

9.64. Paragraphs 9.64–9.74 provide recommendations on meeting Requirement 20 of GSR Part 4 [3] on documentation for Level 1 PSA for shutdown states. The structure of the Level 1 PSA report should comprise procedures for a Level 1 PSA for power operation and, in addition, sections for describing those aspects which are particular to Level 1 PSA for shutdown conditions should be added, such as a section describing in detail the process used for identification of outage types, plant operating states and initiating events.

9.65. The results obtained in each major step of the study, as discussed in the preceding sections, should be integrated and displayed, together with the important engineering insights

gained from the analysis. Assessments of the overall results and findings and a discussion of the uncertainty should be included in the documentation.

9.66. Frequently, written maintenance or operating procedures are improved or introduced in response to preliminary analysis findings. This should be also outlined in the documentation .

9.67. Finally, more general conclusions and recommendations should be presented and discussed. The following subjects should be included in the documentation to the extent necessary for decision making:

(a) Frequencies for end states representing core damage~~Core damage frequency~~ — important contributions integrated over all plant operating states:
  (i) Contribution of the dominant sequences;
  (ii) Contribution of the plant operating states;
  (iii) Contribution of groups of initiating events;
  (iv) Results of uncertainty analysis for core damage frequency;
  (v) Results of importance analysis and sensitivity studies for core damage frequency.
(b) Presentation of results for each plant operating state:
  (i). Contribution of dominant sequences;
  (ii). Contribution of groups of initiating events.
(c) Presentation of interface to Level 2 PSA (if necessary), comprising characteristics and frequencies of plant damage states.
(d) Qualitative insights and conclusions:
  (i). Interpretation of results and engineering insights;
  (ii). Conclusions and recommendations.

9.68. The presentation of the engineering insights and the recommendations should be such that they provide clear input to the decision making process.

9.69. Constructing a risk profile for a typical outage schedule, especially for a refuelling outage, can be helpful. Such a profile could, for example, show the core damage frequency for the different plant operating states as a function of outage time or time after the beginning of power reduction. An example risk profile is provided in Annex III.

9.70. The following detailed information from the Level 1 PSA for shutdown conditions should be included in the report:

(a) Significant minimal cutsets contributing to total core damage frequency;
(b) Significant minimal cutsets contributing to core damage frequency per plant operating state.

The level of significance of minimal cutsets should be determined in accordance with the objectives of the PSA.

9.71. The following should be included in the documentation:

(a) The contribution to core damage frequency of human errors and dependent failures;
(b) The contribution to core damage frequency of independent failures;

(c) The impact on core damage frequency of the various safety functions modelled in the event trees.

9.72. In addition to core damage frequency, other undesired ~~end point~~end states, for example, involving criticality or damage to the fuel pool and their frequencies should be assessed and the results documented.

9.73. The plant model and data should be sufficiently documented and configured in databases and computer files to enable the results to be reproduced and the models readily used for applications.

9.74. The drawing up of documentation should support regulatory review requirements.

10. SPECIFICS OF LEVEL 1 PSA FOR THE SPENT FUEL POOL~~S~~

10.1. In principle, the Level 1 PSA for the spent fuel pool is based on the same methodology as Level 1 PSA for the reactor core outlined in Sections 5-9. Accordingly, the general process for conducting Level 1 PSA for the reactor core should be adapted for the spent fuel pool, considering the specific aspects addressed in this section. Some of the topics addressed hereby are relevant to both the PSA for the reactor and the PSA for the spent fuel pool.

UNDESIRED ~~END POINT~~END STATES

10.2. The undesired ~~end point~~end states of interest regarding the Level 1 spent fuel pool PSA should be clearly defined. If they have been specified in national regulations or guidelines, the ~~The~~ national probabilistic safety goals or criteria applicable to the spent fuel pool should be the basis of specifying the undesired ~~end point~~end states of interest~~, provided that such goals or criteria exist~~.

10.3. A criterion (or criteria, if appropriate) should be developed to characterize the specified undesired end states. Regarding the core (see paras 5.42 and 5.43), it is often assumed that fuel damage occurs if design basis limits for the fuel are exceeded. In lack of detailed thermohydraulic analyses, fuel uncovery (i.e. when the water level in the spent fuel pool drops below the top of the active part of the fuel assemblies as a result of boiling or draining) may also be applied as a criterion to assume fuel damage.

~~10.3. Damage of fuel assemblies to a pre-defined degree should be considered to define the main end point of interest. Mechanical damage of a limited number of fuel rods or of one single fuel assembly during refuelling operation may be screened out from further assessment, if it can be justified that these events will not lead to a large radioactive release.~~

10.4. Beyond fuel damage, fuel uncovery and boiling of the pool water (e.g. for spent fuel pools located outside the containment) should also be considered in the identification process as a potential undesired ~~end point~~end state.

10.5. ~~A criterion (or criteria, if appropriate) should be developed to characterize the specified undesired end points. Regarding the core (see paras 5.42 and 5.43), it is often assumed that fuel damage occurs if design basis limits for the fuel are exceeded. In lack of detailed thermohydraulic analyses, fuel uncovery (i.e. when the water level in the spent fuel pool drops~~

~~below the top of the active part of the fuel assemblies as a result of boiling or draining) may also be applied as a criterion to assume fuel damage.~~ If necessary for risk assessment, damage of fuel assemblies to a pre-defined degree should be considered to define the main end point of interest. Mechanical damage of a limited number of fuel rods or of one single fuel assembly during refueling operation may be screened out from further assessment, if it can be justified that these events will not lead to a large radioactive release.

~~10.5.~~

10.6. Gross mechanical fuel damage due to e.g., internal hazards such as heavy load drops or falling objects (including a consequence of hazard induced structural failures) ~~–~~or hazard combinations should also be considered as an undesired ~~end point~~end state, since such events can challenge the design basis limits for the fuel.

PLANT OPERATING STATES

10.7. Modelling all risk relevant plant operating states may need to consider a large number and variety of spent fuel pool configurations together with the associated scheduled maintenance activities and the changes in the level of residual heat. Grouping of similar states should be conducted to limit the number of plant operating states to a manageable size.

10.8. Such grouping should take into account the following physical and technical aspects and differences in fuel loading patterns of the plant states:

(a) The water inventory of the pool;
(b) The residual heat of the fuel assemblies stored in the spent fuel pool;
(c) The spent fuel pool system configuration (i.e. the spent fuel pool is isolated from or interconnected to the reactor);
(d) The storage position of fuel assemblies in the spent fuel pool (e.g. all fuel assemblies are stored as one layer in the lower part of the pool or as two layers both in the lower and upper parts ~~fuel is also stored in the upper part~~ of the pool);
(e) The handling activities performed;
(f) The availability as well as the scheduled maintenance of credited ~~safety~~ systems;
(g) The time ~~available~~ for recovery actions and repairs to be credited;
(h) Differences in potential initiating events in different fuel storage configurations and the associated fuel manipulations, as necessary.

INITIATING EVENTS

10.9. Examples of the types of initiating event to be considered in the spent fuel pool PSA are as follows:

(a) Loss of cooling (loss of spent fuel pool heat removal system);
(b) Loss of coolant (pipe rupture in the spent fuel pool heat removal circuit);
(c) Loss of off-site power;
(d) Inadvertent draining (due to erroneous human intervention);
~~(d)~~(e) Reactivity accidents (boron dilution, fuel loading errors)
~~(e)~~(f) Initiating events induced by internal hazards that may lead to loss of the spent fuel pool heat removal system (including pipe ruptures as sources of internal flooding in systems

other than the heat removal circuit) or falling of objects onto the fuel assemblies in the spent fuel pool originated by lifting activities;

(g) ~~Internal~~ Initiating events induced by external hazards that may lead to loss of spent fuel pool heat removal, loss of spent fuel pool inventory or falling of objects onto the fuel assemblies in the spent fuel pool due to hazard induced structural failure;

~~(f)~~(h) Initiating events induced by combinations of hazards that may lead to the consequences described above (see item (f) and (g)).~~.~~

ACCIDENT SEQUENCE ANALYSIS

10.10. In the accident sequence analysis, the possibility of actions by operating personnel aimed at recovering spent fuel pool cooling as well as water supply into the spent fuel pool from alternative sources should be considered as mitigation actions at a minimum. Automatic actuations should also be considered, if applicable.

10.11. The specific characteristics of recovering the cooling system of the spent fuel pool, recovery from pipe ruptures and recovery from loss of off-site power should be taken into account in the assessment (e.g., repairment of the failed component). For assessing the time available to recovery, the initial water inventory in the spent fuel pool, the residual heat of the fuel assemblies stored in the spent fuel pool as well as the capacity of the systems available for mitigation should be considered.

10.12. Potential dependencies between Level 1 PSA for the reactor core and Level 1 PSA for the spent fuel pool should be considered, with respect to shared ~~mitigating system~~credited systems and human resources in the case of common initiating events. Consequential effects between SFP and reactor PSA should also be considered, for example flooding effects, structural loads due to external hazards or other phenomena, draining events when SFP and reactor are connected etc.

10.13. When modelling loss of spent fuel pool coolant accidents, flooding should be considered as a consequential hazard. Then, timely isolation for isolable piping can be credited to avoid flooding impact (e.g. the long lasting failure of the spent fuel pool heat removal system).

10.14. The accident sequence analysis should consider that boiling can cause pump cavitation which may prevent successful restart of the cooling system(s) and/or may disable local actions due to degraded ambient environmental conditions in the vicinity of the spent fuel pool.

10.15. For some spent fuel pool accident sequences, slow accident progression due to the large water inventory and low power level should be considered to define the sequence mission time, which can then be relatively long (see para. 9.51) and allows reliable recovery actions and repair activity. Termination of the analysis at a fixed pre-defined sequence mission time may prevent meaningful results from being obtained.

HUMAN RELIABILITY ANALYSIS

10.16. ~~*Owing to slow accident progression in the case of loss of spent fuel pool cooling events, recovery actions and repair activity should be credited.*~~*--- removed ---*

10.17. The slow accident progression in the case of loss of spent fuel pool cooling events makes possible the participation of multiple actors in the process of diagnosis, decision-making and as well as in the execution of recovery actions and repair activity. This should be considered when defining performance shaping factors that mostly affect the ~~success~~ failure probability of recovery actions[41] in these situations.

10.18. The emergency operating procedures may be developed to a different level of detail for spent fuel pool accidents than for reactor core accidents. Such a difference may influence the human reliability when responding to a spent fuel pool accident in comparison with the reactor core. This difference should be considered when carrying out human reliability analysis for the Level 1 spent fuel pool PSA.

10.19. Potential dependencies between human actions to prevent undesired ~~end point~~end states for the spent fuel pool as well as for the reactor core should be considered. In addition, the aggravating effects of the increased workload due to mitigating concurrent accidents simultaneously should be considered when assessing the relevant human error probabilities.

QUANTIFICATION OF THE ANALYSIS

10.20. All recommendations provided in para. 5.167-5.177 are applicable to spent fuel pool PSA. In addition, the PSA models for the reactor core and for fuel in the spent fuel pool should be integrated to correctly model dependencies of the shared systems. This is particularly important for the initiating events affecting both reactor core and spent fuel pool simultaneously and for further Level 2 PSA study (in particular for plants with the spent fuel pool inside the containment).

INTERPRETATION OF RESULTS

10.21. The combined or separate interpretation of risk from accidents involving the spent fuel pool and the reactor core should be consistent with the probabilistic ~~national~~ safety goals or criteria specified in national regulations or guidelines.

10.22. There is no international consensus on whether or not to aggregate the Level 1 PSA risk results of the spent fuel pool with those of the reactor[42]. ~~However, the risk results for the reactor and the spent fuel pool should be aggregated in the Level 2 PSA.~~

10.23. If both risk metric estimates are to be aggregated to generate an overall risk metric estimate that quantitatively describes the vulnerability of the plant to severe accidents, the correlations between the accident sequences of the spent fuel pool and the reactor should be considered, rather than simply summing these estimates (i.e. similar to aggregating multi-unit or site core damage frequencies, see Section 11).

[41] Recovery actions can be credited only in case of slow pace of the accident, sufficient time window and information available for operators to implement these actions.

[42] Risk results for the reactor and the spent fuel pool could be appropriately aggregated in the Level 2 and Level 3 PSA.

11. LEVEL 1 MULTI-UNIT PSA

11.1. Consideration of multi-unit interactions from a single unit Level 1 PSA perspective are presented in Sections 5-10 (e.g. paras 5.7, 5.20, 7.37, 7.73). The recommendations provided in this section are related to the development of a Level 1 Multi-unit PSA (MUPSA) which is aimed to quantify multi-unit risk metrics.

11.2. MUPSA model ~~should be~~is typically developed based on single unit PSA models, and take into account the specifics of each unit under consideration.

MUPSA SCOPE

11.3. As described in para. 2.2, the scope and the need for MUPSA should be correlated with the ~~national~~ probabilistic safety goals or criteria, if they ~~latter~~ have been specified in national regulations or guidelines ~~set~~.

11.4. The scope of MUPSA should include all risk-significant initiating events, hazards and plant operating states, which can be identified from the review of single unit PSA results. For the purpose of determining the scope of a MUPSA, a screening approach may be adopted based on reviewing single unit PSA results, if necessary[43].

MUPSA RISK METRICS

11.5. ~~If the national policy requires, then a~~Additional risk metrics other than the ones used in single unit PSA (e.g. core damage frequency) should be developed in order to express the risk profile in the context of multiple unit nuclear power plants for corresponding decision-making. For example, the following risk metrics for reactor unit can be used for Level 1 multi-unit PSA:

(a) Single unit core damage frequency: frequency per site-year of an accident involving core damage on one and only one reactor on a multi-unit site;
(b) Multiunit core damage frequency: frequency per site-year of an accident involving core damage on two or more reactors on a multi-unit site;
(c) Site core damage frequency: frequency per site-year of an accident involving core damage on one or more reactors;
(d) Multi-Source Fuel Damage Frequency: the frequency per site-year of an accident involving fuel damage from two or more sources (i.e. reactor core, spent fuel pool) on a multi-unit site

Risk metrics for multi-unit PSA should be defined so as to capture different combinations between the reactor cores and spent fuel pools on site and to facilitate the use of the results of the MUPSA for decision-making.

PLANT OPERATING STATES

[43] Depending of the scope of the PSA, for risk aggregation, multi-unit aspects as well as potential effects from other radioactive sources on the nuclear power reactor(s) and/or the spent fuel pool(s) collocated on the site (e.g. interim fuel storage facilities, nuclear waste treatment facilities) might be also considered within the PSA.

11.6. For a MUPSA, a representative set of combinations of plant operating states for each unit should be selected such that the most risk-significant combinations can be taken into account.

11.7. The selected combinations should consider different configurations of all reactors at power and in shutdown states, as well as spent fuel pool plant operating states. Some combinations may be eliminated due to plant operating practices, for example ensuring that two units are not refuelled at the same time. Simplifications to the combinations of plant operating states should be justified in terms of risk significance.

11.8. As recommended in paras 9.8 and 10.7, grouping of plant operating states could be necessary. This grouping should be done so as not to mask the potential for risk significant initiating events from multi-unit risk perspectives.

