12 April 2022

IAEA SAFETY STANDARDS

for protecting people and the environment

STATUS: Step 11

Review of the draft publication by the review Committees (NUSSC, NSGC)

Reviewed in NSOC (Wright/Asfaw)

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 on 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[1]:

> "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 to ensure the safety of a nuclear power plant in relation to potential initiating events that might be caused by random component failure or 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:

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016)

"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 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[2] and the corresponding core and/or fuel damage frequencies are estimated. Level 1 PSA provides insights into the strengths and weaknesses of systems, structures and components (SSCs) important to safety, and procedures in place or envisaged to prevent 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 evaluated, including a quantitative assessment of phenomena arising from severe damage to reactor fuel and/or to spent 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 frequency and other relevant characteristics of releases of radionuclides 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 radionuclides to the environment (e.g. a containment building). Further information is provided in IAEA Safety Standards Series No. SSG-4, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants [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 radioactive material to the environment.

1.5. Level 1 PSA, Level 2 PSA and Level 3 PSA are sequential analyses, with the results of each assessment usually serving 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 to accidents leading to major releases of radioactive material with potential consequences for human health and the environment. Level 2 PSA provides 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

[2] As sections 5–9 focus on the reactor core, the term 'core damage' is used in these sections unless fuel damage is being referred to specifically. Spent fuel pool specific considerations of core and fuel damage are provided in Sections 10 and 12, whereas considerations specific to multi-unit PSA are discussed in Section 11.

insights into weaknesses in confinement functions and measures for the mitigation and management of severe accidents, along with ways of improving them, as described in SSG-4 [4]. Level 3 PSA provides insights into the relative importance of accident prevention and mitigation measures, expressed in terms of 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], International Nuclear Safety Group 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 (Rev. 1) [3] in relation to performing or managing a Level 1 PSA project for a nuclear power plant and using it to support the plant's 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. This Safety Guide is not intended to pre-empt the use of equivalent new or alternative methods; rather, it is intended to encourage the use of any method that achieves the objectives of Level 1 PSA. 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 existing 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. The scope of a Level 1 PSA addressed in this Safety Guide includes all operating states of the plant (i.e. in power operation 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, floods, explosions, turbine missiles) and (c) external hazards, both natural (e.g. earthquake, external flooding, high

[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).

winds, other meteorological hazards) and human induced (e.g. aircraft crash, explosion pressure waves, accidents at nearby industrial facilities) as well as combinations of external hazards.

1.12. This Safety Guide focuses on the assessment of the nuclear power plant reactor core and the fuel in the core and in the spent fuel pools. An assessment of other sources of radioactive material on the site (e.g. in interim fuel storage facilities) is not in the scope of this Safety Guide; however, in the case of hazards that affect the whole site, any adverse effects that such facilities might have on the reactor(s) and spent fuel pool(s) are taken into consideration in the safety assessment and are therefore addressed in this Safety Guide. This Safety Guide also covers multi-unit aspects, which may be considered when developing a Level 1 multi-unit PSA to quantify multi-unit risk metrics.

1.13. The consideration of hazards arising from malicious acts is not within the scope of this Safety Guide.[4]

1.14. In performing Level 1 PSA, the most common practice is to perform the analysis for the various hazards and operating states in the integrated model, using a Level 1 PSA for power operation for internal initiating events as a basis. This Safety Guide presents information on various PSA types included in the integrated model.

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 various types of nuclear power plant.

STRUCTURE

1.16. Section 2 provides recommendations on general issues concerning the performance and use of the 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 performing the PSA with the nuclear power plant. Sections 5–8 provide recommendations on the methodology of a Level 1 PSA for power operation, including low power states, for various initiating events and hazards. Specifically, 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 specific aspects of Level 1 PSA for internal hazards and external hazards, respectively. Section 9 provides key recommendations on Level 1 PSA for shutdown states. Section 10 addresses the specifics of the development of a PSA for spent fuel pools. Section 11 provides recommendations on Level 1 multi-unit PSA aimed at quantifying 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 on the applications of a Level 1 PSA. The three annexes provide an example of a generic list of internal and external hazards, examples of a fire propagation event tree and a seismic event tree and supporting information on PSA for shutdown states.

[4] Nonetheless, a Level 1 PSA is considered as sensitive information and treated accordingly (see IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [11]).

2. GENERAL CONSIDERATIONS RELATING TO THE PERFORMANCE 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. Although 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. Requirement 1 of GSR Part 4 (Rev. 1) [3] states:

> **"A graded approach shall be used in determining the scope and level of detail of the safety assessment carried out at a particular stage for any particular facility or activity, consistent with the magnitude of the possible radiation risks arising from the facility or activity."**

While Requirement 14 of GSR Part 4 (Rev. 1) [3] states that **"The performance of a facility or activity in all operational states and, as necessary, in the post-operational phase shall be assessed in the safety analysis."**

The scope of the PSA to be undertaken should be correlated with the probabilistic safety goals or criteria if they have been specified in national regulations or guidelines. 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 (i) core damage frequency or fuel damage frequency, (ii) frequency of radioactive releases of various types or (iii) societal risks, and which might therefore necessitate the performance of a Level 1, Level 2 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 to verify 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 the Level 1 PSA should include consideration of fuel in the reactor core of a single unit, for which Recommendations on the development of a Level 1 PSA for the reactor core of a single unit are provided in Sections 5–9. The Level 1 PSA should also include consideration of fuel in the spent fuel pool, for which recommendations are provided in Section 10. It might further 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. Requirement 18 of GSR Part 4 (Rev. 1) [3] states that "**Any calculational methods and computer codes used in the safety analysis shall undergo verification and validation.**" PSA involves a number of analytical methods. These include the analysis of accident sequences and their associated systems, typically through the development of event tree and fault tree logic models along with methods for the solution of these logic models, the development of models of phenomena that could occur, for instance, within the containment of a nuclear power plant following core damage and/or fuel damage, and the development of models for the transport of radionuclides in the environment to determine their effects on health and the environment, 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. In accordance with para. 4.60 of GSR Part 4 (Rev. 1) [3], the computer codes that support these analytical methods should be adequate for the purpose and scope of the analysis, and the controlling physical and logical equations should be correctly programmed in the computer codes.

2.6. Requirement 21 of GSR Part 4 (Rev. 1) [3] states that "**The operating organization shall carry out an independent verification of the safety assessment before it is used by the operating organization or submitted to the regulatory body**." It is a widely accepted practice for the organization conducting a PSA to commission an independent peer review of the PSA by an external body, sometimes from a different State, to provide a degree of assurance that the scope, modelling and data are adequate (e.g. consistent with the scope of the document submitted to the regulatory body), 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. Requirement 24 of GSR Part 4 (Rev. 1) [3] states that "**The safety assessment shall be periodically reviewed and updated.**" In the operating lifetime of a nuclear power plant, modifications are often made to the SSC design 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, updated knowledge, new operating experience and more sophisticated methods and tools might be acquired, which might 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 for which it is intended.

2.8. Data should be collected throughout the lifetime of the nuclear power plant to check or update the analysis. These 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. Emerging data sets from other plants of the same type or of similar configuration, if available, should also be used for the improvement of the living PSA

2.9. The development of a living PSA should be encouraged in order to assist the decision making process in the normal operation of the plant. Many decisions, 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.

PROBABILISITC SAFETY GOALS OR CRITERIA

2.10. Requirement 4 of GSR Part 4 (Rev. 1) [3] states:

> "**The primary purposes of the safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body…have been fulfilled.**"

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 the performance of safety functions;
(b) The frequency of core damage[5] or fuel damage (Level 1 PSA);
(c) The frequency of a specific release (specified, e.g., in terms of its quantity, isotopes or timing) of radioactive material from the plant or the frequency of release of radioactive material as a function of its magnitude (Level 2 PSA);
(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. In the Member States, probabilistic reference values are typically identified either as criteria, targets, goals, objectives, guidelines or values for orientation. In addition, the

[5] Specific probabilistic safety goals or criteria need to be specified for core damage, as described in Section 5 of this Safety Guide. These safety goals or criteria may be different for different reactor designs.

numerical values for the levels of risk, which correspond to the threshold of tolerability and the design targets, differ from State to State.[6]

2.13. For the probability of failure of safety functions or systems, the probabilistic targets can be set at the level of the safety function or 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 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, proposed numerical values have been defined on a national level in some Member States to be used for existing and new nuclear power plants. The International Nuclear Safety Group has proposed the objectives for core damage frequency separately for existing plants and future plants (see Ref. [8])[7].

2.15. Core damage frequency and 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. Requirement 23 of GSR Part 4 (Rev. 1) [3] states:

> "**The results of the safety assessment shall be used to specify the programme for maintenance, surveillance and inspection; to specify the procedures to be put in place for all operational activities significant to safety, and for responding to anticipated operational occurrences and accidents; to specify the necessary competences for the staff involved in the facility or activity; and to make decisions in an integrated, risk informed approach.**"

2.17. 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 analysis and considerations of defence in depth.

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

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

[6] Available frameworks and examples for the definition of probabilistic safety criteria are provided in Ref. [12].

[7] 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 is 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.

2.19. 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.

2.20. The PSA should address the actual design or operation 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 the agreed modifications are completed, in order 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.

2.21. For a plant in the design stage, the results of the PSA should be used as part of the design process to assess the level of safety. The insights gained from the 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.

2.22. In addition, the results of the PSA should be compared with the reference values such as probabilistic safety goals or criteria if these have been specified in national regulations or guidelines. This should be done for all probabilistic goals or criteria defined for the plant, including those that address system reliability, core damage frequency and/or fuel damage frequency, frequency 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.

2.23. The PSA should aim to identify all accident sequences that contribute in a non-negligible way[8] to risk.[9] If the analysis does not address all significant contributions to risk (e.g. if it omits external hazards or shutdown states), then the conclusions drawn from the PSA about the level of risk from the plant, the balance of the safety features provided and the need for changes to be made to the design or operation to reduce risk might be biased. Such limitations should be acknowledged when using PSA to support decision making. The use of the full scope PSA model is therefore recommended.

2.24. The results of the PSA should be used to identify weaknesses in the design or operation of the plant. These weaknesses can be identified by considering the contributions to risk from groups of initiating events, the importance measures of the SSCs 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, such changes should be incorporated where reasonably achievable, taking the relative costs and benefits of any modifications into account (see Ref. [13]).

2.25. Section 12 provides detailed recommendations on specific applications of PSA for decision making by the regulatory body and by operating or design organizations.

[8] Contribution to risk could be deemed as negligible on the basis of the evaluated potential impact on the final results and the subsequent decision making process.

[9] This relates only to scenarios that are not triggered by security events such as malicious acts.

3. PROJECT MANAGEMENT AND ORGANIZATION FOR PSA

DEFINITION OF OBJECTIVES AND SCOPE OF THE PSA PROJECT

3.1. Determination of the objectives of the PSA together with its intended and potential uses is an important step to undertake before embarking on a PSA. The scope of the PSA is defined by the analysis level (i.e. Level 1, 2 or 3), the initiating events and hazards considered, and the operating states (i.e. in power operation or shutdown states[10]) addressed. The scope of the PSA should be compatible with both the objectives of the analysis and the available resources and information, such as the necessary procedures and methods, available personnel, expertise and 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 (e.g. the fuel in the spent fuel pool) might need to be analysed, depending on the formulation of the probabilistic safety goals.

3.2. The intended applications of PSA might have an impact the scope of the PSA, the modelling approaches and the level of detail. If this impact 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 to Level 2 or even Level 3 should also be envisaged if the PSA is to be used to support the 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 model should be 'symmetrical' in its modelling of initiating events.[11] More details on the PSA features necessary for its various applications are provided in Section 12.

PROJECT MANAGEMENT FOR PSA

3.3. Requirement 5 of GSR Part 4 (Rev. 1) [3] states:

> "**The first stage of carrying out the safety assessment shall be to ensure that the necessary resources, information, data, analytical tools as well as safety criteria are identified and are available.**"

3.4. Furthermore, Requirement 22 of GSR Part 4 (Rev. 1) [3] states that "**The processes by which the safety assessment is produced shall be planned, organized, applied, audited and reviewed.**".

3.5. Project management of the PSA depends strongly on the specific conditions in a State, namely:

(a) The organizations participating in the PSA project;

[10] PSA for low power and shutdown states is sometimes performed as part of the same, stand-alone study; however, it may be more practical to perform low power PSA as part of the PSA for power operation (that is how the states are being covered within this Safety Guide).

[11] A PSA model is considered symmetrical if it explicitly models initiating events in all locations in which they can occur, including all primary circuit loops, all trains of the credited systems, and all running and standby trains of normally operating systems (cf. para. 5.82). Non-symmetrical modelling of initiating events could create obstacles in obtaining a realistic risk profile through the risk monitor when introducing specific changes in the plant configuration.

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

After the objectives and 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.

3.6. 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 the above bodies or by consultants, research institutes, universities, technical support organizations, or a combination of these. The operating organization should always participate as a source of operational knowledge, as well as being a beneficiary from the insights obtained.[12]

3.7. It is desirable to start 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 at any stage 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.

3.8. 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.

3.9. 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

3.10. Appropriate working methods and procedures should be established at the outset of the project with a view to their minimal modification during the project. Unnecessary iterations in methods and procedures might cause delays in the PSA project. General guidance on 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

[12] Implementation of this recommendation could be challenging in the case of PSA performed at the design stage. If a generic PSA is being performed for a reference plant, the contribution of operating experience from the operating organization might be particularly beneficial.

be interfaced with the tasks of quality assurance and training to produce a detailed plan of the tasks, including a schedule for the project.

3.11. The resources needed to complete a PSA, including the expertise of the specialists involved, human resources, computer time and calendar time, depend greatly on the scope of the PSA, which is in turn governed by the overall objectives, and on the expertise already available in the PSA team. Activities should be scheduled in accordance with the detailed procedures established and taking into account the availability of personnel.

TEAM SELECTION AND ORGANIZATION

3.12. The members of the team performing the PSA can be characterized by the organization they represent (if different organizations are involved) and the technical expertise they provide. Once the necessary personnel have been selected, lines of communication should be established and specific tasks should be assigned. The necessary training should be determined, in accordance with the activities of the PSA, and subsequently organized. The formation and training of the team is closely associated with the quality assurance tasks addressed in paras 3.15–3.16.

3.13. The expertise necessary to conduct a PSA should comprise two essential elements: knowledge of PSA techniques and knowledge of the plant. This expertise can vary in depth, depending on the scope of the PSA, but the participation of the plant designer and/or the operating organization of the plant should be foreseen. More specifically, expertise relating to knowledge of the plant should come from persons with extensive familiarity with the design and operation of the plant in operating states and accident conditions.

3.14. A team performing a PSA for the first time should be provided with training to acquire the expertise necessary to complete the analysis successfully.

ESTABLISHING A QUALITY ASSURANCE PROGRAMME FOR PSA

3.15. A quality assurance[13] programme for 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 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.

3.16. Quality assurance of the PSA should be viewed and established as an integral part of the PSA project, and 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 technical work, quality assurance procedures are aimed at ensuring consistency among goals, scope, methods and assumptions, as well as accuracy in the application of methods and in calculations. Quality assurance procedures should include

[13] In other IAEA safety standards, including IAEA Safety Standards Series No. GSR Part 2, Leadership and Management for Safety [14], the term ‘management system’ is used. The term ‘quality assurance’ is used in this Safety Guide, however, to reflect widely accepted current practices and terminology used in the area of PSA.

control of PSA documentation of the PSA and of the different versions of the PSA models. General requirements for control of documents are established in GSR Part 2 [14].

GENERAL ASPECTS OF PSA DOCUMENTATION

Objectives and content of PSA documentation

3.17. Requirement 20 of GSR Part 4 (Rev. 1) [3] states that "**The results and findings of the safety assessment shall be documented.**" The primary objectives of PSA documentation should be to meet the needs of its users and to be suitable for the specific applications of the PSA. Possible users of the PSA include:

(a) Operating organizations of nuclear power plants (i.e. management, engineering, operations and maintenance 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 primarily use the summary report of the PSA, while others might use the full PSA documentation, including the computer model.

3.18. PSA documentation includes work files, computer inputs and outputs with explanations, correspondence, interim reports and the final report of the PSA. The PSA documentation should be complete, well structured, clear and easy to follow, including for its review and update. The documentation should be presented in a traceable and sequential manner, i.e. the order of appearance of analyses in the final documentation should follow, as far as possible, the order in which they were actually performed. Explicit presentation of the assumptions, exclusions and limitations for extending and interpreting the PSA is also of critical importance to users.

3.19. The documentation should provide within the report (or by reference to available material) all the information needed 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

3.20. 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.

3.21. 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 before consulting the main report.

3.22. The summary report of a PSA should include a subsection on the structure of the main report, with a very brief indication of the contents of the sections of the main report and appendices. The relation between various parts of the PSA should also be included in this subsection of the summary report.

3.23. 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, as well as recommendations. 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.

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

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

4. FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION

4.1. In preparation for a Level 1 PSA, the PSA team members 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) 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 needed, 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, the PSA documentation may refer to the corresponding sections of the safety analysis report, e.g. descriptions of systems. All information should be clearly referenced so that it 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 as a result of the hazard. Specific guidance for plant familiarization in relation to 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 (Rev. 1) [3] when performing a Level 1 PSA for internal initiating events. In particular, it provides recommendations on the technical issues that need to be addressed in performing a Level 1 PSA for internal initiating events caused by random component failures and human errors during 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 Level 1 PSA. The overall approach and methodology should provide for the modelling of fault sequences that could occur, starting from an initiating event, and for the identification of combinations of SSC failures and human errors that could lead to core damage.