11.9. For a MUPSA, the probability or fraction of time that is spent in each modelled combination of plant operating state for each reactor unit should be estimated.

INITIATING EVENTS ANALYSIS

11.10. Screening of multi-unit initiating events[44] in a MUPSA should be implemented, taking into account their risk-significance. Multi-unit initiating events could be screened out if a detailed realistic analysis would not make a significant contribution to the selected MUPSA risk metrics.

11.11. The grouping of single unit initiating events should be checked and revised, if necessary, considering that the grouped initiating events could potentially have a different impact on a multiple unit plant.

11.12. For a MUPSA, hazard event frequencies that are dependent on the combination of plant operating states should be calculated, taking into account the probability of the combination. For single unit PSAs, frequencies are estimated on a reactor calendar year basis, whereas for MUPSAs, frequencies are estimated on a site calendar year basis.

SYSTEM ANALYSIS

11.13. SSCs and resources that are shared among the units should be explicitly modelled in MUPSA.

11.14. The availability of a shared SSCs or resources to each unit during accidents involving multiple units should be taken into account.

11.15. The priorities of usage of shared SSCs and resources for different units should be considered and modelled as realistically as possible.

11.16. Functional and spatial dependencies between SSCs of different units on site should be considered in MUPSA system analysis.

HUMAN RELIABILITY ANALYSIS

[44] A multi-unit initiating event is an initiating event that immediately results in a trip or challenge to normal operation (or a degraded condition that eventually leads to a trip or challenge to normal operation) of two or more units.

11.17. For multi-unit initiating events and/or accident sequences, human actions associated with the need to manage multiple reactor units should be considered.

11.18. Human reliability analysis methods used in MUPSA should take into consideration the contextual characteristics of multiple units such as increased stress due to site level accident conditions, shared human resources, working in the shared control rooms (when applicable), and the interaction of units with a common technical support centre.

11.19. The potential for dependencies between actions by operating personnel in different units should be considered. The level of dependencies should be evaluated taking into account influencing factors, such as shared resources, interaction with a common technical support centre or another organization coordinating the activities on site, and the impact of internal hazards and external hazards.

11.20. In the case of an accident on one or more units on site simultaneously, the adverse effects on the control and accident management on the other units should be considered, taking into account the factors connected with severe accidents at other units at the site (e.g. radiological release, hydrogen detonation).

COMMON CAUSE FAILURE AND HAZARD FRAGILITY CORRELATIONS

11.21. Inter-unit common cause failure for relevant SSCs should be identified and modelled.

11.22. Inter-unit hazards fragility correlations should be identified and modelled.

QUANTIFICATION OF A MUPSA RISK PROFILE

11.23. The quantification of the MUPSA risk profile should take into account all undesired ~~end point~~end state combinations of the units on site. In order to address all effects and interdependencies of multiple collocated units and/or spent fuel pools it is practical to use the integral PSA model for the site which includes all considered initiating events, accident sequences and mitigating system functions.

11.24. Minimal cutsets should be reviewed to ensure that the model correctly ~~accounted~~ accounts for aspects of multiple unit plants, such as shared SSCs, simultaneous accident conditions, and damage to multiple units.

11.25. The results obtained from the MUPSA should be used as an input for risk-informed decision making.

12. USE AND APPLICATIONS OF PSA

GENERAL ASPECTS OF PSA APPLICATIONS

12.1. This section discusses a number of PSA applications practiced in individual States based on national safety policies and regulations, and provides recommendations on meeting the following requirements:

— Requirement 23 of GSR Part 4 [3] on the general use of ~~Level 1~~ PSA;

— Requirements 6, 10, 16, 42 of SSR-2/1 (Rev. 1) [2] on the use of ~~Level 1~~ PSA in the design of nuclear power plants;

— Requirement 22 of SSR-2/1 (Rev. 1) [2] on the use of ~~Level 1~~ PSA for safety classification;

— Requirement 31 of IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [34] on the use of PSA for test and maintenance optimization;

— Requirement 12 of SSR-2/2 (Rev. 1) [34] on the use of Level-1 PSA for periodic safety review;

— Requirement 8 of SSR-2/2 (Rev. 1) [34] on the quality of Level-1 PSA used to support safety related activities.

12.2. The PSA should be used throughout the design and operation of the plant to assist in the decision making process on the safety of the plant to prioritize and to optimize the design and safety related activities so that they focus on areas that have the highest risk significance.

12.3. The results of the PSA should be used to provide insights into the design and operation of SSCs important to safety in preventing fuel damage either in the reactor core or in the spent fuel pool. Such use of the PSA results should include a comparison with the overall probabilistic safety goal or criteria where these have been specified.

12.4. The PSA to be used for any application should be maintained as a 'living PSA' that is regularly updated to reflect the current design and operation of the plant and current analysis of its transients and has been fully documented so that the analysis can be traced back to details of the design and supporting analysis[45]. ~~The quality attributes of Level 1 PSA models essential for particular PSA applications are provided in IAEA-TECDOC-1804 [35].~~

12.5. The PSA should be updated throughout the lifetime of the plant, with the scope, level of detail and accuracy of the PSA increasing as the design develops, as more analysis is carried out to support the modelling assumptions in the PSA and as data become available from plant operating experience. The results of the PSA should be used to identify weaknesses in the design and operation and to assess and rank options for improving the design or operation.

12.6. In deriving risk insights from the PSA, care should be taken to understand the relative significance of the contributions from the various types of accident initiator (internal initiating events, internal fires, internal floods, earthquakes) and plant operating states to the PSA results. In particular, it should be recognized that aggregation of various risk contributors (various hazards, various plant operating states, various facilities) implies a certain level of heterogeneity in terms of the level of details, resolution, inherent conservatism and uncertainties for individual contributors. The heterogeneity might lead to misleading insights from PSA and therefore should be taken into consideration during the decision-making.[46] This is of particular importance for applications of PSA that rely on the evaluation of importance

[45] The quality attributes of Level 1 PSA models essential for particular PSA applications are provided in IAEA-TECDOC-1804 [35].

[46] For example, when analysing the risk from fire, it is common to use a successive bounding and screening approach so that the level of detail for the analysis of a particular fire area is a function of whether its contribution to core or fuel damage frequency is judged to be low enough in accordance with the screening criterion adopted. This is done to optimize the resources spent on detailed fire modelling or cable tracing. External flooding is another example where uncertainties associated with hazard may be significantly larger than those associated with internal events.

measures and for risk monitor type applications.

12.7. PSA applications for operating plants should include adequate communication of the techniques, applications and implications of PSA to plant management to develop an integral understanding in terms of management responsibilities.

12.8. The PSA results and a detailed qualitative summary of the results and associated risk insights and risk importance of all modelled SSCs and events are needed in these applications to add risk informed insights to the safety culture. In addition, the plant management's active participation in all risk informed application would build an awareness of how to manage the risks.

12.9. How well the PSA model reflects the as-built and as-operated plant necessary for the management to have confidence in the PSA results, is one of the most important attributes for many PSA applications [35, 36]. In accordance with Requirement 8 of SSR-2/2 (Rev. 1) [34], PSA to be used for decision making purposes is required to be of appropriate quality and scope ~~adequate~~ for particular decision making purposes. The risk analysis should be performed by appropriately skilled analysts and should be used in a manner that complements the deterministic approach to decision making, in compliance with applicable regulations and plant licence conditions. This should be accompanied by a basic understanding of ~~Level 1~~ PSA concepts and methods so that the results can be interpreted properly.

SCOPE OF PSA FOR APPLICATIONS

12.10. GSR Part 4 [3] requires that the safety assessment includes a full scope PSA for evaluating and assessing challenges to safety in normal operation, anticipated operational occurrences and accident conditions. The completeness of the PSA (which includes a comprehensive set of internal initiating events, internal hazards and natural and human induced external hazards and addresses all plant operating states including startup, operation at power, low power, shutdown and refuelling) will ensure that the insights from the PSA relating to the risk significance of accident sequences, SSCs, human errors and common cause failures, are derived from a comprehensive, integrated model of the plant. However, for some PSA applications, it is expected that insights from a plant specific or a generic Level 2 or even a Level 3 PSA may be necessary.

12.11. In many cases, the scope of the PSA that is necessary to support a specific application may vary from the full scope described above. In any case, when the risk insights are to be derived from a PSA that has a smaller scope than the full scope described in this Safety Guide (e.g. not all initiating events and hazards considered) this should be recognized in applying the insights from the PSA[47].

12.12. If a PSA is intended for use as a representative PSA for more than one similar unit at a site, the impact of any differences between a specific unit and the representative model should be identified and the impact on the results of the PSA should be assessed.

12.13. For multiple unit nuclear power plants, the national safety policy or regulations may require the risk associated with multiple units to be used in risk-informed decision making. In such cases, either insights from a MUPSA should be used (if available) or the insights from PSA study which appropriately considers multi-unit interactions from single unit perspectives

[47] For example, if the Level 1 PSA does not contain a fire PSA, it is not feasible to use PSA insights in relation to cable routing.

(e.g. consideration of initiating events simultaneously affecting more than one unit, shared systems among the units, impact on human performance and resources, evaluation of inter-unit dependencies, consideration of cascading or concurrent releases).

RISK INFORMED APPROACH

12.14. In any of the PSA applications described in this Section, the insights from PSA should be used as part of the process of risk informed decision making that takes account of the following [9, 37]:

(a) Any mandatory requirements that relate to the PSA application being addressed (which would typically include any legal requirements or regulations that need to be complied with);
(b) The insights from deterministic safety analysis (such as whether the provision of the defence in depth requirement is met, whether there are adequate safety margins and whether lower level requirements such as the provision of sufficient levels of redundancy and diversity in the ~~safety systems~~SSCs that perform safety functions are met and that the equipment in the plant has been qualified to a sufficient level so that it can withstand the harsh environments that would follow initiating events);
(c) Any other applicable insights or information (which could include a cost–benefit analysis and details on the remaining lifetime of the plant, inspection findings, operating experience, doses to workers from making changes to the plant).

12.15. When applying PSA in a risk informed approach it should be ensured that a balanced approach is taken for any decisions that are made and all the relevant factors are taken into account. The PSA applications addressed in the remainder of this section do not cover all possible PSA applications, but the most commonly used in individual States.[48]

USE OF PSA FOR DESIGN EVALUATION

12.16. The PSA should be used to provide one of the inputs into the evaluation of the design throughout the lifetime of the plant, as follows:

(a) The PSA should be used at the concept stage to provide insights into whether the proposed design of the ~~mitigating system~~credited systems and the layout of the plant are adequate;
(b) The PSA should be used at the concept stage to determine the spectrum of initiating events that need to be considered as the design basis and the licensing basis of the plant.
(c) The PSA should be updated throughout the detailed design and construction stages to take account of new information relating to design, safety analysis and siting as it becomes available;
(d) The PSA should be maintained as a living PSA for the plant in operation and used as one of the inputs for resolving issues relating to operations, periodic safety reviews and extension of the lifetime of the plant, and to provide insights into whether proposed

[48] Examples of publications providing additional information on application of PSA are IAEA-TECDOC-1804 "Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants" [35] and IAEA-TECDOC-1200 on "Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants" [36].

design modifications and operating changes are adequate.

(e) Used at the decommissioning phase of the plant to ensure that risks associated with the decommissioning process and remaining radioactive materials stored at the site are negligible (see paragraph 4.28 of IAEA Safety Standards Series No. WS-G-5.2 [38])

Use of PSA to support decisions made during the design of a nuclear power plant

12.17. To obtain maximum benefit, the PSA used for design evaluation should be a full scope PSA as specified in para. 12.11. This will ensure that a wide range of issues for the design and operation of the plant can be addressed using the PSA. The scope of the PSA relates mainly to the range of initiating events and internal hazards and external hazards included in the PSA and the range of plant operating states addressed in the PSA.

12.18. In accordance with para. 5.76 of SSR-2/1 (Rev. 1) [2], a PSA of the design is required to be used for establishing the balanced design, preventing cliff edge effects and comparing the risk level with acceptance criteria or safety goal.

12.19. Insights from ~~Level 1~~ PSA allows the optimization of the design of a new plant in terms of risk metrics and cost. The results of the ~~Level 1~~ PSA should be used to provide an approach for determining the following:

(a) Whether the ~~mitigating system~~credited systems have adequate levels of diversity and redundancy;
(b) Whether there are sufficient levels of equipment qualification for SSCs that experience harsh conditions in accident conditions;
(c) Whether there is sufficient separation and segregation of areas for hazards such as fire and flooding;
(d) Whether the design of the human–machine interface is adequate to ensure that the potential for human error has been reduced to a sufficiently low level.

12.20. The results of the ~~Level 1~~ PSA should also be used to determine the needs for additional measures ~~need~~ to be incorporated to reduce risk.

12.21. The PSA should include an investigation of variants and exploratory design options, the sufficiency of the redundancy and diversity of systems, and the effectiveness of emergency response and accident management measures. PSA results should be used to allocate reliability and availability targets for SSCs to meet probabilistic safety goals or criteria, thereby forming part of the design specification. PSA should be also used as a supporting tool to select or modify the design basis accidents and design extension conditions (DEC), to define general design criteria~~,~~. PSA may also be used to ~~and~~ provide an input to cost-benefit analysis.

12.22. When applying PSA for the design of a nuclear power plant, particular effort should be made to correctly reflect new design features that might not be known in previous PSAs (e.g. unique initiating events, failure modes, common cause failures, specific event sequences and dependencies)

12.23. In a ~~Level 1~~ PSA conducted at an early design stage, the reasons for additional assumptions that are needed due to a lack of design and operating details should be documented, and at a later stages of the design (e.g. construction or pre-operational stages) these assumptions should be checked for their validity.

12.24. The uncertainties in input information, data used and resulting risk estimates should be assessed using uncertainty analyses and sensitivity studies. It should be proven that risk insights used for design optimization and safety assessment are not dependent on major assumptions and key uncertainties.

12.25. The list of minimal cutsets from the Level 1 PSA model should be used to identify where there are relative weaknesses in the design and operation of the plant. This review should be carried out for the minimal cutsets that make significant contributions to core or fuel damage frequency to identify the initiating event groups, component failures and human failures events that make the greatest contributions to the core damage frequency or fuel damage frequency. This should also be done for minimal cutsets containing basic events whose importance values are high.

12.26. The contributions to the core damage frequency or fuel damage frequency from individual groups of initiating events and contribution of minimal cutsets to core damage frequency or fuel damage frequency for individual groups should be used to determine whether the design of the plant is balanced in that no particular group of initiating events and no particular accident sequence within the group makes an unduly large contribution to the core or fuel damage frequency[49].

12.27. The PSA should be used to verify the single failure criterion for the given design. This could be done using the list of minimal cutsets to determine whether there are any minimal cutsets that contain only an initiating event and a single failure event or single human failure event (not counting for configurational basic events used to control the proper systems configurations in particular plant operating mode) that may indicate that the single failure requirement is not satisfied for the design.

12.28. The list of dominant minimal cutsets should be reviewed to determine whether there are opportunities to enhance defence in depth if any deficiencies are identified.