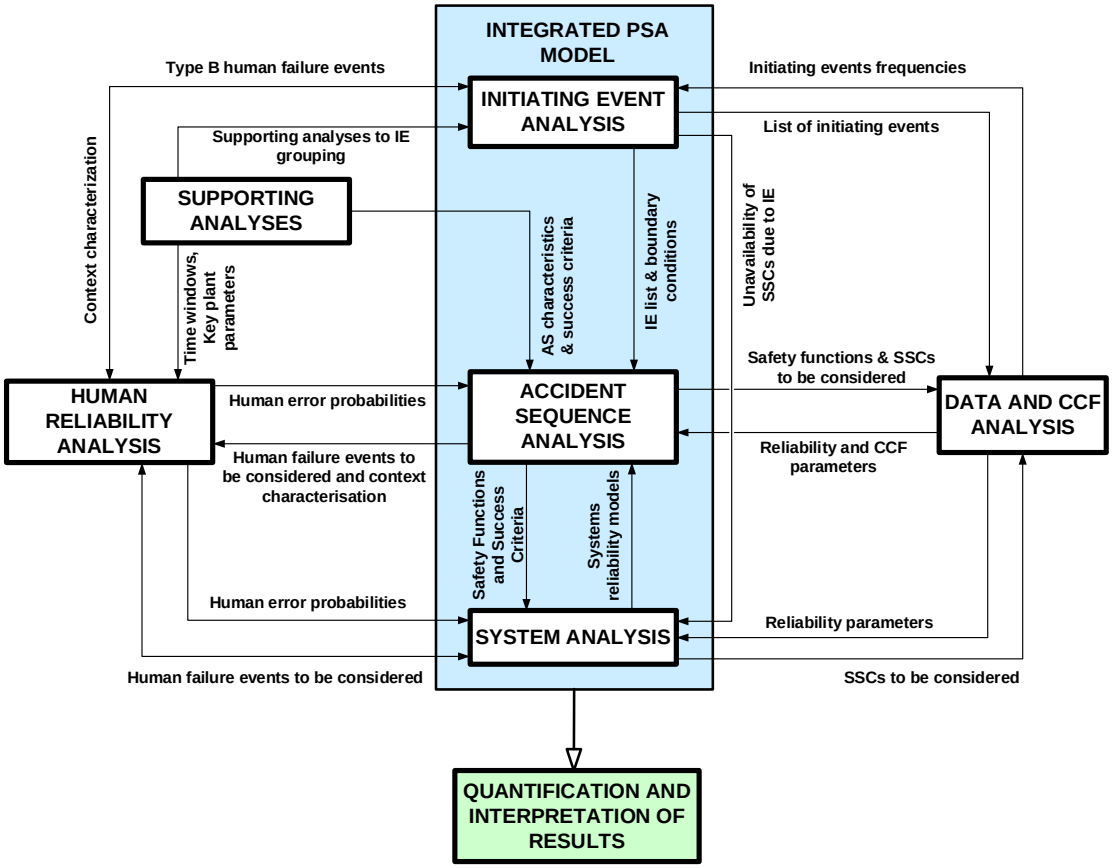

FIG. 1. General analysis framework of a Level 1 PSA for internal initiating events. IE: initiating event; AS: accident sequence; CCF: common cause failure

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 conducting 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 credited systems[14], lead either to a successful outcome, to 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 credited systems to carry out their safety functions. The dependencies (between different credited systems or between a credited system and initiating event) are modelled in the fault trees and in the event trees.

5.5. Another approach taken is to perform the analysis using large event trees and small fault trees. In this approach, the failures of safety functions, 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 perform the analysis using event trees only or fault trees only. However,

[14] 'Credited systems' are systems credited in the PSA, which include operating and standby safety systems and non-safety systems whose operation during an accident can help prevent an undesired end state (e.g. core damage, fuel damage).

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. The use of a conservative approach should be justified. Where a best estimate of the NPP's response to an initiator is not available, one or more of the following sources might be used: a) bounding deterministic analysis; b) design analysis; c) commissioning tests; d) operational tests; and e) expert judgment.

5.7. For plants with multiple units, the interactions between the units (both positive and negative, from a risk point of view) should be considered in Level 1 PSA from the perspective of the unit under consideration. Recommendations on multi-unit PSA developed to quantify multi-unit risk metrics are provided in Section 11.[15]

5.8. It should be possible to use the Level 1 PSA model for the intended applications and to update it 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 determining the minimal cutsets by Boolean logic reduction.
(c) It should be capable of quantifying the PSA model in a reasonably short time frame.
(d) 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 development of a Level 1 PSA model is an iterative process and it should be continued 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 challenges normal operation, and which necessitates successful mitigation 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, initiating events that could arise

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

in the spent fuel pool in Section 10 and initiating events that could arise in relation to multi-unit PSA in Section 11.

Identification of initiating events

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

(a) Review of the deterministic design basis accident analysis and design extension conditions analysis and the safety analysis report;
(b) Identification of initiating events on the basis of the analysis of operating experience from the plant being analysed and from similar plants;
(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) Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for plant SSCs to determine whether their failures, either partial or complete, could lead to an initiating event;
(e) 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;

5.14. The set of internal initiating events used as the basis for Level 1 PSA should be as comprehensive as possible. The use of a sufficiently comprehensive combination of the approaches listed in para. 5.13, bolsters confidence that the set of initiating events identified for the plant is as complete 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 for which there is little or no operating experience, where special efforts should be made to identify unique initiating events, failure modes, accident sequences and dependencies that are particular to that design. The analytical methods indicated in para. 5.13(d) should be carried out for all the operating systems and standby systems to identify possible initiating events (or consequential failures that might 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 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 of 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 (e.g. reduction of feed to steam generators or loss of feed to one steam generator) as well as complete failures (e.g. complete loss of feed to all steam generators). This is important because initiating events involving partial failures could still make a significant contribution to the risk.

5.18. The set of initiating events identified should include those that can occur during all 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 might 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 might 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 conducted to ensure that any initiating events that have actually occurred are included in the set of initiating events addressed in the Level 1 PSA. The causes of such initiating events should be identified and taken into account in the analysis.

Transients

5.23. The Level 1 PSA should be based on a comprehensive set of transients that could occur. In terms of principal effects on potential degradation of fundamental safety functions, transients are categorized into the following categories:

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

5.24. 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 frequency of occurrence and duration, and should take into account the likelihood of recovery of off-site power. This information should be based on details of the design and operating experience in relation to the grid connections to the plant.

5.25. When loss of off-site power that could occur as a result of internal hazards (such as a fire in the plant) and external hazards (such as extreme environmental conditions or an earthquake) is 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.

5.26. Particular attention should be paid to loss of off-site power event when it is followed by loss of all on-site AC power in the event sequence, since PSA studies have shown that this situation (known as station blackout) has made a significant contribution to risk for a number of plants.

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 an initiating event and the support system also provides a safety function after the initiating event.

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 of breaks should be identified on the basis of the actual design and layout of the plant. The set of loss of coolant accidents should also include failures of pipework and valves, in particular, relief valves.

5.30. Loss of coolant accidents that can result in the discharge of primary coolant outside the containment should be identified. These typically include steam generator tube ruptures and loss of coolant accidents in interfacing systems where the primary coolant leakage from the break bypasses the containment and is therefore 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 SSCs that need 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 response needed from the coolant injection systems to mitigate the loss of coolant accident. Depending on the plant design, a different set of equipment may be needed 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 keep the analysis needed for Level 1 PSA to a manageable size, the initiating events should be grouped before proceeding to the accident sequence analysis.

5.33. If, in order to reduce the size of the PSA model further, the initiating event groups are screened and some are excluded from the model, the screening criteria should be consistent with the purpose of 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 credited systems;
(c) The effect of the initiating event on the availability and operation of 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 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 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. This aspect may be particularly important for applications for which Level 2 PSA is not available, as the consequences are greater.

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 by plant operating personnel to each group of initiating events that necessitates the operation of 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 removing 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 SSCs and human actions taken in carrying out the safety functions needed for the groups of initiating events. The end states of the accident sequence models will correspond either to a safe stable state where all necessary safety functions have been successfully fulfilled or to core damage. Criteria should be developed on what constitutes a safe stable state.[16]

Core damage

5.42. A criterion (or criteria, if appropriate) should be developed on what constitutes core damage or a particular degree of core damage.[17] For example, for light water reactors, it is often

[16] Several safe stable states can be specified (e.g. hot standby, cold shutdown).
[17] Several core damage states can be specified if there are varying degrees of damage. For example, in channel type reactors, damage to different channels is usually considered depending on the severity of the consequences. (for CANDU and RBMK type reactors severe core damage 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 one of the fuel parameters (such as the cladding temperature) exceeds its design basis limit or a higher limit if this can be justified.. In addition, criteria for other undesired consequences may also be assigned, such as reactor vessel cold overpressure, reactivity transient or boiling in the spent fuel pool.

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 uncovering of the core or if a maximum specified cladding temperature is exceeded. If a significantly long time interval is needed to cause core damage after the uncovering of the core, this should be taken into account in framing a realistic definition of core damage.

Safety functions 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, accident sequence analysis should be pursued over a time period that will enable the effect of long term measures to be analysed. This will ensure that the risk estimate beyond the sequence mission time is negligible (as compared to the risk during the mission) 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 needed will depend on the reactor type and the nature of the initiating event and will typically include:

(a) Shutdown of the reactor and maintaining subcriticality;
(b) Heat removal from the reactor core;
(c) Maintaining the integrity of the primary circuit.

5.47. The credited systems and actions by operating personnel that will be needed to perform each of these safety functions should be identified, along with the associated success criteria.

5.48. The actions by operating personnel that will be necessary to bring the plant to a safe, stable state should be identified on the basis of an analysis of plant procedures. It is good practice to identify these actions collaboratively among plant operating personnel, systems analysts and human reliability analysts.

5.49. The success criterion should define the minimum level of performance for each credited system (including systems with supporting functions such as the service water system and power supply systems) necessary to fulfil the safety function, taking into account the specific features of each sequence. Where redundant trains of the credited system are involved, the success criteria should be defined as the number of trains that are needed to remain operable. Where multiple credited systems are involved, the success criteria should take into account the performance needed from each of the different systems. This could include partial operation of each of the systems as supported by the safety analysis with sufficient details to provide an 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 first moment when the action will not lead to fulfilment of the safety function (taking into account the time needed for diagnosis and for the action to be taken).

5.51. Systems and components that are credited for the mitigation of an initiating event but which would fail as a result of the initiating event should be identified and taken into account in specifying the success criteria. Examples of such cases are where the initiating event involves the failure of a support system such as the electrical power or cooling water system, or where the initiating event produces a harsh environment in an area where the equipment credited for mitigation of the event is located. Either of these cases might lead to failure of the necessary systems. In the case of a large or intermediate loss of coolant accident in a pressurized water reactor, if the break occurs in any leg connected to the reactor, the flow from the trains of the emergency core cooling system connected to that leg will be lost.

5.52. The success criteria should specify the mission times for the credited systemsIn many cases, this has been taken to be 24 or 48 hours for most initiating events. The mission time should be defined adequately for capturing possible cliff edge effects and ensuring that the residual risk accrued after the mission time is negligible.

5.53. The Level 1 PSA documentation should include a list of the safety functions, credited systems and actions by operating personnel that are necessary for each initiating event to bring the reactor to a safe state, along with the associated success criteria.