12.29. Importance measures for basic events, groups of basic events, ~~mitigating system~~credited systems and initiating event groups, should be calculated and used to interpret the results of the PSA[50]. A high Fussell–Vesely importance value or Birnbaum importance value for an independent failure event may indicate insufficient redundancy of the system in some plant operating states or low reliability and hence a need for improvement. A high risk achievement worth for an independent failure event may indicate that the level of reliability of the equipment should be carefully maintained to avoid an increase in risk. A high Fussell–Vesely importance value for a common cause failure may indicate insufficient diversity of ~~mitigating system~~credited systems in respect of a particular safety function. In this case, a considerable change in the design basis might be required. Several importance measures should be used in complementary manner to support decisions during plant design.

12.30. For multiple unit sites and/or sources collocated at a site the impact of one of these to ~~unit~~ NPP units being investigated ~~on the other units~~ should be considered in risk-informed design optimization process to support reduction of the risk significance of such impact.

[49] International practice shows that it could be difficult to achieve this objective for external hazards, especially for new designs, where the CDF values could be relatively low for internal initiating events.

[50] For explanation of the various importance measures, see para. 5.178

Use of PSA in the licensing process

12.31. The assessment of the overall plant safety is necessary for applying for an operational licence and usually involves a full scope Level 1. A comparison of the results against probabilistic safety goals or criteria (if set) should be performed within this application. A safety evaluation for applying for a pre-construction licence may involve a limited scope of the PSA (e.g. using the data from the similar plants); however, at the stage of applying for an operational licence, a full scope level 1 PSA should be available[51].

12.32. The overall results of the Level 1 PSA (usually the core damage frequency or fuel damage frequency) should be compared with probabilistic safety goals or criteria (where these have been defined) to determine whether the proposed design and operation of the plant will ensure a sufficiently low level of risk. The aim should be to determine whether goals and criteria have been met and to provide a broad indication of sufficient level of safety has been achieved for the plant, that is, whether sufficient ~~mitigating system~~credited systems have been incorporated in the plant design and adequate emergency, operating, maintenance and testing procedures are available for operation to prevent core or fuel damage.

12.33. Comparison of the results of the Level 1 PSA with probabilistic safety goal or criteria should be made starting from the concept design and at various points of the design stage, construction stage and operations stage to identify and suggest the best results for safety, technical and organizational decisions and to check that the design is adequate.

12.34. In making the comparison described in para. 12.33, account should be taken of the results of the sensitivity studies and the uncertainty analysis that have been carried out. This will indicate the degree of confidence in meeting the criterion and/or goals and the likelihood that they have been met.

12.35. This application should include providing information in the pre-licensing process aimed at obtaining public acceptance for the construction and operation of the nuclear power plant.

Comparison of design options

12.36. When modifications are being considered for a nuclear power plant, there are usually a number of options available. The ~~Level 1~~ PSA should be used to provide an input into the comparison of options. The way that this is done depends on the complexity of the modification being considered, but could range from carrying out a revision of the ~~Level 1~~ PSA model to incorporate a proposed new ~~mitigating system~~credited system, to carrying out post-processing of the minimal cutsets to take account of simpler changes. The ~~Level 1~~ PSA should provide one of the inputs for an integrated risk informed decision making process to determine which of the options to choose [9, 37].

12.37. For operating plants, the use of assumptions and simplifications should be limited, in comparison to the PSA for newly designed plants, as the use of plant specific information

[51] States have different requirements for the scope of PSA applicable for licensing in terms of hazards and IEs consideration and location of the fuel (reactor and spent fuel pool, fresh fuel and irradiated fuel storage).

should be always preferable.

Use of PSA in periodic safety review

12.38. In accordance with Requirement 12 of SSR-2/2 (Rev. 1) [34] probabilistic safety assessment is required to be used as an input to the periodic safety review to provide insight into the contributions to safety of different safety related aspects of the plant.

12.39. A safety assessment process for this application should consists identifying ~~of identification of~~ safety issues, determination of their safety significance and making decisions on the need for corrective measures.

12.40. A PSA included in a periodic safety review should be used to create an up to date overview of the whole plant and to help in identification of cost-effective improvements to safety [52]. Consequently, the PSA should use plant specific data, model as-built-as-operated plant conditions, and address the possible impact of aging phenomena and component lifetime considerations on the overall risk metrics. Sensitivity calculations could be performed to assess the potential effect of ageing on passive components, which are not normally maintained or replaced[53].

12.41. ~~As a part of periodic safety review, PSA could be used to support the extension of the lifetime of the plant, to support a cost benefit evaluation of possible backfits to reduce the risk of severe accidents and to evaluate the risk importance of safety-related issues (e.g. deviations from the regulations).~~--- removed ---

Optimization of protection against internal hazards and external hazards

12.42. The ~~Level 1~~ PSA for internal hazards and external hazards PSA should be performed from the start of the design development to allow for an early optimization of the design in relation to initiating events induced by internal hazards and external hazards.

12.43. The ~~Level 1~~ PSA supporting optimization of the design against internal and hazards external hazards should be used to provide input for the following:

(a) Robustness of the SSCs against internal hazards and external hazards, including containment (based on the results of ~~seismic PSA, tsunami PSA, tornado and aircraft crash~~ internal and external hazards PSAs);

(b) Establishing criteria for equipment separation, cable tracing, plant layout (e.g. based on the results of fire and flood PSA);

---

[52] As a part of periodic safety review, PSA could be used to support the extension of the lifetime of the plant, to support a cost benefit evaluation of possible backfits to reduce the risk of severe accidents and to evaluate the risk importance of safety-related issues (e.g. deviations from the regulations).

[53] Currently, modelling of SSC aging in terms of PSA is in an exploratory stage and aging effects are typically addressed qualitatively.

(c) Understanding hazard occurrence factors (e.g. critical locations of high energy lines, critical fire sources) and designing the hazards protective features (e.g. fire detection, fire mitigation, location of flood or fire rated barriers, external flood protective measures);

(d) Establishing criteria for drainage system, flood detection and isolation, and fire isolation of the compartments;

(e) Identifying and reducing maintenance activities that can lead to fire or floods events.

12.44. PSA results and insights are dependent on the design features and provisions, including human interactions and associated procedures, that are credited in the PSA. The actual implementation of features and provisions to achieve acceptably low risk estimates at the pre-construction stage should be verified in the PSA performed when applying for an operations licence. If any discrepancies leading to higher risk are identified they should be reflected in the ~~Level 1~~ PSA and proposals for changes to reduce the risk should be made.

12.45. Uncertainties related to the aspects important for the internal hazards and external hazards PSA at the design stage (e.g. detailed cable tracing, fire and flood barriers, anchorage of the SSCs, location and orientation of the components) should be taken into account.

USE OF PSA FOR INSPECTIONS, TESTS AND MAINTENANCE OPTIMIZATION

12.46. ~~Requirement 31 of~~ SSR-2/2 (Rev. 1) [34] states:

~~"A probabilistic safety analysis should be used to ensure that effective programmes for maintenance, testing, surveillance and inspection are established and implemented".~~

~~Furthermore SSR-2/2 (Rev. 1) [34] states:~~

"8.5. The frequency of maintenance, testing, surveillance and inspection of individual structures, systems and components shall be determined on the basis of:

(a) The importance to safety of the structures, systems and components, with insights from probabilistic safety assessment taken into account;
(b) Their reliability in, and availability for, operation;
(c) Their assessed potential for degradation in operation and their ageing characteristics;
(d) Operating experience;
(e) Recommendations of vendors." ~~(para. 8.5 of SSR-2/2 (Rev. 1) [34].)~~

"8.6. A comprehensive and structured approach to identifying failure scenarios shall be taken to ensure the proper management of maintenance activities, using methods of probabilistic safety analysis as appropriate". ~~(para. 8.6 of SSR-2/2 (Rev. 1) [34].)~~

"8.13. The operating organization shall ensure that maintenance work during power operation is carried out with adequate defence in depth. Probabilistic safety assessment shall be used, as appropriate, to demonstrate that the risks are not significantly increased." ~~(para. 8.13 of SSR-2/2 (Rev. 1) [34].)~~

Risk informed technical specifications

12.47. PSA should be used to provide a consistent basis to risk-inform technical

specifications, which specify the limits and conditions for plant operation and maintenance, related to the risk significance of the affected plant features [54].

12.48. Insights from PSA should be used as an input to the process of establishing or ~~verification~~ verifying of measures to be implemented if an abnormal event that does not lead to immediate reactor scram occurs. This includes the following:

(a) At the design stage, the Level-1 PSA allows the quantification of the risk associated with different allowed times, measures and actions in response to the same abnormal event. The comparison of such risks should be performed and the most risk beneficial option should be proposed for inclusion in technical specifications. When quantifying such risks, both risks for continued operation during allowed time and risks after the measure has been implemented should be taken into account.

(b) For the operating plant where technical specifications and operational limits and conditions are already available, the Level-1 PSA should be used to justify their appropriateness and to suggest measures and revisions of allowed outage times where justification is not sufficient.

In both cases, a full scope Level-1 PSA should be used and modified as appropriate to consider all aspects associated with a particular abnormal event or plant configuration. If Level-1 PSA is of limited scope, it could be used only when the impact of the abnormal event or plant configuration on the risk associated with missing parts of the PSA is proved to be negligible.

12.49. Where it is proposed to move a particular maintenance activity from power operation to shutdown state (or vice versa), the PSA should be used to assess the risk associated with the revised plant configurations.

12.50. The insights provided by the ~~Level 1~~ PSA should include the information necessary for comparison with the decision criteria or guidelines used to support the risk informing of the technical specifications. Such information may include, for example, the conditional core damage frequency or fuel damage frequency when the plant item is undergoing maintenance; the incremental conditional core damage probability; the cumulative, incremental, conditional core damage probability over the year and the impact of a change on the average yearly core or fuel damage frequency.

Determination and evaluation of surveillance test intervals

12.51. The surveillance test intervals give the testing requirements for SSCs important to safety and specify the frequency of testing and sometimes the testing strategy that should be followed. PSA based evaluation of surveillance test intervals considers the risk from unavailability due to undetected failures, and the risk from unavailability due to tests and test

[54] The technical specifications specify, for example, the measures to be implemented if an abnormal event that does not lead to an immediate reactor scram occurs, the allowed outage times before implementation of these measures and additional actions necessary (e.g. the additional testing requirements for redundant equipment, reduction of power level, disconnection of affected equipment, immediate repair of failed component). If the allowed outage time is exceeded, the technical specifications specify the further actions that operating personnel should take. Also limiting conditions for operation specify the requirements for equipment operability usually limiting the combinations of equipment that can be removed for maintenance at the same time (usually referred to as configuration control). Currently the requirements of the technical specifications are traditionally based on deterministic requirements and engineering judgement.

induced failures.

12.52. The goal of this applications is to optimize the surveillance test intervals with respect to their impact on equipment reliability and how these tests impact the cost of operations. Human errors during service test intervals that might have an adverse impact on safety, for example by leading to plant trips and initiating events, are normally considered in optimizing the test intervals.

12.53. At the design stage, all SSCs that are included in the Level 1 PSA model should be considered to quantify the risk associated with different service test interval strategies and to select the strategies that will ensure the following:

(a) The overall probabilistic safety goals or criteria for the design are achieved;

(b) The components that have high importance for safety have more stringent testing requirements;

(c) The probability of HFEs during and after testing that can lead to unavailability of equipment or cause initiating events are reduced;

(d) The service testing intervals do not lead to exercise wearing of the tested components.

12.54. For the operating plant, where service testing interval strategies are already available, the Level 1 PSA should be used to justify their appropriateness and to suggest changes in service testing intervals for the components that have the highest risk contribution and high risk importance values.

12.55. When quantifying such risks, the uncertainty in both mathematical models for tested components and data should be taken into account.

12.56. In providing input from the Level 1 PSA for the optimization or justification of the service testing interval strategies the following should be investigated and taken into account:

(a) The correlation between the surveillance test interval and the component failure probability (e.g. wearing due to frequent tests);

(b) Common cause failures with due account taken of the type of testing (staggered or non-staggered);

(c) The potential for HFEs during and after testing, leading to component(s) unavailability and/or an initiating event;

(d) The potential for errors of commission that may be introduced due testing strategies.

12.57. For both new and operating nuclear power plants, a full scope Level 1 PSA should be used to consider impact of different service testing interval strategies. If the Level 1 PSA is of limited scope, it should be only used if it is demonstrated that changes in the service testing interval strategy have a negligible impact on the risks associated with missing parts of the PSA.

12.58. The PSA model should explicitly model the unavailability of SSCs due to testing and provide a capability to predict the impact of changes to a service testing interval for each affected SSC.

12.59. Risk importance measures should be used to prioritize and rank the candidates for a change of service testing interval. The change in risk metrics should be used to evaluate the risk significance and acceptability of the proposed change and the incremental risk metrics should be used to evaluate the acceptability of the new proposed service testing interval.

12.60. An understanding of how human errors during testing contribute to initiating event frequencies and component failures is needed to balance the positive and negative aspects of surveillance testing. Unavailability of equipment due to human errors to properly restore normal alignments after testing should be taken into account. If it is known that a test may lead to a higher probability of an initiating event (initiating event frequency is related to test frequency) then this relationship should be taken into account if the test frequency is changed.

Risk informed in-service testing

12.61. The current approach to in-service testing requires that it is performed by following a code or standard, which may or may not be incorporated into a prescribed regulation that uses a deterministic approach to decide on the programme of in-service testing that needs to be carried out for SSCs in the plant.

12.62. The aim of the application of a risk informed approach to in-service testing is to use the risk information provided by the PSA to help optimize the in-service testing programme so that it focuses on the components that have the highest risk significance. From the point of view of the operating personnel, a risk informed approach to in-service testing can prioritize the components that have various risk significance and has the potential to ~~reduce overall maintenance costs,~~ prevent undue adverse effects of testing on components, and increase availability of components while still maintaining a very high level of safety.

12.63. In applying a risk informed approach to in-service testing, the results of the PSA should be used along with deterministic and engineering considerations to determine the risk significance of the components to be addressed.

12.64. The risk information from the PSA should be derived using both the Fussell–Vesely importance and the Birnbaum importance (or the risk achievement worth), since both these importance measures provide insights into the risk significance of components and should include common cause failure considerations.

12.65. If a MUPSA model is available, it should be used to support risk-informed testing of components associated with shared systems. The use of a MUPSA model may provide additional insights on the risk significance of shared systems and components in terms of risk metrics for multiple unit nuclear power plants.

12.66. The risk information should be used to identify components with a relatively high safety significance for which rigorous in-service testing is needed, and components with a relatively low safety significance that are candidates for less rigorous testing. The in-service testing programme can then be amended, taking into account the safety significance of components.

12.67. When the in-service test intervals have been revised, the Level 1 PSA should be used to calculate the core damage frequency or fuel damage frequency for the new test intervals in order to determine whether the changes are acceptable

Risk informed pre- and in-service inspection

12.68. The overall aim of the programme for in-service inspection of the pipework at a nuclear power plant is to identify areas of degradation that can be repaired before a failure occurs. The programme of inspections that is carried out has typically been based on a traditional deterministic approach and engineering judgement. The risk informed pre- and in-service inspection approach implied that the risk significance of the piping segment is determined through a combination (for instance in a form of a risk matrix) of the assessment of the degradation potential (qualitative or quantitative) and the assessment of the potential consequences of the piping segment failure (e.g. CCDP).

12.69. The risk informed approach should be used to provide the insights from the PSA to revise the programme of inspections (in terms of the frequency of inspection, methods used and sample size) and focus it on those segments of pipework that have the highest risk significance and reduce the inspections carried out on segments of pipework with a low risk significance. The expectation is that this will lead to a reduction in the overall number of pipework inspections that are carried out ~~, a reduction in costs~~ and a reduction in the associated occupational exposure, without increasing the risk from the plant.[55]

12.70. At the design stage, the application is used to develop the inspection programme to prevent failures of the risk significant pipework. For operating plants this programme should be maintained and updated based on feedback from operating experience.

12.71. Insights from the ~~Level 1~~ PSA should be used as one of the inputs in determining the following:

(a) The pipework segments to be assessed by the risk informed in-service inspection project;
(b) The risk significance of the segments of pipework to be assessed;
(c) The target failure probabilities for the pipework segments that are to be inspected;
(d) The change in the risk resulting from changes to the in-service inspection programme.

12.72. For each pipework segment included in the study, the consequences of failure of the segment should be determined in one of the following ways:

(a) As an initiating event, with account taken of any secondary failure(s) that could occur (e.g. as a result of a release of water or steam, pipe whip);
(b) As a failure in a standby system that could lead to a train of the system (or the whole system) being unavailable to perform its safety function;
(c) As a failure of a train of a system (or the whole system) when it operates on demand due to the loads imposed on the pipework segment.

12.73. Pipework failures that lead directly to initiating events would normally already be included in a full scope ~~Level 1~~ PSA. It should be checked that this is the case and conditional fuel damage probability should be assessed for all initiating events induced by pipework failure. The ranking of these probabilities should be used for identification of the most risk

[55] Several approaches to carrying out risk informed in-service inspection have been developed [39~~7~~]. Examples include methods recommended by Electric Power Research Institute, Westinghouse Owners Group and European Network for Inspection and Qualification.

significant pipework.

12.74. For pipework failures leading to the unavailability of ~~mitigating system~~credited systems or failure of ~~mitigating system~~credited systems ~~on demand~~ on demand, the PSA should be used to calculate the conditional core damage frequency or fuel damage frequency. Such failures are not always included in the PSA model[56], so the model should be revised correspondingly for this PSA application. An approach that is often adopted is to use a surrogate approach where the failures of the segments of pipework not included explicitly in the PSA are correlated with basic events (or groups of basic events) already included in the PSA and for which the consequences of failure are the same. In doing this, consideration should be given to ensuring that any secondary effects of pipework failure are taken into account in the PSA model.

12.75. The more rigorous way of determining the risk significance of all segments of pipework included in the risk informed in-service inspection project would be to revise the PSA model to include these pipework segments explicitly and thereby determine the associated conditional core damage frequency or fuel damage frequency directly. This approach has been used in some of the risk informed in-service inspection projects that have been carried out in various Member States [39].

12.76. When the revised in-service inspection programme has been determined, the PSA should be used to determine the risk insights necessary for comparison with the decision criteria or guidelines used to assess the acceptability of the change in the in-service inspection programme. This should be done by estimating the specific changes in initiating event frequencies or component failure probabilities that would result from a change in the in-service inspection programme and by requantifying the PSA with these revised values, or by carrying out sensitivity studies. In this process, the associated limitations on the PSA in terms of modelling details and scope should be recognized and taken into account.

12.77. If a MUPSA model is available, it should be used to support risk-informed inspection for piping associated with shared systems. The impact of failures in the piping of shared system should be under additional consideration to determine how their inspection strategies should be adjusted using a risk-informed approach.

RISK-INFORMED CLASSIFICATION OF SSCs

12.78. The following set of recommendations is established to support the application of Requirement 22 of SSR-2/1 (Rev. 1) [2], which requires that all items important to safety are identified and classified on the basis of their function and their safety significance. Paragraph 5.34 of SSR-2/1 (Rev. 1) [2] states:

> "The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:
>
> (a) The safety function(s) to be performed by the item;

[56] Sometimes such failures are screened out if the contribution to the failure probability of ~~mitigating system~~credited systems from a failure of the pipework is negligible in comparison to that from failure of active components.

(b) The consequences of failure to perform a safety function;

(c) The frequency with which the item will be called upon to perform a safety function;

(d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function."

In addition, IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [40] provides the following recommendations on the use of PSA for safety classification:

— "Safety classification is an iterative process that should be carried out periodically throughout the design process and maintained throughout the lifetime of the plant. Any assignment of SSCs to particular safety classes should be justified using deterministic safety analysis complemented by insights from probabilistic safety assessment and supported by engineering judgement". (Para. 2.3 of SSG-30 [40].)

— "The next step in the process is to determine the safety classification of all SSCs important to safety. Deterministic methodologies should generally be applied, complemented where appropriate by probabilistic safety assessment and engineering judgement to achieve an appropriate risk profile, i.e. a plant design for which events with a high level of severity of consequences have a very low predicted frequency of occurrence…." (Para. 2.14 of SSG-30 [40].)

— "The adequacy of the safety classification should be verified by using deterministic safety analysis, which should be complemented by insights from probabilistic safety assessment and/or supported by engineering judgement." (Para. 3.27 of SSG-30 [40].)

— "The contribution of the SSC to reduction in the overall plant risk is an important factor in the assignment of its safety class. Consistency between the deterministic and probabilistic approaches will provide confidence that the safety classification is correct. ~~Generally, it is expected that probabilistic criteria for safety classification will match those derived deterministically. If there are differences, however, further assessment should be carried out in order to understand the reasons for these and a final safety class should be assigned, which should be supported by an appropriate justification".~~ (Para. 3.28 of SSG-30 [40].)

12.79. The aim of the application of a risk-informed classification is to provide one of the inputs to the process of assigning safety classes to SSCs in accordance with their risk significance.[57] ~~Level 1~~ PSA should be used to consider whether changes can be made to the traditional prescriptive regulatory requirements for some of the SSCs to bring the requirements more in line with the safety significance of the SSCs. From the point of view of operating personnel, this reduces the resources necessary to carry out the surveillance programme, and from the point of view of the regulatory body, it will remove unnecessary burdens from the operating personnel, without increasing the risk from the plant.

12.80. The Level 1 PSA should be used to determine the risk significance of SSCs used

[57] The historical approach for safety classification is to apply the same high level of quality assurance to all SSCs important to safety. However, the results of many PSAs carried out to date have shown that some of the SSCs that have been classified as important to safety have a relatively low safety significance and some of the SSCs classified as not being important to safety have a relatively high safety significance.

to prevent core or fuel damage. The risk significance should be derived using both the Fussell–Vesely importance and the Birnbaum importance (or the risk achievement worth) since both these importance measures provide insights into the risk significance of SSCs. Conditional core or fuel damage frequency assuming failure of SSCs should be also used as a measure of risk significance.

12.81. Risk significance should be used as one of the inputs to a risk informed decision making process together with other important information such as defence in depth when classifying a system as low/high safety significance.

12.82. Consideration should be given on whether the requirements could be reduced for SSCs that have been classified as important to safety but which have a relatively low safety significance and whether they should be increased for the SSCs that have been classified as not being important to safety but which have a relatively high safety significance.

12.83. Cumulative impact of ~~risk significance of SSCs that~~ proposed ~~for~~ re-classification of SSCs on risk should be also taken into account when making the decision.

MONITORING AND MANAGING RISK CONFIGURATION

12.84. A risk monitor is a real time analysis tool that should be used to generate risk information based on the actual plant configuration in terms of a number of factors that typically include: the plant operating state (power operation or one of the shutdown states), the components that have been removed from service and the choice of operating trains and standby trains for normally operating systems.

12.85. The risk monitor can be used for the planning of future maintenance outages, long term profiling of risk, analysis of the cumulative incremental conditional core damage probability and the evaluation of risks, associated with abnormal plant operation (i.e. unexpected events such as equipment failures).

12.86. The information generated by the risk monitor can be used in day to day maintenance planning to ensure that maintenance activities are scheduled in such a way that high peaks in risk are avoided wherever possible and the cumulative, incremental, conditional core damage probability of the plant is low.

12.87. The quantitative and qualitative risk information produced by the risk monitor for operating plants should be used as part of an integrated, risk informed decision making process that also takes account of the other requirements (such as the plant's technical specifications or maintaining defence in depth). Even though risk monitors are used at operating plants it is a good practice to initiate it development at design stages when plant design is already fixed.

12.88. The risk monitor should provide both quantitative risk information (calculations of the point in time core or fuel damage frequency, allowed configuration time and the cumulative incremental conditional core damage probability) and qualitative risk information (the status of safety functions and systems).

PSA model and software for a risk monitor

12.89. The ~~Level 1~~ PSA model for the risk monitor should be amended so that it calculates the 'point in time risk' for each of the plant configurations entered rather than the average risk generally calculated by the PSA.

12.90. The PSA model should be amended to remove any simplifications made to reduce the amount of analysis needed for the PSA, as they could lead to the risk monitor giving incorrect results for some of the plant configurations that could arise.

12.91. To develop the risk monitor, the PSA model should be enhanced so that it provides a calculation of the risk that relates more closely to the actual plant configuration. For example, it has to be possible to set to TRUE or FALSE the status of basic events that describe component unavailability due to testing or maintenance to reflect actual component configuration. The PSA model developed should also be compatible with the software used for the risk monitor[58].

12.92. The risk monitor should be designed to be used by nuclear power plant personnel knowledgeable about plant design and operations, rather than just PSA specialists.

12.93. The changes that a PSA practitioner and the user of the risk monitor users may make should commensurate with the level of expertise of those individuals and should be well documented.

12.94. The software selected (or developed) for the risk monitor application should be validated, should provide a wide range of functions and should be usable by a wide range of plant staff.

12.95. The software should be capable of providing results within a time frame that meet the needs of needs of its primary users (e.g. work planners and control room operators) to meet its intended functions (e.g. assess and manage configuration risk of planned or emergent conditions).

12.96. The risk monitor should present information in a way that can be understood by the potential users. This is usually done in the form of coloured displays that give the user a clear visual indication of the level of risk or the status of safety functions and systems.

12.97. The risk monitor validation process should aim at providing a high level of confidence that the quantitative results given by the risk monitor are accurate and the same as, or equivalent to, those given by the original PSA for all likely plant configurations.

Limitations of risk monitors

12.98. The users of risk monitor should be aware of important limitations in the scope or level of detail of the risk monitor model and consequent limitations in the risk information provided by the risk monitor. For example, if the model does not include internal and external hazards it may fail to capture the significance of ~~mitigating system~~credited systems that are dedicated to mitigate the events caused by these hazards and should not be used for decision making without justification that the decision under consideration does not impact the missing part of the model.

RISK BASED SAFETY PERFORMANCE INDICATORS

[58] The changes necessary may include changing the event tree and fault tree models developed in the PSA into a logically equivalent large fault tree model (usually referred to as a ‘top logic model’) or changing the way that NOT logic and logical switches are used in the model.

12.99. The PSA results should be used to determine the appropriate set of performance indicators to provide retrospective or current indications of plant safety performance.

12.100. Risk based indicators focused on past plant behaviour integrating the events that have occurred, and failures and unavailabilities, should provide trends and comparisons between expected and calculated risk values for decision makers to pinpoint ageing effects on SSCs.

12.101. Risk based indicators should also provide information on changes in risk associated with planned activities. Such indicators should be based on instantaneous evaluation of risk.

12.102. When risk informed safety performance indicators are established and agreed upon between the regulatory body and the operating organization, they should be used to increase the efficiency of the inspections.

12.103. Risk based indicators should be derived using a risk monitor or a ~~Level 1~~ PSA that are based on plant specific data and actual operating experience.

PSA BASED EVENT ANALYSIS

12.104. Operating events, which may initiate a plant trip and/or degrade or disable ~~safety systems~~SSCs can be analysed and ranked using the PSA model. This is now an increasingly common practice in many States and forms a routine part of operational feedback to complement the traditional deterministic analysis that is carried out to determine root causes.

12.105. The purpose of event analysis is to determine how an operating event could have degenerated into an accident with more serious consequences and to derive the risk significance of such event, so that the event can be responded to in accordance with its risk significance[59].

12.106. PSA based event analysis should be carried out for events at the plant (referred to as 'direct events') and events at other plants ('transposed events'). PSA based event analysis should include the analysis of initiating events (where an initiating event actually occurred and where failures occurred, but where an initiating event was prevented by prompt intervention by operating personnel) and of conditional events (where the likelihood of an initiating event was increased or the availability of the ~~mitigating system~~credited systems required to respond to initiating events was reduced).

12.107. If the event in question is an initiating event, the living Level 1 PSA model should be used to estimate the conditional core or fuel damage ~~frequency~~probability.

12.108. If the event in question impacts the availability of one or more SSCs and/or actions by operating personnel, but is not an initiating event, the PSA model is used to calculate the conditional core damage frequency or fuel damage frequency taking in to account the unavailability of the affected SSCs (e.g. using the risk monitor) .

12.109. The PSA model should be capable of evaluating the appropriate impacts applicable

[59] By risk-based extrapolation of operational events to accident scenarios with serious consequences, valuable insights can be gained regarding accidents on the basis of minor incidents, without suffering their real consequences.

for the event.

12.110. PSA based event analysis should be carried out for events with high potential safety significance. This necessitates that screening criteria be developed that can be applied to screen out events with low safety significance and to rank events in accordance with their significance.

12.111. The condition of the plant, failures that have occurred and the actions by operating personnel that were carried out during the event should be determined and accurately mapped in the PSA model. The PSA model should be re-quantified to generate the results necessary for comparison with the criteria discussed in the previous paragraph. The results necessary for comparison are typically the conditional core damage probability or fuel damage probability for initiating events and the increase in core damage frequency or fuel damage frequency for conditional events.

12.112. The analysis of the event should be supplemented by sensitivity studies to provide the answer to "what if?" questions. For example, "what would the conditional core damage probability have been if operating personnel had failed to respond to the event correctly?" The answers to such questions should be supplemented by qualitative insights to provide an understanding of the principal contributors to the risk of the event.

12.113. PSA based event analysis should be carried out to complement deterministic analysis by allowing multiple failure to be addressed using an integrated model and by providing a quantitative indication of the risk significance of operating events. It should also be used to provide an input into the consideration of what changes could be made to reduce the likelihood of recurrence of such operating events.

12.114. Care should be taken in using the results of the PSA based event analysis for the identification of trends in the performance of a nuclear power plant or a set of nuclear power plants over a period of time. The results of such an application of PSA based event analysis could be misleading unless the analysis uses the same models, methods and assumptions throughout.

12.115. If a MUPSA model is available, it should be used to support PSA based event analyses by accounting for degradation of shared systems and impact of initiating event on the behaviour of operating personnel and shared resources if several units can be affected.