Analysis to support the specification of success criteria

5.54. The success criteria for the credited systems 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 plant specific data wherever possible and should conform to the best practice for using qualified and valid computer codes.

5.55. Wherever possible, realistic success criteria that are based on best estimate supporting analysis should be defined and used in the Level 1 PSA: see IAEA Safety Standards Series No. SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [5].

5.56. 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 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.

5.57. In accordance with Requirement 18 of GSR Part 4 (Rev. 1) [3], 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 only by qualified code users. Best estimate input data and assumptions that avoid unnecessary conservatisms should be used wherever possible: see SSG-2 (Rev. 1) [5].

Modelling of accident sequences

5.58. 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 credited systems, support systems and human actions in performing the safety functions. It is considered good practice to draw detailed event sequence diagrams, including human interactions, before constructing the event tree.

5.59. The event tree for the initiating event group should address all the safety functions that need to be performed and the credited systems that need to be operated as specified by the success criteria. The status of the front line credited systems (i.e. success or failure) for the initiating event group usually forms the headings for a particular event tree. The headings may also include any actions by operating personnel that directly affect the course of an accident, in particular 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.

5.60. 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. However, the headings can sometimes be ordered in another way to simplify treatment of dependencies or to reduce model size.

5.61. The event tree structure should take into account functional and physical dependencies (see para. 5.89) that might occur as a result of the initiating event, equipment failures or human errors.

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

End states of accident sequences and plant damage states

5.63. 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 (or other undesired consequences) do 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 for 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 to specify the plant damage states as part of the Level 1 PSA than to postpone the specification of plant damage states to the first step of the Level 2 PSA.

5.64. 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 defined collaboratively between the Level 1 PSA analysts and the Level 2 PSA analysts.[18]

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

(a) The type of initiating event that has occurred (intact primary circuit or loss of coolant accident);

[18] The combination of Level 1 end states involving severe core damage and failures of containment subsystems may be generated by means of interface event trees: see SSG-4 [4]

(b) Failures of the credited 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 owing 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 for a PSA in power operation. Additional characteristics applicable to shutdown states are provided in Section 9 (see para. 9.34).

5.66. 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 with the possible availability of the credited systems that could prevent or mitigate a release of radioactive material.

5.67. The Level 1 PSA documentation should present the event trees that have been drawn to determine how the accident sequences progress. A description of the logic behind the event tree structure should be given to aid understanding, since the event tree diagram itself provides no reasoning, only the results of reasoning. Explanatory information on the event tree headings should also be provided, for example, whether the heading represents a simple function or 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.

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

SYSTEMS ANALYSIS

5.69. The next step in the analysis is to model the credited 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 credited 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 or 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.

5.70. 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.[19]

Fault tree analysis

5.71. Where fault trees are used, they should be developed at a level of detail sufficient to capture the possible dependencies and to provide a complete logical failure model for all the credited system failure states identified by the event tree analysis.

5.72. The failure criterion that provides the top event of the fault tree for each safety function should be the logical inverse of the accident sequence success criterion, as specified in paras 5.49–5.57. In some cases, more than one fault tree model may be necessary for the same 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.

5.73. 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.

5.74. 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 detail of the analysis is generally left to the discretion of the analysts, but it should be sufficient to capture the possible dependencies and it should be consistent with the available data on component failures and the proposed applications of the Level 1 PSA.

5.75. The set of basic events to be modelled in the fault trees should be identified by means of systematic analysis (e.g. 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.

5.76. The fault tree model should include all the credited system components that need to be operational, including support system components. It should also include passive components whose failure could affect the operation of the system, for example, filter blockages and pipe leaks. The fault tree model should be developed in a way that ensures that dependencies are taken into account explicitly. Omitting the explicit modelling of these dependencies might significantly bias the results and lead to an underestimation of the relative importance of the support systems. Passive components (e.g. pipelines, cables) may be excluded from the PSA model if their reliability is shown to be an order of magnitude higher than the reliability of any component considered in the model whose failure would have the same consequences.

[19] 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).

5.77. 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 (e.g. reliability data might be available for a pump as a whole, but not for its constituent parts, such as the rotating wheel, coupling and bearing). In addition, in defining the degree of resolution of the components in the fault tree, consideration should be given to insights from the PSA in terms of the risk significance of plant equipment or of individual parts of equipment.

5.78. 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 have 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.

5.79. The fault tree models should take account of individual components or trains of equipment in the credited systems that might 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.

5.80. The unavailability of systems owing to testing and maintenance should be modelled in a way that is consistent with plant technical specifications[20] and with testing and maintenance practices in the plant.

5.81. 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.

5.82. 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 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. 5.171 for examples of importance measures).

Required systems information

5.83. Functional descriptions should be produced for each of the systems credited 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;

[20] 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.

(d) The interfaces with other systems;
(e) The operating state being modelled (for systems with more than one state);
(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.

5.84. 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 configurations of the components during normal operation;
(c) The pipe segments or wiring segments connecting the components;
(d) The support system interfaces (e.g. power, instrumentation and control, cooling, ventilation).

5.85. The functional descriptions and schematics provided for the credited 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

5.86. 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.

5.87. 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 owing to shared components, common actuation systems, common isolation requirements or common support systems (e.g. power, instrumentation and control, cooling, ventilation).
(b) Physical dependencies (also referred to as spatial interaction dependencies) owing to an initiating event that can cause failure of credited system equipment. This can occur as a result of pipe whip, missile impact, jet impingement or environmental effects.
(c) Human interaction dependencies owing 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 credited system equipment so that they do not operate when needed following an initiating event.
(d) Component failure dependencies owing to similarities in design, manufacturing or installation errors or errors made by plant personnel during plant operation. These are addressed by a common cause failure analysis (see paras 5.92–5.95).

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

5.89. All functional and physical dependencies should be modelled explicitly. Human interaction dependencies and component failure dependencies should also be modelled; these are discussed further in paras 5.96–5.121 on human reliability analysis and paras 5.92–5.95 on common cause failure analysis.

5.90. All the functional dependencies that could arise within systems should be taken into account 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.

5.91. The intersystem functional dependencies that could arise owing 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 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

5.92. 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, whenever possible, by the collection of data. Addressing both intrasystem and intersystem common cause failure events is considered good practice.

5.93. 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 failure modes. Any assumptions made concerning the defences against common cause failures should be stated in the Level 1 PSA documentation.

5.94. 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 justification should take into account 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.

5.95. Where possible, the common cause failure probabilities should be based on plant specific data and should take into account 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 uncertainty parameters assigned and should be commensurate with the uncertainty in the process of specifying the common cause failure parameters. An example of when only generic data might be available is the PSA at the design stage of a new nuclear power plant.

5.96. The human errors that can contribute to the failure of safety functions or the failure of credited systems should be identified and included in the logic model. A structured and systematic approach should be adopted for the identification of human failure events, 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 contribution made by all types of human failure event to the core damage frequency. A useful starting point is to check the selected approach against one of the approaches generally used to ensure that all the necessary steps for human reliability analysis are taken.

5.97. The recommendations provided in paras 5.99–5.121 relate to the most common methods used for human reliability analysis in a Level 1 PSA (see Ref. [15]). The process for human reliability analysis should consist of the following four iterative steps:

(1) Identification and definition of human failure events to be considered in the PSA;
(2) Qualitative assessment of human failure events;
(3) Quantitative assessment of human failure events;
(4) Integration into PSA model.

5.98. 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.

5.99. The aim of quantitative assessment in human reliability analysis should be to generate probabilities of human errors that are consistent with one another in all the parts of the Level 1 PSA.

5.100. The human reliability analysis should be performed 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 in operating states and accident conditions. If this is not possible (e.g. 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

5.101. A structured and systematic procedure should be applied for the identification and definition of all types of human failure events to be included in the Level 1 PSA.

5.102. 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 (type A human failure events). These events can occur during repair, maintenance, testing, inspection or calibration tasks. If the events remain undetected, the component or component groups affected will be unavailable when needed after an initiating event. Of particular importance are failure events that have the potential to result in the

simultaneous unavailability of multiple trains of credited systems. These sources of unavailability are included in the models at component, train or system level.

5.103. A systematic review of plant procedures should be performed to identify human failure events that might occur during the repair, maintenance, testing, inspection and calibration tasks undertaken by operating personnel for the systems modelled in the Level 1 PSA (type A human failure events). The review should determine the potential for such events to occur and the effect of these potential events on the unavailability or failure of credited system equipment.

5.104. A systematic review of plant procedures should be performed to determine potential human failure events that could lead to an initiating event (type B human failure events). At a minimum, it should be checked that these types of human failure event have been taken into account in the evaluation of frequencies of initiating events used in the analysis.

5.105. A systematic review of plant procedures should be performed to identify the human failure events that might occur during critical actions taken by operating personnel after the occurrence of an initiating event (type C human failure events). The review should determine the potential for human failure events to occur and the effect of these potential errors on the unavailability or failure of a component, system or safety function. type C human failure events usually make a significant contribution to the core damage frequency.

5.106. Significant errors of commission (i.e. incorrectly performing a necessary task or action or performing an extraneous task that is not necessary and might exacerbate the accident progression or cause an initiating event) should be taken into consideration. As a result, additional accident sequences might be created. While it is not yet general practice to include errors of commission in the base case PSA, it is considered good practice to use information on the general causes of errors of commission to reduce their potential (see, e.g., Ref. [15]).

5.107. Repair actions (e.g. the replacement of a motor on a valve so that it can be operated) should be credited in the PSA only if there is strong justification for their feasibility. Human reliability analysis techniques cannot always be 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) the failure can be diagnosed quickly, (ii) the spare parts and repairing personnel are in place, (iii) the environmental and work conditions needed for performing repair are in place or can be ensured, and (iv) the time window is sufficiently long to credibly assume the possibility for repair, including the time needed to bring spare parts and repair personnel to the plant. Recovery is defined in the PSA context as the 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, whereas repair cannot. The appropriateness of the recovery and repair actions should be documented.

5.108. Actions that might be considered ‘heroic’ (e.g. operating personnel entering an environment with extremely high radiation levels to perform the action) or actions that are performed without any procedural guidance or training should not be included or credited in the analysis as normal practice, though exceptions may be made, with justification.

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

Qualitative assessment of human failure events

5.110. The qualitative assessment of human failure events should include the collection, analysis and documentation of information that is relevant for analysts to understand the personnel tasks involved in the human failure events undergoing human reliability analysis.

5.111. Information should be collected from the following sources, as applicable:

(a) Procedural guidance;
(b) Visits to relevant plant locations;
(c) Reviews of operating experience;
(d) Interviews, talk-throughs, and walk-throughs with operating personnel and trainers;
(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.

5.112. Qualitative assessment should lead to a characterization of human failure events so that quantification and modelling can be performed adequately. This characterization is usually achieved through the following main activities:

(a) Task analysis to gain a detailed understanding of the activities required to meet the success criteria associated with human failure events;
(b) Context characterization to characterize the scenario and the performance conditions defining the personnel activities covered by the human failure events, e.g. timing constraints, procedural guidance, relevant cues;
(c) Error identification to identify the cognitive and manual activities that would result in human failure events;
(d) Error characterization 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 human failure event (A, B and C) and for all areas of PSA (see Ref. [15]).

5.113. For newly designed nuclear power plants many of the sources of qualitative information listed in para. 5.112 might not be available. In such cases, the information for similar plants should be used. If this is not possible, then expert judgement should be used for the activities listed above. In any case, the correspondence of qualitative information to the actual plant status should later be verified and the PSA should be updated, as necessary.

Quantitative assessment of human failure events

5.114. 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. Other relevant factors should also

be considered, as appropriate. These factors (often referred to as 'performance shaping factors') should be identified by the qualitative assessment.[21]

5.115. The method used to derive the human error probabilities should be consistent with the methods generally used in PSAs or its use should be explicitly justified.

5.116. While different quantification methods may be applied for different types of human failure event (i.e. for type A, B and C events), the use of the same human reliability analysis approach (the human reliability analysis method or a combination of methods) should be used for the assessment of similar types of human failure event to ensure consistency in the analysis. If different approaches are used for the same type of human failure event the reasons for their selection should be documented.

5.117. The risk importance of human failure events should be evaluated to identify events that should be subject to more detailed analysis. The quantification of human failure events is often performed in two stages:

(1) Screening assessment applying a simple quantification model;

(2) Detailed assessment where more factors are taken into account and the context is characterized in more detail, in particular for the most risk significant actions by operating personnel.

In this approach, it should be ensured that the risk importance of human failure events are accurately characterized after the screening stage so that the risk significant human failure events needing more detailed assessment can be identified.

5.118. The assessment of type C human failure events for internal and external hazards should include the following:

(a) Human failure events that are included in the Level 1 PSA for internal initiating events but are also relevant to the scenarios induced by internal or external hazards. In such cases, it might be necessary to revise the assessment of performance shaping factors as it might be more difficult for operating personnel to implement actions than in the base case scenario (e.g. owing to a higher stress level associated with the hazard context).
(b) Human failure events that are relevant only to a specific hazard (e.g. firefighting using portable fire extinguishing devices). The methods used to assess hazard specific human failure events can usually follow the same principles as the ones used to analyse other types of human failure event.
(c) Undesired responses by operating personnel to spurious alarms and indications. More information on identification and assessment of undesired actions by operating personnel can be found in Ref. [16].

Treatment of dependencies between human failure events

5.119. Analysis of dependent human failure events should be embedded into the overall human reliability analysis process (identification, qualitative assessment, quantitative assessment, integration of human failure events into the PSA model). There are likely to be

[21] 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.

interdependencies between the individual human failure events included in the logic model. Such interdependencies could arise from the use of a common cue or procedural step, cognitive coupling owing to the structure or content of plant procedures, drivers of diagnosis and response planning, or similarities in conditions for taking 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.

5.120. All minimal cutsets or scenarios involving multiple human failure events should be identified.[22] The set of human failure events 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 human failure events in the PSA model

5.121. Human failure events should be incorporated as basic events into the logic model. Depending on the definition and effect of a human failure event, the corresponding basic event can appear at an appropriate level in the system fault trees or it can represent an event tree heading. Recovery type human failure events may also be implemented during the post-processing phase of quantification. The integration step should include a thorough examination of the minimal cutsets to verify that human failure events have been incorporated correctly. This examination should include a step to identify combinations of human failure events which may need a dependency assessment (see paras 5.119–5.120).

OTHER MODELLING ISSUES

Passive systems

5.122. A functional reliability assessment of passive systems to satisfactorily perform their safety functions (i.e. assessment of their failure probability) should be considered in the PSA. This section relates to passive systems incorporating moving fluids or expanding solid structures, direct action devices and stored energy sources (i.e. passive systems of categories B, C and D, as defined in Ref. [17]). The demonstration of the functionality (including the reliability and availability) of passive systems generally involves the use of one or more techniques such as thermohydraulic calculations, validation, expert judgement, testing and performance monitoring to demonstrate their reliability.

5.123. The 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 are distinguished from one another by whether their engineered SSCs rely on external mechanical and/or electrical power, signals or forces. In a passive system, the absence of reliance on an external input means that the reliance is instead placed on natural laws, properties of materials, internally stored energy or capacity and environmental conditions. Potential causes of failure of active systems, such as lack of human action or power failure, may be eliminated when passive safety is employed. It is necessary to understand not only the individual processes involved but also how they may be

[22] This can be done 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.

combined with one another. These processes and their combinations, which define the actual performance of the system, may vary depending on changes in the conditions of state, boundary conditions and failure or malfunctioning of components within the system.

5.124. As passive safety systems (especially thermohydraulic systems) generally rely on smaller driving forces than active safety systems, they are more sensitive to environmental and boundary conditions. The reliability assessment of passive systems should therefore cover failure mechanisms and events potentially affecting the environmental and other boundary conditions, such as the conditions that influence natural phenomena to effectively mitigate accident conditions and mechanical or structural degradation (including ageing effects) that are unique to passive systems. For example, natural circulation might 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; potential imperfections of the passive system components (e.g. undesired inclination of pipes owing to improper construction) might also degrade the performance of certain passive systems owing to the low magnitude of driving forces.

5.125. The reliability assessment of passive systems should also take into consideration periodic testing and maintenance practices or planned procedures, since such practices or procedures might have a significant influence on the reliability of passive systems. For instance, feedback from periodic testing and maintenance, if it exists, might reveal age-related material degradations or might demonstrate a need to modify the testing or maintenance strategies.

5.126. The general approach for the reliability analysis of passive components and systems should be similar to the approach for other systems considered in the PSA. Specific emphasis should be placed on gaining confidence that the system failure modes relevant to PSA have been defined properly and that the associated failure probabilities have been assessed in a justifiable manner. Therefore, to assess the reliability of a passive system, a model based approach might need to be developed (see Ref. [18]) and/or other techniques such as testing and expert judgement might need to be used.

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

(a) System characterization to define the mission of the system, associated accident scenarios, failure modes and success or failure criteria;
(b) Identification of system failure mechanisms;
(c) System modelling to enable consideration of system performance in various conditions;
(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.

5.128. Common cause failure is one of the most important failure modes of passive systems that should also be considered. Typically, for type C and D passive systems, the common cause failure of moving parts or instrumentation and control components is assessed using a standard technique for similar components in redundant trains. However, for type B passive systems, the causes of system failure might be the same for all system trains. This

should be reflected in the passive system model if the dependent failure of redundant trains might have the same or close to the same probability as for any single train.

Software based systems

5.129. The reliability assessment of software based systems that are considered to be SSCs credited to ensure safety functions or that can cause initiating events should be considered in the PSA. In this context, software based systems are assumed to include various instrumentation and control equipment with programmable modules.

5.130. A graded approach should be used to determine the scope and the method used for the reliability assessment of software based systems, on the basis of the risk significance of the systems from a PSA point of view. For instance, a computer based system used to control the reactor protection system, reactor control systems or other risk significant systems would be expected to need a more detailed analysis than the programmable components of lower risk significant instrumentation and control systems. Simplified approaches for assessing the reliability of software based systems could be adopted for modelling, taking into consideration the architecture and the safety classification of the systems.

5.131. The reliability assessment of operator interface systems should take into consideration other instrumentation and control system failure dependencies through normal PSA fault tree and event tree modelling, in which the failures of systems credited earlier in an accident sequence are routinely cascaded. The operator and correlated operator interface system interdependencies between different instrumentation and control systems should be considered. For those programmable operator interface systems that are modelled in a simplified manner, justification should be provided for the limitations in the analysis.

5.132. The reliability assessment of software based systems should cover both hardware and software components as well as configuration data for the programmable logic devices of those systems. Modelling the reliability of software based systems is a challenge because the standard statistical approaches have limited applicability for the software modules.

5.133. As for any systems analysis, the first task for the reliability assessment of a digital 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, could have adverse effects on a safety function. In addition, the interactions between the instrumentation and control systems should be analysed to define system dependencies for the system tasks under consideration.

5.134. The analysis of a software based system should be sufficiently detailed to capture the functionally relevant failure modes of the system and to capture the dependencies between systems. Both the failure modes ‘failure to actuate certain instrumentation and control function’ and ‘spurious actuation’ should be considered. The level of detail needed depends on the instrumentation and control architecture and the system’s fault tolerant features; a detailed functional analysis of failures (including common cause failures) might need to be performed to help make a decision on the level of detail needed. When more simplified models are used, they should include, at a minimum, the major failure modes identified by the failure analysis used in the development of the system (see Ref. [19]).