RISK INFORMED REGULATIONS

12.116. ~~Level 1~~ PSA should be used to identify plant specific or generic risk insights and design or operating changes that could enhance safety. PSA insights should be also used to guide long term prioritization of regulatory objectives and requirements, and of related safety research. Change in risk metrics are used to evaluate possible changes to regulatory requirements needed to implement the risk management strategy.

12.117. Regulatory bodies should consider using PSA insights to promulgate risk-informed regulations that enhance public safety or issue plant-specific orders in accordance with the national safety policies and regulations.

12.118. In some situations, PSA insights may show that regulations impose significant burdens on operating organizations with negligible safety benefits. In such situations, regulatory bodies should consider whether it is appropriate to promulgate risk-informed alternatives to existing regulations or eliminate such regulations using in accordance with

national safety policies and regulatory requirements.

12.119. In developing and updating regulations and regulatory guides, the regulatory body should employ a risk informed approach that takes account of the risk information and insights provided by the ~~Level 1~~ PSA, as follows:

(a) The aim should be to use insights from the ~~Level 1~~ PSA to identify areas not covered by existing regulations that are risk significant so that additional regulations can be established;

(b) To determine the relative risk significance of existing regulations or requirements so that they can be amended, commensurate with their risk significance;

(c) To identify unnecessary or ineffective parts of regulations or requirements so that they can be withdrawn.

12.120. The scope and level of details of the ~~Level 1~~ PSA should commensurate with the issue under investigation and ~~Level 1~~ PSA should be able to take into account all aspects dealing with the issue.

RISK-INFORMED OVERSIGHT AND ENFORCEMENT

12.121. The activities carried out by a regulatory body for operating plant include issuing, amending, suspending or revoking authorizations or licences; carrying out regulatory oversight; ensuring that corrective actions are taken and taking enforcement actions when necessary. Qualitative or ~~quantities~~ quantitative risk insights derived from PSA ~~Level 1~~ should be used to prioritize and to optimize the oversight activities of the regulatory body, for example, as follows:

(a) For defining plant design and operational aspects to ensure that inspections are focused on areas of the plant design and operation that have high risk significance and are reduced or not carried out in areas that have low risk significance.

(b) For planning regulatory actions in response to plant-specific events or plant-specific potentially degraded conditions revealed by operating experience, the regulators should consider the risk significance to determine the magnitude of the follow-up activities. (e.g. need for follow-up regulatory actions and enforcement);

(c) For assessment of the significance of the failure by the operating organization to meet regulatory expectations and comply with enforcement actions.

(d) For assessment of changes in risk measures associated with inspection findings. Change in risk metrics and conditional risk metrics can be used to evaluate the risk impact of degradations or issues that are found during the inspections and to evaluate possible corrective actions.

(e) For development and evaluation of corrective measures regarding safety issues identified in oversight process. This may include exploratory investigation on different variants to resolve a particular issue when change in risk metrics are used to determine the risk significance and risk acceptability of the proposed measures based on risk characterization. Change in risk metrics should be used to determine the risk significance and risk acceptability of the proposed measures based on risk characterization.

12.122. ~~Level 1~~ PSA should be used for evaluation and ranking both generic and newly

identified plant specific safety issues. Contributors to risk and risk importance measures should be used to identify and rank safety issues. Also, safety issues identified outside the PSA can be evaluated by the PSA to determine their risk significance once the issues have been assessed for risk characterization, i.e. determination of affected initiating events, accident sequences, SSCs and actions by operating personnel.

12.123. PSA is also used to define regulatory interim decisions to alleviate a regulatory concern, while longer term solutions can be evaluated. Issues that typically require an interim decision are: (i) need for regulatory action in response to an event at a plant, (ii) one-time exemptions from technical specifications or other licensing requirements, and (iii) temporary modifications to hardware configuration or procedures.

12.124. The scope of PSA to be used should be sufficient to provide valuable information and depends on the area of regulatory concerns and inspection findings. Simplified generic PSA models initially could be used to perform a conservative screening evaluation first and if the results are significant, it should be followed by a more realistic and detailed evaluation. It should be extended when needed to evaluate specific issue of concerns.

USE OF PSA INSIGHTS TO DEVELOP OR ENHANCE EMERGENCY OPERATING PROCEDURES

12.125. The systematic assessment of plant vulnerabilities and the insights derived from the Level 1 PSA should be used to identify any potential need to further develop (i.e. refine or extend coverage scope) emergency operating procedures by providing assurance that a broad scope of vulnerabilities is addressed in a realistic, appropriately detailed and consistent manner.

12.126. At the design stage, Level 1 PSA uses emergency operating procedures from reference plants for accident sequence modelling and human reliability analysis. The PSA process allows procedures that do not fully take into account specific design features to be identified. At the design stage, risk insight should be used to identify procedures that are not available at reference plants and should be developed, or procedures that need to be further elaborated. Risk insight should also provide information on the particular human actions that should be included, and conditions that should be explicitly described, in the emergency operating procedures to allow operating personnel to correctly perform actions.

12.127. For operating plants, information available from accident sequence analysis in Level 1 PSA carried out using existing emergency operating procedures, and the assessment of the associated human interactions, should be used for identification of emergency operating procedures that need improving in the light of PSA insights.

12.128. Level 1 PSA results should be reviewed to look for plant event sequences making an excessive risk contribution and for which ~~mitigating system~~credited systems are still available but cannot be credited because of lack of adequate emergency operating procedures. For such plant event sequences, emergency operating procedures should be further developed.

12.129. The insights derived from the Level 1 PSA should be used to identify and evaluate risk benefit from existing, alternative or additional systems, equipment and measures that can be proposed for inclusion in the emergency operating procedures with the purpose of restoring the function of ~~mitigating system~~credited systems and for preventing degradation of events into severe accidents. The integral view of plant response utilized in the ~~Level 1~~ PSA methodology should be used in determining the potential for negative effects of certain measures.

12.130. Risk importance measures[60] of affected or proposed actions and associated accident sequences should be used to help prioritize candidate procedural changes and changes in core damage frequency or fuel damage frequency should be used to justify acceptable risk impacts and to determine risk significance.

12.131. A Level 1 PSA treatment of actions by operating personnel should support the enhancement of emergency operating procedures for those actions aimed at preventing severe core or fuel damage.

12.132. The level of detail of the Level 1 PSA model in the areas affected by the procedure changes including the accident sequences should be increased when existing Level 1 PSA does not explicitly represent accident sequences and actions by operating personnel that refer specifically to invoking the relevant emergency operating procedures.

12.133. The human reliability analysis method used in the Level 1 PSA should be capable of predicting the impact of the procedure changes to support this application, otherwise they should be reconsidered.

12.134. Level 1 PSA should also provide the ~~basis~~ feedback and potential revision of the specified ~~for specifying the~~ decision points for ~~when the~~ transition to severe accident management guidelines ~~should occur~~.

USE OF PSA INSIGHTS TO RISK-INFORM THE TRAINING OF OPERATING PERSONNEL

Improvement of the training programme for operating personnel

12.135. The results of the Level 1 PSA should be used to determine the subset of risk-significant actions by operating personnel and to develop (for plants under designs) or improve (for operating plants) the training programme for operating personnel by providing information on the accident processes, the relative likelihood of the dominant accident sequences, and the associated actions necessary to prevent or mitigate core or fuel damage.

12.136. Descriptions of dominant accident sequences for core or fuel damage frequency in which HFEs play a significant role, risk importance measures of HFEs and associated SSCs, recovery actions and accident management actions with high risk importance should be used to enhance the training programme for operating personnel. These should also be used to mitigate the consequences of HFEs and the PSA results should be used to select those actions that would benefit from enhanced training[61].

12.137. The human reliability analysis methods used in the ~~Level 1~~ PSA treatment should be capable of measuring the affected changes, and change in risk metrics should allow analysts to evaluate the significance and acceptability of the proposed change.

12.138. Operating personnel at nuclear power plants spend a significant fraction of their

[60] Typically, Fussell–Vesely importance and the Birnbaum importance (or the risk achievement worth)

[61] The risk achievement worth importance of a human failure events is representative of the ratio by which the fuel damage will increase if an individual fails to perform an action. Conversely, the Fussel-Vessely importance parameter is representative of the fraction by which fuel damage frequency can be reduced if the individual is successful. Therefore, both importance parameters should be used as an input to risk-inform the training of operating personnel.

time being trained on large number of plant procedures; consequently, the above risk insights should be used to risk-inform training and ensure that operating personnel receive sufficient time to learn about risk-significant actions.

12.139. The enhancements to the training should, at a minimum, include informing operating personnel about the risk significant actions. Other enhancements may include making adjustments to the frequency of simulator training on certain scenarios, adding risk-significant scenarios to qualification programs for operating personnel, and using risk-significant scenarios in drills.

Improvement of the training programme for maintenance personnel

12.140. Training of maintenance staff should be enhanced based on insights and information from the ~~Level 1~~ PSA by focusing on potential risk significant impacts of maintenance activities, such as common cause failure and maintenance-induced failure of multiple system trains.

12.141. Risk insights provide information on risk significant SSCs and on risk significant functions and failure modes that should be addressed in the maintenance programme as well as opportunities to optimize maintenance tasks that are not significant to risk management.

12.142. The same risk importance measures as recommended in para. 12.130 should be used to identify risk significant SSCs, pre-accident HFEs, and basic events dealing with maintenance and common cause failures and to rank them to consider for potential maintenance programme changes.

12.143. Changes in risk metrics (e.g. fuel damage frequency) should be used to evaluate the significance and acceptability of the proposed change to maintenance training programme.

USE OF PSA TO ADDRESS EMERGING ISSUES

12.144. As plants continue to operate, operating experience may reveal various issues that were unknown during the design, construction, and early operation of the plants (e.g. new age-related failure mechanisms of passive systems, structures, or components).

12.145. PSA insights (qualitative and\or quantitative) should be used to assess the risk significance of emerging issues.

12.146. Since many issues that emerge are passive age-related degradations and challenges associated with replacing aged components that are obsolete, these might not be explicitly modelled in the PSA. Therefore, a PSA should carefully evaluate how the issue should be accurately modelled (e.g. without overly conservative assumptions) using the PSA model (e.g. a degraded condition in a subset of control rods should not be modelled as failure to insert rods). Since emerging issues in general provide limited information, sensitivity analyses should be used to glean PSA insights.

12.147. Operating personnel should use insights from ~~Level 1~~ PSA discussed above to determine the priority and timelines appropriate to resolve the emerging issue within the construct of national policies and regulatory requirements.

12.148. Regulators should use insights from ~~Level 1~~ PSA to impose appropriate timeline on the operating organization to resolve these issues, within the construct of national safety

policies and regulations.

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-4, IAEA, Vienna (2010).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev.1), IAEA, Vienna (2019).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards in the Design of Nuclear Power Plants (former IAEA Safety Standards Series No. NS-G-1.7, currently being revised DS494).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Existing Nuclear Installations, IAEA Safety Standards Series No. NS-G-2.13, IAEA, Vienna (2009) (currently being revised DS522).

[8] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, A REPORT BY THE INTERNATIONAL NUCLEAR SAFETY GROUP. A Framework for an Integrated Risk Informed Decision Making Process, IAEA; INSAG-25, IAEA, Vienna (2011).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Nuclear Safety, Legal Series No. 16, IAEA, Vienna (1994).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Hierarchical Structure of Safety Goals for Nuclear Installations, IAEA-TECDOC-1874, Vienna (2019).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, CANDU Level 1 Probabilistic Safety Assessment practices for Nuclear Power Plants with CANDU-type reactors, IAEA-TECDOC (draft)

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Human reliability analysis for nuclear installations, Safety Report Series (draft).

[15] US NUCLEAR REGULATORY COMMISSION, NUREG-1921, EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report, ELECTRIC POWER RESEARCH INSTITUTE, Palo Alto, California, 2012.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors, IAEA-TECDOC-1752, Vienna (2014).

[18] OECD/NEA, Failure modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis, NEA/CSNI/R(2014)16, Paris (2015).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Energy Series No. NP-T-3.27, Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants. IAEA, Vienna (2018).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSR-1, IAEA, Vienna (2019).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002)

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-9, IAEA, Vienna (2010).

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD METEOROLOGICAL ORGANIZATION, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-18, IAEA, Vienna (2011).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodologies for seismic safety evaluation of existing nuclear installations, Safety Report Series No 103, IAEA, Vienna (2020).

[26] ELECTRIC POWER RESEARCH INSTITUTE, Identification of External Hazards for Analysis in Probabilistic Risk Assessment: Update of Report 1022997, EPRI, Technical Report 3002005287, Palo Alto, California, USA, (2015).

[27] List of External Hazards to be considered in ASAMPSA_E, Technical Report, ASAMPSA_E / WP21 / D21.2 / 2017-41, (2016).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events, IAEA-TECDOC-1834, IAEA, Vienna (2017).

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003) (currently being revised DS498).

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Safety in the Operation of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.1, IAEA, Vienna (2000).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for seismic events, IAEA-TECDOC (in publication).

[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-21, IAEA, Vienna (2012).

[33] ELECTRIC POWER RESEARCH INSTITUTE, Methodology for Seismically Induced Internal Fire and Flood Probabilistic Risk Assessment. EPRI, Palo Alto, CA: 2018. 3002012980.

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1804, IAEA, Vienna (2016).

[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, IAEA, Vienna (2001).

[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on Performing Integrated Risk Informed Decision Making, IAEA-TECDOC-1909, Vienna (2019).

[38] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for the Decommissioning of Facilities Using Radioactive Material. IAEA Safety Standards Series No. WS-G-5.2, IAEA, Vienna (2008).

[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk-informed In-service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues and Development, No. NP-T-3.1 (2010).

[40] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2011).

[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Terminology Used in Nuclear Safety and Radiation Protection (IAEA Safety Glossary), draft revision, 2020

[42] US NUCLEAR REGULATORY COMMISSION, NUREG/CR-6580, EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, 2005.