5.135. In the analysis of programmable components (e.g. processors, communication modules, sensors, actuators), the starting point should be to consider both the hardware and software parts of the components (e.g. modules, subcomponents), and then to decompose this

hardware and software further if necessary and feasible, and if applicable data are available. The reliability assessment of programmable components should include a justification for the selected level of detail in the analysis of components. Reference [19] provides an example failure modes taxonomy for digital instrumentation and control systems.

5.136. The reliability of the hardware modules should be assessed using standard techniques, as long as these techniques can model the system behaviour, failure modes and dependencies identified.

5.137. The reliability assessment of software modules should include an assessment of existing operating experience (including from other nuclear power plants or from other industrial applications) and an assessment of the development processes (including the validation and verification process) to gain as much confidence as possible in the reliability estimates provided. The reliability assessment of software modules still poses a challenge, with recognized industrial practice still to be established.[23] For further information, see Ref. [20].

5.138. The treatment of recovery actions taken for loss of programmable system functions should be coordinated with human failure event models for the main control room design, minimum alarms and controls inventory. If recovery actions are credited to back up the loss of digital system functions, possible dependencies in relation to the loss of instrumentation should be taken into account.

5.139. The reliability assessment of programmable systems, including communications networks, should include an assessment of intersystem common cause failures. Attention should be paid to computer systems carrying out similar or the same functions. If credible dependencies in the hardware and software of the two computer systems are identified, they should be taken into account in the Level 1 PSA.

5.140. Uncertainties in the modelling of digital systems and data should be identified and addressed, at least qualitatively. Data uncertainties should also be addressed.

5.141. IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [21] states that “Insights gained from probabilistic safety assessment should be considered in the design of [instrumentation and control] systems.” The derivation of instrumentation and control system reliability should be substantiated and based on internationally recognized approaches. Assumptions should be documented and justified. In this respect, practices differ in Member States. Some Member States expect quantitative estimates of probability of instrumentation and control system errors caused by 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 for software reliability claims.

[23] The applicability of the assessment method varies depending on the type of software module (e.g. operating system, application software) and the failure mode being considered, but in practice all methods have limitations in producing a justifiable reliability number, as ideally expected in PSA. Significant uncertainty in the identification of failure modes and modelling of dynamic interactions and data have been noted (see Ref. [20]). This needs to be taken into account in the use of PSA in risk informed applications.

DATA REQUIRED FOR A LEVEL 1 PSA

5.142. Requirement 19 of GSR Part 4 (Rev. 1) [3]states that "**Data on operational safety performance shall be collected and assessed.**"

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

5.144. Plant specific data should be used whenever possible, supplemented by data from similar plants, if it can be shown that these data are relevant, thus providing a broader range 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 such cases, data from similar plants should be used; if these are not available, generic data from the operation of all types of nuclear power plant should be used.

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

5.146. 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 various sources and determine whether any differences can be explained. In general, a judgement will need to be made in selecting the best data source.

5.147. 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.

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

Frequencies of initiating events

5.149. A frequency should be assigned to each initiating event or 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. The frequency should be denoted in occurrences per reactor calendar year such that the frequencies account for the fraction of time the nuclear power plant is in the applicable plant operating state.

5.150. In addition to the techniques mentioned in paras 5.142–5.148, 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 fault tree analysis are inconsistent with operating experience, these results should be reconsidered in light of the intended applications of the Level 1 PSA.

5.151. 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.

5.152. The Level 1 PSA report should give a description of each initiating event or initiating event group 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

5.153. 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, its surveillance (i.e. periodical testing), the boundaries defined for the component in the Level 1 PSA model and its failure modes.

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

5.155. For components such as pumps that need to operate for some time, the mission time should be specified. Determination of component mission times should be based on the system mission time defined through accident sequence analysis (see para. 5.52).

5.156. 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.

Component outage frequencies and durations

5.157. The quantification of the Level 1 PSA should take account of the unavailability of components and systems owing to testing, maintenance or repair. The numerical values used for the frequencies and durations of component outages should be a realistic reflection of the practices in use at, or planned for, the plant.

5.158. Wherever possible, determination of component 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.

5.159. 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

5.160. The logic model developed in the Level 1 PSA should be quantified using the data indicated in paras 5.142–5.159. The accident sequence frequencies should then be 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.

5.161. For the approach using a combination of small event trees and large fault trees (the fault tree linking approach, see paras 5.4 and 5.5), Boolean reduction needs to be performed for the logic models developed using event trees and fault trees for each initiating event group. Logic loops might be generated during fault tree integration owing to mutual system

dependencies, often among the support systems such as service water, instrument air and electric power systems. Before quantifying the Level 1 PSA, care should be taken to ensure that no logic loops exist in the model. If they do exist, breaking the loops is a prerequisite for quantification. The Level 1 PSA report should provide details of how any logic loops in the model were broken.

5.162. In line with Requirement 18 of GSR Part 4 (Rev. 1) [3], any computer code used for the quantification of the Level 1 PSA is required to undergo verification and validation. A number of sophisticated Level 1 PSA computer codes that can be used to perform this analysis are available commercially or have been developed in various Member States.

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

5.164. 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 initiating event group;
(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 (e.g. risk achievement worth, risk reduction worth, Fussell–Vesely and Birnbaum importance for basic events) that are used for the interpretation of the Level 1 PSA;
(f) Frequencies of plant damage states (if they are defined) to provide the interface between Level 1 PSA and Level 2 PSA.

5.165. 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. A sample of the sequences should be checked, 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.

5.166. The analysts should define what is meant by ‘a significant contribution to the risk’ as used in para. 5.165. This could take the form of an absolute criterion or a relative criterion (e.g. relative to total core damage frequency).

5.167. A check should be made that any post-processing performed 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.

5.168. 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 and any post-processing that has been performed.

5.169. The analysts should define what is meant by ‘significant sequence’ and ‘significant minimal cutset’ as used in para. 5.168. These could take the form of absolute criteria or relative criteria (e.g. relative to total core damage frequency).

5.170. 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

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

(a) Fussell–Vesely importance[24];
(b) Risk reduction worth[25];
(c) Risk achievement worth[26];
(d) Birnbaum importance[27].

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 SSCs and actions by operating personnel that contribute significantly 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 [9], [13].

Types of uncertainty

5.172. Requirement 17 of GSR Part 4 (Rev. 1) [3] states that “**Uncertainty and sensitivity analysis shall be performed and taken into account in the results of the safety analysis and the conclusions drawn from it.**” It is recognized that there will be uncertainties in the

[24] 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.

[25] Risk reduction worth is the relative decrease in the frequency of core damage if the probability of the basic event is considered to be zero. Risk reduction worth is a direct function of the basic event probability and can be used to assess the contribution of the basic event to the core damage frequency.

[26] Risk achievement worth is the relative increase in the frequency of core damage if the probability of the basic event is considered to be certain. Risk achievement worth is a measure of the importance of the function represented by the basic event. It identifies basic events playing a major role with regard to safety, even if the underlying failure rate of such basic events is very low.

[27] The Birnbaum importance measure is a measure of the increase in risk when the probability of a basic event is one compared with when it is zero.

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 performing sensitivity studies or an uncertainty analysis, as appropriate. The uncertainties in the Level 1 PSA are normally classified into three general categories as follows:

(a) **Incompleteness uncertainty**: The overall aim of a Level 1 PSA is to perform a systematic analysis to identify all the accident sequences that contribute to the core damage frequency. However, there can be no guarantee that this process is 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.
(b) **Modelling uncertainty**: This arises owing 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.
(c) **Parameter uncertainty**: This arises owing to the uncertainties in the parameters used in the quantification of the Level 1 PSA. This type of uncertainty is usually addressed through an uncertainty analysis, by specifying uncertainty distributions for all the parameters and propagating them throughout the analysis.

5.173. Consideration needs to be given as to how to use the uncertainty information in the design evaluation and decision making process, bearing in mind that probabilistic safety goals and criteria for core damage frequency often relate to point estimates[28] rather than to uncertainty distributions. The way in which the Level 1 PSA is used for the identification of weaknesses also relates to point estimates rather than to uncertainty distributions.

Sensitivity studies

5.174. Studies should be conducted to determine the sensitivity of the results of the Level 1 PSA to the assumptions made and the data used.

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

5.176. The analysts should define what is meant by ‘significant impact on the results of the Level 1 PSA’ as used in para. 5.175. This could take the form of a numerical criterion in an absolute or a relative form (see para. 5.166), a qualitative criterion, or a combination of both quantitative and qualitative criteria.

5.177. 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

[28] In this context, a point estimate is meant to be either calculated by a PSA computer code or another parameter or quantile of the probability distribution, such as the mean or median.

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.

5.178. Sensitivity studies are usually conducted for one assumption or one parameter at a time and the results of the sensitivity studies have no statistical significance. The sensitivity of relevant combinations of assumptions can also be analysed.

Uncertainty analysis

5.179. An uncertainty analysis should be performed 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.

5.180. As part of the data analysis, uncertainty distributions should be specified for the parameters used in the quantification of the Level 1 PSA. These uncertainty distributions should be propagated through the analysis to determine the uncertainties in the core damage frequency. These uncertainties should be used to provide an indication of the level of confidence that may be placed in any insight or result derived the Level 1 PSA.

5.181. Failure rate coupling should be considered in uncertainty analysis with a view to addressing the correlation of data derived from the same source. This can be achieved 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 might lead to internal initiating events, fault sequences might be caused by the damage imposed by other hazards. This section provides recommendations on meeting Requirements 6–13 of GSR Part 4 (Rev. 1) [3] for Level 1 PSA in relation to other hazards, which can be categorized as follows:

(a) **Internal hazards**, which originate from within the site boundary and are associated with failures of facilities and activities that are under the control of the operating organization. Hazards caused by (or occurring at) different facilities on the same site are also considered to be internal hazards. Examples of internal hazards are internal fires, internal floods, internal explosions, internal missiles (e.g. turbine missiles), drop of heavy loads, on-site transport accidents and releases of hazardous substances from on-site storage facilities.