ANNEX I. EXAMPLE OF A GENERIC LIST OF INTERNAL AND EXTERNAL HAZARDS

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
Air based natural hazards			
A1	Strong wind	The hazard is defined in terms of damage to the plant due to strong winds. It includes both direct damage from wind pressure and indirect damage due to wind-borne missiles.	The hazard does not include tornado (A2) due to the unique characteristics of this hazard. The hazard does not include the differentiating effects of snowstorm (included in A7), saltstorm (A12) or sandstorm (A13). However, the wind effects of these hazards are included. Effects of storm surges are covered by the hazard high water level (W3).
A2	Tornado	The hazard is defined in terms of damage to the plant due to tornadoes. The hazard is separated from other strong winds owing to its special characteristics with respect to duration, wind speed and frequency of occurrence.	
A3	Downburst ~~High air temperature~~	The hazard is defined in terms of impact on the plant of downburst.~~The hazard is defined in terms of impact on the plant of high air temperature.~~	This hazard has also unique characteristics (e.g. wind speed vertical profile) that differ from strong winds. Wind speed does not decrease at lower levels from the ground, as with strong winds.~~Plant impact due to high water temperatures is treated separately (W4).~~
A4	High air temperature~~Low air temperature~~	The hazard is defined in terms of impact on the plant of high air temperature.~~The hazard is defined in terms of impact on the plant of low air temperature.~~	Plant impact due to high water temperatures is treated separately (W4).~~Plant impact due to low water temperature (W4) or ice impact (W7, W8, W9) is treated separately.~~
A5	Low air temperature~~Extreme air pressure (high/low gradient)~~	The hazard is defined in terms of impact on the plant of low air temperature.~~The hazard is defined in terms of impact on the plant of high or low air pressure or of rapid pressure changes.~~	Plant impact due to low water temperature (W4) or ice impact (W7, W8, W9) is treated separately.
A6	Extreme air pressure (high/low gradient)~~Extreme rain~~	The hazard is defined in terms of impact on the plant of high or low air pressure or of rapid pressure changes.~~The hazard is defined in terms of damage to the plant due to extreme rain.~~	~~It includes both damage due to rain load on structures and damage due to rain induced flooding.~~
A7	Extreme rain~~Extreme snow (including snowstorm)~~	The hazard is defined in terms of damage to the plant due to extreme rain. ~~The hazard is defined in terms of damage to the plant due to extreme snow, including snowstorms.~~	It includes both damage due to rain load on structures and damage due to rain induced flooding.~~Wind effects due to snowstorms are covered by the hazard strong wind (A1). Flooding effects due to melting of snow are judged to be bounded by flooding effects due to extreme rain (A6).~~

A8	Extreme snow (including snowstorm) ~~Extreme hail~~	The hazard is defined in terms of damage to the plant due to extreme snow, including snowstorms.~~The hazard is defined in terms of damage to the plant due to extreme hail. It includes damage due to hail load on structures.~~	Wind effects due to snowstorms are covered by the hazard strong wind (A1). Flooding effects due to melting of snow are judged to be bounded by flooding effects due to extreme rain (A6).~~Flooding effects due to melting of hail are bounded by flooding effects due to extreme rain (A6). Any possible effects on the ultimate heat sink are judged to be bounded by ice hazards (W7, W8, W9).~~
A9	Extreme hail ~~Mist~~	The hazard is defined in terms of damage to the plant due to extreme hail. It includes damage due to hail load on structures.~~The hazard is defined in terms of impact on the plant of mist.~~	Flooding effects due to melting of hail are bounded by flooding effects due to extreme rain (A6). Any possible effects on the ultimate heat sink are judged to be bounded by ice hazards (W7, W8, W9).
A10	Mist ~~White frost~~	The hazard is defined in terms of impact on the plant of mist.~~The hazard is defined in terms of impact on the plant of white frost.~~	
A11	White frost ~~Drought~~	The hazard is defined in terms of impact on the plant of white frost.~~The hazard is defined as an extended drought period that lowers the water level of lakes, rivers and open water basins.~~	~~Possible plant impacts due to high air temperature (A3) or high water temperature (W4) are covered by the analysis of these hazards. There is considered to be no effect on water level (heat sink).~~
A12	Drought ~~Saltstorm~~	The hazard is defined as an extended drought period that lowers the water level of lakes, rivers and open water basins.~~The hazard is defined as a storm involving salt covering of plant structures.~~	Possible plant impacts due to high air temperature (A3) or high water temperature (W4) are covered by the analysis of these hazards. There is considered to be no effect on water level (heat sink).~~Wind effects from saltstorms are covered by the hazard strong wind (A1).~~
A13	Saltstorm ~~Sandstorm~~	The hazard is defined as a storm involving salt covering of plant structures.~~The hazard is defined in terms of impact on the plant of storm-borne sand.~~	Wind effects from saltstorms are covered by the hazard strong wind (A1).~~Wind effects from sandstorms are covered by the hazard strong wind (A1).~~
A14	Sandstorm ~~Lightning~~	The hazard is defined in terms of impact on the plant of storm-borne sand.~~The hazard is defined in terms of damage to the plant due to lightning. The impact may be direct, causing structural damage or hazards relating to loss of off-site power, or indirect through an electromagnetic feeder fire started by lightning.~~	Wind effects from sandstorms are covered by the hazard strong wind (A1).~~Fire started by lightning is bounded by external fire (G7) and by the internal fire analysis.~~
A15	Lightning ~~Meteorite~~	The hazard is defined in terms of damage to the plant due to lightning. The impact may be direct, causing structural damage or hazards relating to loss of off-site power, or indirect through an electromagnetic feeder fire started by lightning.~~The hazard is defined in terms of damage to the plant due to meteorite impact.~~	Fire started by lightning is bounded by external fire (G7) and by the internal fire analysis.

A16	Meteorite	The hazard is defined in terms of damage to the plant due to meteorite impact.	
Ground based natural hazards			
G1	Land rise	The hazard is defined in terms of impact on the plant of land rise.	
G2	Soil frost	The hazard is defined in terms of impact on the plant of soil frost.	
G3	Animals	The hazard is defined in terms of impact on the plant of animals.	Impact on intake water from fish, mussels, etc., is covered by W10.
G4	Volcanic phenomena	The hazard is defined in terms of impact on the plant of volcanic eruptions.	
G5	Avalanche	The hazard is defined in terms of impact on the plant of avalanches.	
G6	Above water landslide	The hazard is defined in terms of impact on the plant of above water landslide.	
G7	External fire	The hazard is defined in terms of impact on the plant of fire originating from outside the plant, inside or outside the site area.	Internal fires spreading from another plant on the site are treated separately (M15). Fires resulting as secondary effects of other external hazards are treated as part of these hazards (M2, M11, M20). Internal fires are analysed as part of the PSA for internal hazards.
G8	Seismic hazards	The hazard is defined in terms of impact on the plant of an earthquake.	
G9	Karsts	The hazard is defined in terms of impact due to fissures, sinkholes, underground streams and caverns caused by erosion.	
Water based natural hazards			
W1	Strong water current (underwater erosion)	The hazard is defined in terms of damage to plant structures due to strong water current.	The effects of underwater landslide are treated separately (W6).
W2	Low water level	The hazard is defined in terms of impact on the plant of low water level.	Level decrease due to land rise is covered by G1.
W3	High water level	The hazard is defined in terms of impact on the plant of high water level. High water levels may be due to storm surges, waves, meteotsunamis or seiches. High water levels are also affected by tidal variations.	

W4	High water temperature	The hazard is defined in terms of impact on the plant of high water temperature.	Plant impact due to high air temperature is treated separately (A3).
W5	Low water temperature	The hazard is defined in terms of impact on the plant of low water temperature.	Plant impact due to low air temperature (A4) or ice impact (W7, W8, W9) is treated separately.
W6	Underwater landslide	The hazard is defined in terms of impact on the plant of underwater landslide.	An underwater landslide may be due to above water causes, such as prolonged and intense precipitation. Plant impact due to underwater erosion is treated as part of the strong current hazard (W1).
W7	Surface ice	The hazard is defined in terms of impact on the plant of thick surface ice.	The hazard does not include effects due to frazil ice (W8) and ice barriers (W9).
W8	Frazil ice	The hazard is defined in terms of impact on the plant of frazil ice in the cooling water intake.	
W9	Ice barriers	The hazard is defined in terms of impact on the plant of ice barriers.	
W10	Organic material in water	The hazard is defined in terms of impact on the plant of organic material in intake water. The material may be algae, seaweed, fish, mussels, jellyfish, etc.	
W11	Corrosion (from salt water)	The hazard is defined in terms of impact on the plant of corrosion.	
W12	Solid or fluid (nongaseous) impurities from ship release	The hazard is defined in terms of impact on the plant of solid or fluid (non-gaseous) impurities released into the water from a ship.	
W13	Chemical release to water	The hazard is defined in terms of impact on the plant of chemical releases to water. The focus is on reduction of water quality. The releases may be due to a ship accident, but may also originate on land.	The hazard does not include effects due to release of solid or fluid (non-gaseous) impurities (W12).
W14	Tsunami	The hazard is defined in terms of damage to the plant due to high water level and pressure from the wave.	
Off-site accidents			

M1	Direct impact from ship collision	The hazard is defined in terms of the direct impact of a ship.	The hazard does not cover consequences of releases in connection with a ship accident (explosion, pollution, intake clogging or release of toxic gases), as these hazards are handled separately (M2, M3, W12, W13).
M2	Explosion after transportation accident	The hazard is defined in terms of damage to the plant resulting from explosion after ground transportation accidents outside the site or due to sea, lake or river transportation accidents. The damage may be due to pressure impact or impact from missiles.	The hazard does not include damage due to aircraft crash (M20) or originating from pipeline accident (M5). Toxic effects from a chemical release are covered by M3.
M3	Chemical release after transportation accident	The hazard is defined in terms of intake clogging or toxic impact on the plant resulting from chemical release after ground transportation accidents outside the site or due to sea, lake or river transportation accidents.	Explosion effects from transportation accidents are covered by M2.
M4	Explosion outside plant	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) of solid substances or gas clouds outside the site. The damage may be due to pressure impact or impact of missiles.	The hazard does not include explosions in connection with transportation accidents outside the site (M2) or originating from pipelines (M5). Toxic effects from a chemical release are covered by M6.
M5	Explosion after pipeline accident	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) after a pipeline accident. The damage may be due to pressure impact or impact of missiles.	Toxic effects from a chemical release are covered by M7. Explosion effects from a release outside or within the site are covered by M4 and M11. Toxic effects after transportation or pipeline accidents are analysed in M3 and M7.
M6	Chemical release outside site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release outside the site. These releases may originate from process accidents outside the plant or from leakages of substances stored outside the plant.	
M7	Chemical release after pipeline accident	The hazard is defined in terms of toxic impact on the plant resulting from chemical release after a pipeline accident.	Explosion effects from pipeline accidents are covered by M5.

M8	Missiles from military activity	The hazard is defined in terms of impact on the plant of missiles from military activity.	Impact on power supply and heat sink assumed to be bounded by other hazards.
M9	Excavation work	The hazard is defined in terms of impact on the plant of excavation work, inside or outside the site area.	
On-site accidents			
M10	Direct impact of heavy transportation within the site	The hazard is defined in terms of damage to the plant resulting from direct impact of heavy transportation within the site, but outside the plant buildings. This also includes transportation of the containment external maintenance platform.	Heavy transportation within plant buildings is analysed as part of the PSA for internal hazards.
M11	Explosion within the site	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) of solid substances or gas clouds within the site, but outside the plant buildings. The damage may be due to pressure impact or impact of missiles.	The explosions within plant buildings are analysed as part of the PSA for internal hazards.
M12	Explosion after pipeline accident within the site	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) after a pipeline rupture on the site. The damage may be due to pressure impact or impact from missiles.	
M13	Chemical release within the site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release within the site.	These releases may originate from process accidents inside the plant or from leakages of substances stored within the site, but outside the plant buildings. The chemical releases from substances stored inside buildings are analysed as part of the PSA for internal hazards.
M14	Chemical release after pipeline accident within the site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release after a pipeline accident at the site.	
M15	Internal fire spreading from other units on the site	The hazard is defined in terms of impact on the plant of fires originating in another unit on the site.	External fires are treated separately (G7). Fires resulting as secondary effects from other external hazards are treated as part of these hazards (M2, M11, M20).

M16	Missiles from other units on the site	The hazard is defined in terms of damage to the plant resulting from missiles generated at another unit on the site.	
M17	Internal flood and harsh environment spreading from other units on the site	This hazard is defined in terms of damage to the plant resulting from water spreading effects from other units.	
M18	Excavation work within the site area	The hazard is defined in terms of impact on the plant of excavation work within the site area.	
Aircraft crash			
M19	Satellite crash	The hazard is defined in terms of damage to the plant resulting from satellite impact.	
M20	Aircraft crash	The hazard is defined in terms of damage to plant structures resulting from an aircraft crash within the site area. The aircraft may be commercial, private or military.	
Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
Other human-induced hazards			
M21	Magnetic disturbance	The hazard is defined in terms of impact on the plant of human-induced magnetic or electrical fields. The main examples of such fields are those attributable to radar, radio and mobile phones.	
M22	Failure of a dam upstream of the plant	The hazard is defined in terms of damage to SSCs resulting from high level water and water waves.	

Note: The list of hazards is based on Ref. [I–1]. Internal hazards originating inside plant buildings are not included in the table.

REFERENCES TO ANNEX I

[I–1] KNOCHENHAUER, M., LOUKO, P., Guidance for External Events Analysis, Rep. SKI-R-02/27-SE, SKI, Stockholm, February 2003.

ANNEX II. EXAMPLES OF FIRE PROPAGATION EVENT TREES AND SEISMIC EVENT TREES

ILLUSTRATION OF THE USE OF THE EVENT TREE TECHNIQUE FOR THE ANALYSIS OF FIRE MITIGATION AND PROPAGATION

II–1. The example of a fire propagation event tree presented in Fig. II–1 comprises the relevant features starting with fire initiation. Early and late detection of fire are distinguished as these cases are associated with different probabilities to control and extinguish the fire. For fire propagation, it is relevant whether and to what degree the room is closed. Further modelling addresses available fire suppression equipment, taking into account possible damage to safety relevant items caused by the means of suppression. Figure II–1 provides an illustration of how the event tree technique can be used to analyse fire mitigation and propagation.

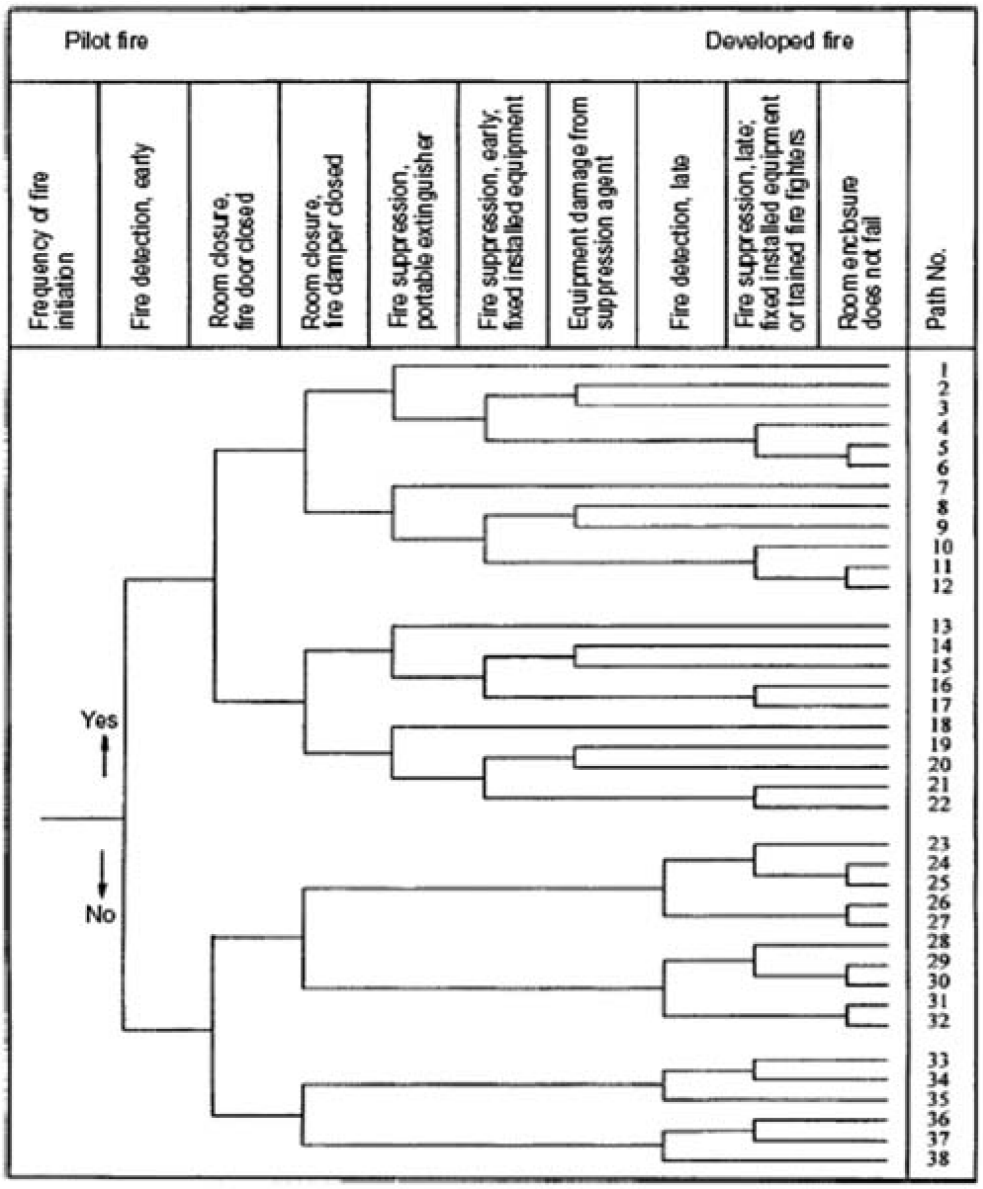

FIG. II–1. Example of a fire propagation event tree.

ILLUSTRATION OF THE USE OF THE EVENT TREE TECHNIQUE FOR IDENTIFICATION OF SEISMICALLY INDUCED INITIATING EVENTS

II–2. Figure II–2 provides an illustration of how the event tree technique can be used to model different consequences of seismically induced initiating events. ~~In this example, it is assumed that the seismic initiating event always leads to a loss of off-site power.~~

Seismic event	Large LOCA	Small LOCA	Loss of service water	Loss of offsite power	General transient		
SE	IE_LLOCA	IE_SLOCA	IE_LOSW	IE_LOOP	IE_TRAN	No.	Consequences
						1	OK
						2	General transient
						3	Loss of offsite power
						4	Loss of service water
						5	Small LOCA
						6	Large LOCA

FIG. II–2. Example of an event tree for the modelling of a seismically induced initiating event. Loss of coolant accident.

ANNEX III. SUPPORTING INFORMATION ON PSA FOR SHUTDOWN STATES

EXAMPLES OF PLANT OPERATING STATES AND ASSOCIATED INITIATING EVENTS

III–1. In the framework of a PSA for the German boiling water reactor type SWR 69, a probabilistic evaluation of shutdown states was performed [III–1]. An example of a pressurized water reactor plant is provided in Ref. [III–2].

III–2. On the basis of Ref. [III–1], information is presented to illustrate how the plant operating state can be specified and how initiating events can be associated with the plant operating state. For the description of the changing of system related and physical states, the outage was divided into plant operating states (see Fig. III–1 and Table III–1). The plant operating states were chosen in such a way that the system availability and the physical states are as constant as possible. Normally, during the outage (states 3-1 to 3-7), one of the two electrical redundancies for emergency power supply, two of the four trains of the residual heat removal system and one of the two trains of the emergency standby system are available. In state 3-4, where most of the maintenance work is performed, the leakage return system in the reactor building sump needs to be available.

III–3. A detailed evaluation of operating experience in Germany was performed to find events that can lead to initiating events or that can influence the control of accidents during shutdown states. In addition to evaluating German operating experience, the results of international shutdown PSAs were evaluated [III–3, III–4].

III–4. German documents providing guidance on PSA were also used as a basis for identification of initiating events [III–5 to III–7].

III–5. The identification of the initiating events and the assignment to the plant operating state in which they can occur lead to the matrix shown in Table III–2. The cells marked with an ‘X’ in Table III–2 indicate that the initiating event can occur in this plant operating state. As pointed out in para. 9.12, the end states to be included have to be decided on the basis of national probabilistic safety goal or criteria.

III–6. As an example, corresponding information for a pressurized water reactor type plant is provided in Ref. [III–2] and summarized in Tables III–3 and III–4. Table III–3 shows the plant operating states to be distinguished. In Table III–4, the initiating events to be considered in the different plant operating states are displayed. This list is based on an analysis of national and international operating experience.

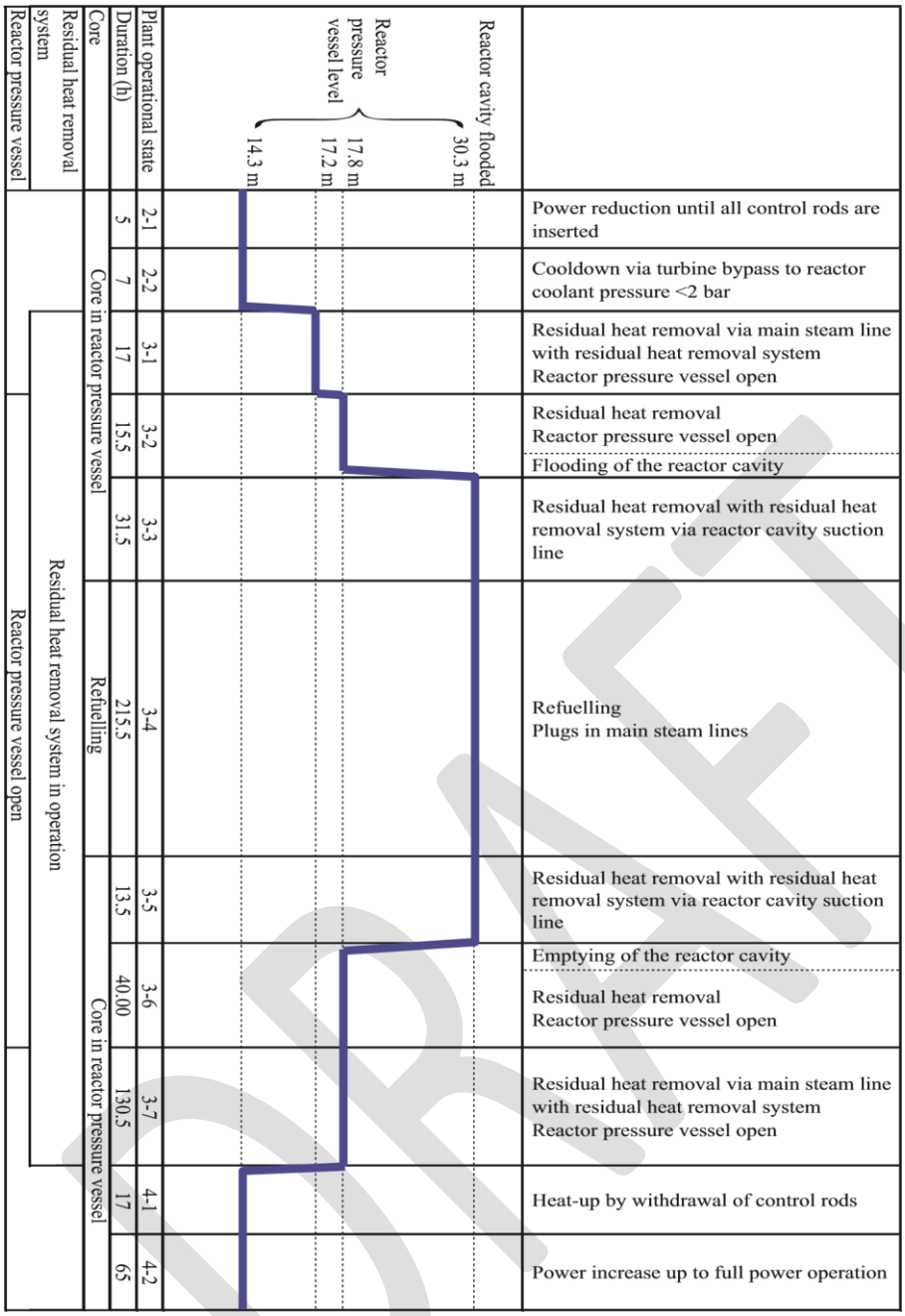

FIG. III–1. Reactor coolant level during outage.

TABLE III–1. PLANT OPERATING STATES DURING OUTAGE IN THE REFERENCE PLANT

	Plant operating state	Characterization of plant operating state
Shutdown	2-1	Power reduction until all control rods are inserted
	2-2	Cooldown via turbine bypass to reactor coolant pressure <2 bar; closing of main steam isolation valves; increase of water level in the reactor above the main steam lines by injection from residual heat removal system
Outage	3-1	Residual heat removal via main steam line with residual heat removal system; reactor pressure vessel closed; reactor coolant temperature 130–50°C
	3-2	Residual heat removal via main steam line with residual heat removal system; reactor pressure vessel open; reactor coolant temperature <40°C; mounting of the reactor cavity seal liner; flooding of the reactor cavity
	3-3	Reactor cavity flooded; residual heat removal with residual heat removal system via reactor cavity suction line; opening of the refuelling hatch; insertion of plugs in main steam lines
	3-4	Refuelling; residual heat removal with residual heat removal system via reactor cavity suction line
	3-5	Removal of plugs in main steam lines; closing of the refuelling hatch; residual heat removal with residual heat removal system via reactor cavity suction line
	3-6	Emptying of the reactor cavity; residual heat removal via main steam line with residual heat removal system; removal of the reactor cavity seal liner
	3-7	Reactor pressure vessel closed; residual heat removal via main steam line with residual heat removal system
Restart	4-1	Shutdown of residual heat removal system; level lowering in the reactor below main steam lines; withdrawal of control rods for heat-up
	4-2	Turbine bypass operation; turbogenerator in operation; synchronization; power increase up to full power operation

TABLE III–2. INITIATING EVENTS DURING OUTAGE IN THE REFERENCE PLANT *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event respectively)*

Initiating event		Plant operating state										
		Shutdown		Outage							Restart	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
Transients												
T1	Loss of main heat sink	X	X									X
T2	Loss of preferred power	X	X	X	X	X	X	X	X	X	X	X
T3	Loss of main feedwater	X	X									X
T4	Loss of main feedwater and main heat sink	X	X									X
T5	Failure to close a safety valve	X	X								X	X
T6	Leak at suppression pool		X		X							
T7	Overfeeding of reactor pressure vessel with main feedwater system	X	X									X
T8	Overfeeding of reactor pressure vessel with residual heat removal system		X									
T9	Loss of residual heat removal			X	X	X	X	X	X	X		
T10	Loss of spent fuel pool cooling	X	X	X	X	X	X	X	X	X	X	X
TA	Anticipated transient without scram	X									X	X
Loss of coolant accidents												
S1	Leak at the reactor pressure vessel inside containment											
S1.1	Due to pipe rupture:											
S1.1.1	Above the core (A-nozzle)					X	X	X				
S1.1.2	Underneath the core (L-nozzle)					X	X	X				

TABLE III–2. INITIATING EVENTS DURING OUTAGE IN THE REFERENCE PLANT (cont.)

Initiating event		Plant operating state										
		Shutdown		Outage							Restart	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
S1.2	Due to human error during:											
S1.2.1	Inspection of valves in main steam line						X					
S1.2.2	Inspection of valves in core spray and in primary make-up systems						X					
S1.2.3	Pulling the shaft of a recirculation pump						X					
S1.2.4	Inspection of control rod drives						X					
S1.2.5	Change of in-core neutron flux detectors						X					
S2	Leak at the residual heat removal system			X	X	X	X	X	X	X		
S3	Leak at the reactor cavity seal liner				X	X	X	X	X			
S4	Leak into a connected system											
S4.1	Failure to control the level in reactor pressure vessel			X	X				X	X		
S4.2	Opening of a safety valve during residual heat removal			X	X	X		X	X	X		
S4.3	Leak in residual heat removal heat exchanger			X	X	X	X	X	X	X		
S5	Leak at the spent fuel pool			X	X	X	X	X	X	X		
Fire and internal flooding												
B1	Fire inside containment	X	X	X	X	X	X	X	X	X	X	X
B2	Fire outside containment	X	X	X	X	X	X	X	X	X	X	X
IF	Internal flooding			X	X	X	X	X	X	X		
Criticality accidents												
K1	Erroneous withdrawal of control rods						X					
K2	Erroneous removal of control rods						X					
K3	Fuel loading error						X					
Heavy load drop												
H1	Drop of a fuel element						X					
H2	Drop of heavy load			X	X	X	X	X	X	X		

TABLE III–3. PLANT OPERATING STATES OF A TWO WEEK OUTAGE IN THE REFERENCE PRESSURIZED WATER REACTOR PLANT

No.	Changes in physical condition / *System features*
(1)A0	Power reduction to condition subcritical hot / *Reactor protection signals and availability of safety systems same as during power operation*
(1)A1	Shutdown via steam generators down to primary system pressure of 3.1 MPa and primary system temperature of 120°C / *All reactor protection systems still available*
(1)B1	Primary system cooldown to depressurized cold / *Startup of the residual heat removal system at 120 °C, accumulators and high pressure pumps are disconnected*
(1)B2	Level lowering to mid-loop, mid-loop operation / *Core within reactor pressure vessel, primary system pressure tight closed*
(1)C	Opening reactor pressure vessel head, mid-loop operation / *Core within reactor pressure vessel, primary system not pressure tight closed, refuelling hatch between setdown pool and fuel pool closed*
(1)D	Flooding of reactor cavity, unloading of fuel elements / *Core wholly or partially within reactor pressure vessel, refuelling hatch open*
E	Emptying of reactor cavity and reactor pressure vessel / *Core fully unloaded, refuelling hatch closed, work performed at lower edge loop level*
(2)D	Refilling of reactor cavity, loading of fuel elements / *Core wholly or partially within reactor pressure vessel, refuelling hatch open*
(2)C	Level lowering to mid-loop, closing of the reactor pressure vessel head / *Core within reactor pressure vessel, primary system not pressure tight closed, refuelling hatch closed*
(2)B2	Evacuation and refilling of primary system / *Core within reactor pressure vessel, primary system pressure tight closed*
(2)B1	Primary system heat-up with main coolant pumps / *All reactor protection systems available*
(2)A1	De-boration of coolant and taking reactor to critical condition / *Withdrawal of control rods and/or de-boration*
(2)A0	Power increase up to specified level / *Reactor protection signals and availability of safety systems same as during power operation*

Note: (1) denotes plant operating state during shutdown, (2) denotes plant operating state during restart.