(b) **External hazards**, including natural or human induced events, which originate outside the site boundary and outside the activities that are under the control of the operating organization, over which the operating organization therefore has very little or no control. Examples of natural external hazards are seismic hazards, external floods, high winds and other severe weather conditions; examples of human induced hazards are aircraft crashes, explosion pressure waves (blast), off-site transport accidents and releases of hazardous substances from outside the nuclear power plant site.

6.2. Hazards, including combined hazards, can damage the plant SSCs and thus generate accident sequences that might lead to core and/or fuel damage (or to other undesired end states

as appropriate, if these are to be considered in the Level 1 PSA). Hazards often have the potential to affect many SSCs simultaneously and adversely impact plant personnel. Both internal and external hazards (and combinations thereof) should be included in the Level 1 PSA.[29]

6.3. Combined hazards may refer to combinations of two or more external hazards, combinations of external and internal hazards or combinations of two or more internal hazards. Details on the types of combinations to be considered can be found in IAEA Safety Standards Series No. SSG-64, Protection Against Internal Hazards in the Design of Nuclear Power Plants [6]. Combinations of hazards might have a significantly higher impact on plant safety than each individual hazard considered separately, and the frequency of occurrence of hazard combinations might be comparable to that of the individual hazards, e.g. a severe storm might cause heavy precipitation together with simultaneous dam failure, resulting in high water levels on the plant platform.

ANALYSIS PROCESS

6.4. A consistent approach should be applied to the identification of internal and external hazards and the analysis of their contribution to core and/or fuel damage frequency. The main stages of the analysis of internal and external hazards are typically as follows:

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

The overall analysis approach is illustrated in Fig. 2.

6.5. While the stages of hazard identification and screening are similar for internal and external hazards, the bounding assessment and detailed analysis for each hazard might involve tasks that are unique to that hazard, 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.

6.6. All potential internal and external hazards that might 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 [22].

6.7. As explained in para. 5.161, the technique used to break logic loops within Level 1 PSA for internal initiating events consists of 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

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

owing to internal and external hazards should be incorporated in the Level 1 PSA models for internal and external hazards.

COLLECTION OF INITIAL INFORMATION

6.8. 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, geography and topography of the site and its surroundings;
(d) Environmental conditions, such as climate zone and meteorological characteristics, and detailed observations on the meteorological and hydrological processes and phenomena in the area where the nuclear power plant is located, in accordance with the country's natural phenomena observation programme;
(e) Current information on the location of pipelines, transport routes (rail, road, water) and on-site and off-site storage facilities for hazardous (e.g. combustible, toxic, asphyxiant, explosive, corrosive) materials;
(f) Current information on the location of industrial and military facilities in the vicinity of the site;
(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.

6.9. 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

6.10. 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 as follows (see Refs [6, 7, 23–26] for more information):

Internal hazards:

(a) Internal fires;
(b) Internal explosions;
(c) Internal missiles;
(d) Pipe breaks (including pipe whip and jet effects);
(e) Internal flooding;
(f) Heavy load drops;
(g) On-site electromagnetic interference;
(h) On-site release of hazardous substances;
(i) High energy arcing fault;
(j) On-site transport accidents;
(k) On-site static electricity (large eddy currents);
(l) Radiation accidents involving other reactor units or radioactive sources located at the same site.

External natural hazards:

(a) Seismic hazards;
(b) Hydrological hazards, including external flooding[30];
(c) Meteorological hazards, including extreme meteorological conditions[31] and high winds[32];
(d) Extraterrestrial phenomena, such as meteorites and solar flares;
(e) Biological phenomena[33];
(f) Geological phenomena;
(g) Natural fires.

[30] The term ‘external floods’ covers multiple hazards such as dam failure, tsunamis, meteotsunamis, riverine floods and storm surges.

[31] According to IAEA Safety Series No. SSG-68 Design of Nuclear Installations Against External Events Excluding Earthquakes in the Design of Nuclear Power Plants [29], extreme meteorological conditions include extreme air temperature and humidity, extreme water temperature, snowpack, freezing precipitation and frost related phenomena, and lightning. Other hazards may be connected to these, such as hail and frazil ice.

[32] The term ‘high winds’ covers multiple hazards such as tornadoes, hurricanes, typhoons, downbursts and straight winds..

[33] Typical examples of biological phenomena are abnormal fish population in the cooling pond, and algae, leaves or floating bodies (e.g. from animals) in the cooling water inlet.

External human induced hazards:

(a) Accidental aircraft crashes (of military or civil aircrafts);
(b) Off-site explosion pressure waves (blasts) (from industrial or military installations);
(c) Off-site transport accidents (air, rail, road, water);
(d) Off-site industrial storage accidents;
(e) Accidental off-site releases of hazardous substances;
(f) Off-site electromagnetic interference;
(g) Off-site human induced fires;
(h) Other military accidents (not intentional);
(i) Other industrial accidents.

6.11. As a starting point, the hazards presented in Refs [28–30] and those examined in past PSA 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.

6.12. Additional site or plant specific hazards should be added to this generic list, and the list should be updated regularly to ensure that all such hazards are included. The identification of site or plant specific hazards should be performed in a systematic, structured manner to ensure completeness. For existing plants, an integral part of the internal and external hazard identification process should be a dedicated site survey and plant/site walkdown.

6.13. A list of potential combined hazards that might be significant to risk should be developed. In this context, SSG-64 [6] establishes three types of hazard combinations: consequent (subsequent) events, correlated events and unrelated (independent) events.

6.14. All three categories of hazard combinations should be included in the hazard identification and screening process for combined hazards.

6.15. For combinations of unrelated events, account should be taken of the duration of the impact of individual hazards in the combination (e.g. a seismic event during a long drought period, an internal fire at the plant during long-lasting external flooding).

6.16. The potential combined hazards should be identified on the basis of the list of individual internal and external hazards applicable to the site. The complete list of applicable hazards should be used for this purpose before any screening analysis is performed.[34]

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

SCREENING OF HAZARDS AND HAZARD COMBINATIONS

6.18. A successive screening process is generally established to minimize the emphasis on internal and external hazards and hazard combinations identified in accordance with paras 6.11–6.13 whose significance to risk is low, and instead 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 that none of the significant risk contributors from

[34] 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 human induced hazards are also possible and cannot be excluded a priori (e.g. an increased risk of ship accidents during severe weather conditions).

any internal or external hazard or hazard combination 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.

6.19. 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 neither lead directly to an initiating event nor significantly increase the core damage frequency for a given time period. 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. 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 hazard 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 a more severe hazard.
(d) The impact of a combined hazard is not greater than the impact of the more severe hazard in the combination.

6.20. 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 on the basis of full scope PSA). For more information, see Refs. [28, 29]. 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.

6.21. 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).

6.22. Specific emphasis should be placed on the analysis of the following hazard groups as they are the most significant at many sites:

(a) Seismic hazards;
(b) Hydrological hazards;
(c) Meteorological hazards;
(d) Human induced hazards.

6.23. In order to screen out specific hazards, it should be proven that the conditions specific to the location of the plant (e.g. topographical, geographical, meteorological or biological conditions) support the assumption that these hazards are not sufficient to damage the plant (e.g. hurricanes in a non-coastal area).

6.24. External hazards with a certain potential for damage should be screened out only if it is demonstrated that the frequency of exceedance of a particular magnitude is negligible.

6.25. For each individual hazard, on the basis of pessimistic assumptions about events subsequent to the initiating event, an approximate maximum impact should be determined for use in the screening process.

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 subclasses and the screening criteria applied to each subclass, so as to avoid screening out hazards with low frequency but high potential for damage. However, this approach should not be taken if a quantitative screening criterion can be applied to the hazard as a whole, as it might result in the screening out of each individual subclass and thus to the screening out of the hazard as a whole.

6.27. Initiating events occurring at the plant might 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.

6.28. 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 either 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.[35]

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 (Rev. 1) [3] for a Level 1 PSA for internal hazards (see para. 6.8 for a list of typical internal hazards). Specific recommendations are provided for Level 1 PSA relating to the internal hazards for nuclear power plants. Other internal hazards are not explicitly covered in this Safety Guide but may be addressed using similar approaches.

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

7.2. Internal hazards (see paras 6.1 and 6.8) 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

[35] The following examples of changes are for the purposes of illustration:
(a) Changes in military or industrial facilities within a 30 km radius around the site or changes in nearby transport routes (i.e. railways, aircraft routes, roads and rivers) leading to changes in the range and magnitude of human induced external hazards.
(b) Changes in dam construction on rivers upstream of the plant site leading to an increase in the damage potential of the external flood hazard.
(c) Changes in environmental conditions (e.g. average and maximum annual wind speed, water level, temperature, local precipitation) which might lead to a change in the frequency of natural external hazards with a higher damage potential.

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 of the Level 1 PSA for internal hazards 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. Most internal hazards (e.g. internal explosions, fire, explosion, flooding) can occur in a variety of different locations within the plant boundary (inside or outside buildings). Therefore, the hazard characterization should specify:

(1) A global plant analysis boundary so that all locations that could contribute to the hazard risk are considered;
(2) 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 area where it was initiated.

7.4. Contributions to core and/or fuel damage frequency from the internal hazards that remain after 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 power operation and shutdown states. The availability of a Level 1 PSA for internal initiating events should be a prerequisite for the development of a Level 1 PSA for internal hazards. The results of the hazard analysis may yield further initiating events in addition to those found by performing 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:

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

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 performed 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 through plant walkdowns.