TABLE III–4. INITIATING EVENTS DURING SHUTDOWN STATES FOR PRESSURIZED WATER REACTOR *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event, respectively)*

	Plant operating state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Transients	Reactor pressure vessel closed				Reactor pressure vessel open					Reactor pressure vessel closed			
Loss of preferred power – external	x	x	x	x	x	x	x	x	x	x	x	x	x
Loss of preferred power – internal						x	x	x					
Loss of main feedwater without loss of main heat supply	x	x										x	x
Loss of main heat sink without loss of main feedwater	x	x										x	x
Loss of main feedwater and main heat sink	x	x										x	x
Main steam line leak outside containment	x	x										x	x
Main steam line leak inside containment	x	x										x	x
Feedwater line leak in turbine building	x	x										x	x
Feedwater line leak inside containment, non-isolable	x	x										x	x
Loss of residual heat removal due to:													
— Faulty level lowering				x					x				
— Operational failure of residual heat removal trains			x	x	x	x		x	x	x			
Unintended activation of emergency core cooling system signals				x									
Small primary system leak A<25 cm²	x	x	x								x	x	x
Small primary system leak 25 cm²<A<200 cm²	x	x	x								x	x	x
Inadvertent open pressurizer safety valve	x	x	x								x	x	x
Medium primary system leak 200 cm²<A<500 cm²	x	x	x								x	x	x
Large primary system leak A>500 cm²	x	x	x								x	x	x
Inadvertent open P-bdVa due to maintenance fault		x	x	x						x	x	x	
Inadvertent open P-bdV on loss of off-site power	x	x	x								x	x	x
Inadvertent open P-bdV after turbine trip	x	x	x								x	x	x
Steam generator tube leak	x	x	x								x	x	x
Leak in residual heat removal system inside containment			x	x	x	x	x	x	x	x			
Leak in residual heat removal system in annulus			x	x	x	x	x	x	x	x			
Leak in volume control system	x	x	x	x	x	x	x	x	x	x	x	x	x
Leak in reactor cavity/setdown pool						x		x					
Leak into an affiliated system			x	x	x	x	x	x	x	x			

	Plant operating state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Leaks from system containing unborated water:													
— Steam generator tube leak			x	x	x	x	x	x	x	x	x		
— Leak in residual heat removal heat exchanger			x	x	x	x	x	x	x	x	x		
— Leak in bearing seal			x	x	x	x	x	x	x	x	x		
— Inadvertent primary system injection			x	x	x	x	x	x	x	x	x		
Inadvertent unborated water in residual heat removal system			x	x	x	x	x	x	x	x	x		
Boron dilution during decontamination work									x				
Boron dilution during level raising										x			
Borating fault on shutdown		x											
Inadvertent boron dilution on shutdown following loss of all main coolant pumps												x	

[a] P-bdV denotes pressurizer blow down valve.

EXAMPLES FOR SPECIFIC SYSTEM MODELLING REQUIREMENTS

III–7. Reference [III–8] has been the primary and almost exclusive source for the examples presented in paras III–8 to III–10.

III–8. Particular systems may require specific modelling for shutdown conditions. For example, fuel pool cooling systems might not be included in the analysis for power operation, but could be important during shutdown conditions. Certain operating states of the residual heat removal system may also be used only during outages and these therefore need to be considered. The system models have to reflect the operating states and specific system alignments. Success criteria, for example, *k* out of *n* trains of a particular system required, may be less stringent for shutdown conditions because of the lower decay heat level. Detailed thermohydraulic calculations need to be performed to determine these criteria. The automatic start features of a system may be bypassed during shutdown conditions in order to prevent an inadvertent start. For example, safety injection systems may be blocked with regard to automatic start mode to prevent actuation during shutdown. Thus, the control logic in the fault trees for these systems needs to be changed to reflect the fact that the systems will have to be manually initiated if required. Models for the related human interactions also need to be developed.

III–9. Manual recovery actions credited in the analysis for power operation might not be possible during the outage due to ongoing activities as part of the outage. For example, cross-connecting of low pressure systems may be an appropriate action during power operation. However, during an outage, the cross-connection may be locked closed, or a system train may be entirely disabled. Therefore, if actions of this type are included in the fault trees for power operation, they need to be modified for the shutdown evaluation. In summary, each fault tree from the PSA for power operation adapted to the PSA for shutdown states needs to be reviewed for each plant operating state to determine whether there are any features of that plant operating state that might have an impact on the logic of the fault tree structure.

III–10. The changing availabilities of the various systems during outage complicate the task of system modelling. Some systems or parts of systems might not be available during certain plant operating states. Also, the probability of component failure represented by a basic event may change. Most PSA software packages are based on a ‘fast cutset algorithm’, which generates and stores equations for minimal cutsets. An analysis of minimal cutsets can be carried out on several levels: a particular fault tree gate, an individual event tree sequence, or a particular consequence (every event tree sequence can be assigned one or more consequences, e.g. a plant damage state). An analysis case can specify a ‘boundary condition set’, which includes a list of value specifications or changes that need to be applied to the model. The boundary condition set can include true/false settings for logical switches, setting of probabilities for basic events and fault tree gates, setting of true/false states for basic events and fault tree gates and setting of values for parameters. This is very useful for performing analyses of the same basic model with different variations depending on the plant operating states. Of course, it is also possible to perform the analysis without using logical switches, but then for every boundary condition set, different individual fault tree models are added to the complete PSA model for shutdown states, which complicates the effort necessary for modelling and review if some changes have to be made because of the number of different fault tree models to be considered.

APPROACH TO IDENTIFYING PRE-INITIATOR HUMAN FAILURE EVENTS AND HUMAN INDUCED INITIATORS RELEVANT TO PSA FOR SHUTDOWN STATES

III–11. As a detailed analysis of all measures that could be taken by personnel during shutdown is simply not feasible, an efficient screening step of the pre-initiator actions is indispensable. The outcome of this step will be a list of actions indicating the actions for which a qualitative evaluation is sufficient, the actions for which an estimate needs to be done and the actions for which a detailed quantitative analysis is necessary. The approach described in paras III–12 to III–18 is outlined in Ref. [III–6].

III–12. The basis for the screening approach is a plant specific list of the main steps and tasks for a standard outage plan. Obviously, there is a close relationship between this list and the plant operating state selected for the PSA for shutdown states. For a boiling water reactor, it typically comprises 30 steps or tasks. In Ref. [III–6], the following list of main steps and tasks is displayed as an example:

— Implement power reduction;
— Start testing in relation to plant shutdown and isolation of systems;
— Disconnect generator from grid;
— Continue power reduction until start of residual heat removal;
— Open containment for fuel transfer;
— Open reactor pressure vessel;
— Install compensator for flooding the reactor cavity;
— Commence flooding;
— Undertake reactor pressure vessel activities;
— Remove steam dryer;
— Set plugs and plates;
— Work on redundant trains;
— Work on components and systems;
— Carry out sipping test;
— Change fuel elements;
— Remove and reinstall feedwater sparger;

— Remove plugs and plates;
— Install steam dryer;
— Empty flooded cavity;
— Remove compensator;
— Close reactor pressure vessel;
— Close containment;
— Conduct testing in relation to startup;
— Increase power;
— Synchronize generator connection to grid;
— Increase to power operation.

III–13. For the elements of this list, empirical evaluations, including, for example, plant walkdowns, of the working environment and the tasks are performed to identify potential human errors and consequences. The significance of each potential error is then judged. In determining possible consequences, it is distinguished between unavailabilities of components or system parts on the one hand and initiating events on the other.

III–14. In the first case, it is assessed how the failure can be detected, for which time interval unavailabilities or latent faults would result and for which initiating events these unavailabilities or latent faults would become evident. Finally, possible counter measures and consequences are described.

III–15. In the second case, the initiating event is classified (e.g. loss of coolant accident). Again, possible counter measures and consequences are described.

III–16. One important objective of such a screening analysis is to prepare, in a transparent and systematic way, a table comprising the entire screening results. Operating experience relevant to the potential errors or consequences is included.

III–17. If detailed analysis is deemed necessary, it can be performed using the approaches to human reliability analysis described in Section 5.

III–18. As an intermediate case, for groups of initiating events of similar nature (e.g. loss of coolant accidents with leak positions above the core), a rough estimate of the integral failure probability could be sufficient.

EXAMPLE OF AN OUTAGE RISK PROFILE AS AN OUTCOME OF A PSA FOR SHUTDOWN STATES FOR A BOILING WATER REACTOR PLANT

III–19. In Ref. [III–9], results of a PSA for shutdown states are presented for a boiling water reactor plant. Six plant operating states (“POS” in Figs III–2 and III–3) have been specified:

(1) Plant operating state 1: Power operation and startup with pressure from rated conditions (71 kg/cm^2) to 35 kg/cm^2 and thermal power not greater than 15%.
(2) Plant operating state 2: Startup and hot shutdown with pressure from 35 kg/cm^2 to 10 kg/cm^2.
(3) Plant operating state 3: Hot shutdown with pressure lower than 10 kg/cm^2 and temperature higher than 93ºC.
(4) Plant operating state 4: Cold shutdown with temperature lower than 93ºC until the vessel head is removed.

(5) Plant operating state 5: Refuelling with the vessel head removed and the water level raised to the steam lines.

(6) Plant operating state 6: Refuelling with the vessel head removed and the water level raised to the spent fuel pool and the refuelling transfer tube open.

III–20. In Fig. III–2, for plant operating states 1–4, the thermal power and the pressure in the primary circuit are displayed as a function of time. In Fig. III–3, for plant operating states 1–4, the risk profile is shown. Clearly, the risk in plant operating state 4 is the highest, compared with the risk in the other plant operating states. This example emphasizes the insights provided by a risk profile, thereby helping to allocate efforts for safety improvements.

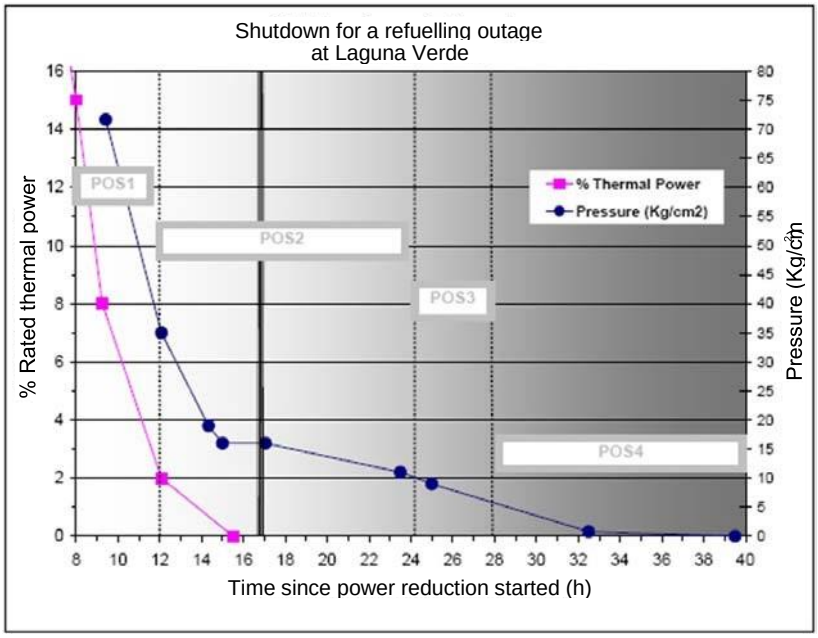

FIG. III–2. Plant operating states in PSA for shutdown states at Laguna Verde nuclear power plant. POS: plant operating state.

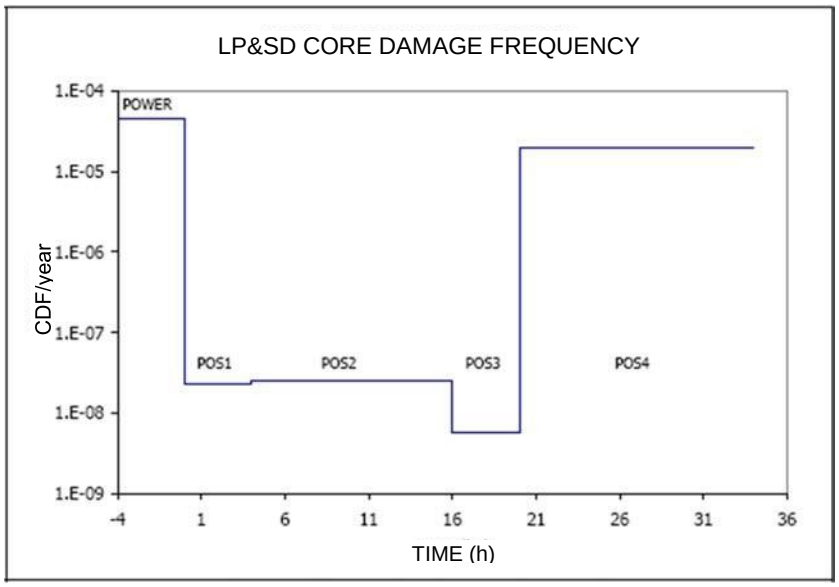

FIG. III–3. Comparison of core damage frequency per year for PSA for power operation and shutdown states. POS: plant operating state.

REFERENCES TO ANNEX III

[III–1] BABST, S., et al., Insights and results of the shutdown PSA for a German SWR 69 type reactor, Probabilistic Safety Assessment and Management (Proc. 8th Int. Conf. New Orleans, 2006), ASME, New York (2006).

[III–2] MÜLLER-ECKER, D., MAYER, G., GASSMANN, D., Probabilistic safety analysis for a modern 1300-MWE pressurized water reactor under low-power and shut-down conditions, Probabilistic Safety Assessment and Management (Proc. 6th Int. Conf. San Juan, Puerto Rico, 2002), Elsevier Science, Oxford (2002).

[III–3] COOPERATIVE PROBABILISTIC RISK ASSESSMENT PROGRAM (COOPRA), Cooperative Probabilistic Risk Analysis, Low Power Shutdown Working Group, Status Report, October 2001, Idaho National Engineering and Environmental Laboratory, Idaho Falls (2001).

[III–4] COOPERATIVE PROBABILISTIC RISK ASSESSMENT PROGRAM (COOPRA), Cooperative Probabilistic Risk Analysis, Low Power Shutdown Working Group, Initiating Events — Summary, July 2004, Idaho National Engineering and Environmental Laboratory, Idaho Falls (2004).

[III–5] BUNDESMINISTERIUM FÜR UMWELT, NATURSCHUTZ UND REAKTORSICHERHEIT, Bekanntmachung des Leitfadens zur Durchführung der "Sicherheitsüberprüfung gemäß §19a des Atomgesetzes — Leitfaden Probabilistische Sicherheitsanalyse" für Kernkraftwerke in der Bundesrepublik Deutschland vom 30. August 2005, Bundesanzeiger 207a (3 November 2005).

[III–6] FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-37/05, Bundesamt für Strahlenschutz, Salzgitter (2005).

[III–7] FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-38/05, Bundesamt für Strahlenschutz, Salzgitter (2005).

[III–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA-TECDOC-1144, IAEA, Vienna (2000).

[III–9] ESQUIVEL TORRES, J.L., LÓPEZ MORONES, R., Probabilistic safety assessment for low-power and shutdown states for LVNPP, Probabilistic Safety Assessment and Management (Proc. 8th Int. Conf. New Orleans, 2006), ASME, New York (2006).