7.9. Since the information from plant walkdowns might provide 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 specific tasks (i.e. detailed analysis for selected hazards) could necessitate 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 [31]:

(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 owing to actuation of fire suppression systems (e.g. spray and flood caused by fire suppression systems might damage equipment that would otherwise survive a fire, or the failure mode of such equipment might be altered);

(e) The effects of fire on SSCs and their associated 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 SSCs and to the integrity of the plant's structural features (e.g. walls, ceilings, columns, roof beams);
(g) The effects of fire on component dependencies and component failure probabilities;
(h) The effects of fire on human actions and human error probabilities;
(i) The effects of 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. Physical separation (i.e. fire barriers) between redundant trains of SSCs important to safety can limit the extent of fire damage. The quantification of the contribution of fire to the core damage frequency using the Level 1 PSA model for internal fire should therefore 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, taking into consideration the following:

(a) Smoke might cause electrical and/or electronic devices to fail, in particular when accompanied by high temperature.
(b) Human error probability might be higher as a result of smoke (which can be toxic as well as merely irritating) and heat.
(c) The presence of smoke may necessitate evacuation of the main control room.

7.15. For a Level 1 PSA for internal fire in 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 in shutdown states, as presented in Section 9;
(b) The performance of separate screening to take into account the potentially higher and additional fire loads (e.g. transient combustibles) and additional potential ignition sources typically associated with maintenance activities performed during shutdown states;
(c) The availability of fire protection means;
(d) The potential for further paths for fire propagation (e.g. some doors might be open during shutdown states);
(e) The increased occupancy of different plant locations during outages, which might improve the fire detection capabilities but might also create additional fire sources;
(f) The fire related plant operating and configuration changes that are implemented to control combustibles and those that are implemented to provide compensatory measures for system or component outages.

7.16. Deterministic fire hazard analysis and fire safe shutdown analysis, performed as applicable during plant design (see SSG-64 [6]) and operation (see NS-G-2.1 [32]), should be used to provide an important input to the Level 1 PSA for internal fire. The information provided might include a list of components and cables and their locations and details of the

partitioning of the plant into 'fire compartments'[36], on the basis of functional and detailed fire impact analyses performed specifically for the design of 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: see Ref. [31]. To facilitate this analysis, the plant should be divided into fire compartments, which are then scrutinized individually. The plant partitioning performed during design might be useful as a starting point for the division of these physical areas. The criteria applied for specifying fire compartments should be justified and documented.

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 7.19–7.67. 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 the level of detail of the analysis for the Level 1 PSA for internal fire, the frequency associated with a particular fire scenario depends on the ignition frequency and the probability of fire suppression.

Data collection and assessment of potential for internal fire

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 from operating experience related to:
    (i) fire events;
    (ii) observations of failures and/or deterioration of fire protection features;
(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 fire suppression means;
(f) Human actions in the event of a fire and human error probabilities;
(g) Fire brigade availability and capability;
(h) Fire suppression system and equipment characteristics (e.g. timing of system actuation, fire suppression agents that might cause equipment damage or prevent operating personnel from entering the fire compartment);
(i) Equipment failure modes induced by fire and fire damage criteria.

[36] In SSG-64 [6] a fire compartment is described as "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 simply be a well enclosed room that is not necessarily surrounded by fire resistant barriers.

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

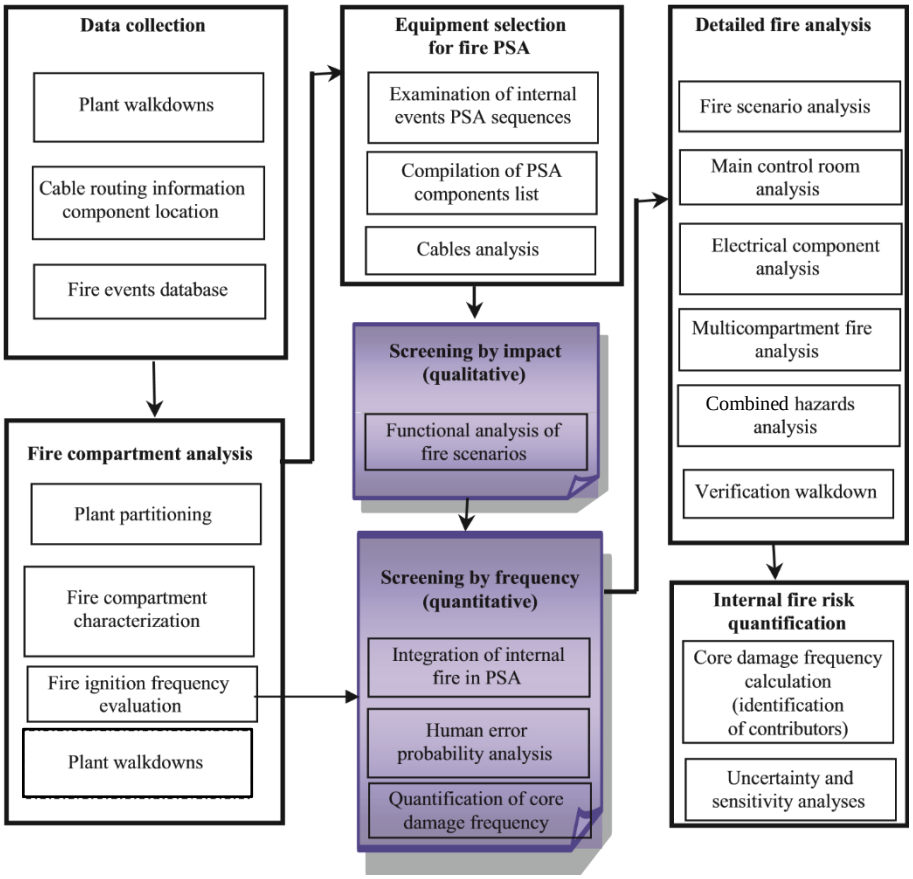

FIG. 3. Process for development of a Level 1 PSA for internal fire.

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 in place (e.g. fire detection and extinguishing systems and equipment);
(c) The fire resistance rating of the barriers surrounding the compartment;
(d) The components and equipment, including cables, located inside the fire compartment;
(e) Adjacent fire compartments and 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, whether permanent or temporary);
(h) Potential ignition sources (e.g. type, amount, location);
(i) Procedures and other administrative provisions for control of combustible materials;

(j) Occupancy level (i.e. the possibility of fire detection 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 in 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 fire ignition frequency, both for fire compartments and for fire sources, 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 ignition frequency associated with fire ignition sources and/or fire compartments should be evaluated as far as feasible using plant specific data. If these data are insufficient to estimate fire ignition frequency, generic data should be used along with the available plant specific data, adjusted on the basis of the actual fire ignition sources present (including sources resulting from hot work), and the amounts of permanent and temporary combustible and ignition sources 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, including transient fires and fires caused by welding, cutting or other hot work in different plant operating states).

7.27. Fire frequency should be estimated as a mean value with statistical uncertainty intervals.

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 Level 1 PSA for internal fire 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 failure events);
(d) The failure might lead to spurious actuation of functions that could induce other unsafe effects on the plant, both during 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 including 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. As passive components could be also affected by fire, the vulnerable parts of such components should be considered in the Level 1 PSA for internal fire.

7.30. Identification of all 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 from 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 determine more accurately 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 the identification of critical fire compartments and areas, followed by the specification of 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 both of the following apply:

(a) The fire load density is below a specified accepted threshold and the potential for propagation is very low;
(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) There is very low potential for fire effects spreading to other fire compartments containing SSCs important to safety.

7.34. For the purposes of screening, all components and cables exposed to fire should be assumed failed, that is, the pessimistic assumption is made that the fire detection and extinguishing features are either ineffective or not available. Other protective measures (e.g. fire shields, protective coatings, enclosures not qualified as fire resistant) 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 individual fire compartment, complexes of compartments where fire could propagate are defined by adding all the compartments adjacent in any direction and all the compartments connected with that compartment by ventilation without necessarily being adjacent to it. 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 pessimistic assumptions could be made regarding the reliability and effectiveness of fire barrier elements, on the basis of 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 spread of fire from the transformer yard into the turbine hall).

7.37. For a multi-unit site and/or multi-source site, the potential spread of a fire from one reactor unit or radioactive source to a fire compartment of another reactor unit should be considered in the analysis. The possibility of fires in common areas (e.g. diesels shared between units, switchyard) should be considered.

Screening by 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. For evaluating the frequencies of occurrence of fire scenarios and the associated conditional unavailability of the necessary safety functions owing 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. actions 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 human failure events are penalized to take account of the fire context, as described in para 5.118(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, the spread of fire to other compartments 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 human failure events for Level 1 PSAs for internal fire should include the following (see Ref. [16] for general guidelines on fire human reliability analysis):

(a) Human failure events 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 owing to the possibility that it might be harder for operating personnel to implement actions than in the base case.

(b) Human failure events that are relevant only for fire, including abandonment of the main control room. In this case the methods to assess fire specific human failure events usually follow the same principles as other types of human failure event.
(c) Undesired responses by operating personnel to fire induced spurious alarms and indications.

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 taking these 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 internal 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 contribution of fire in an individual fire compartment to the core damage frequency is sufficiently low to retain 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.

7.46. Screening by considering the contribution of fire to the core damage frequency should take into account 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 (i.e. screening by impact and by frequency) should be as follows:

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

(b) A list of fire scenarios associated with fire compartments that might represent significant contributors to risk, and which therefore 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. The detailed analysis of fire should be aimed 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 fire extinguishing systems and equipment in place in the fire compartment and other aspects such as growth and propagation of fire should all be taken into account. All direct effects of fire, including flame, plume, ceiling jet, radiant heat from hot gases, fire by-products such as smoke and soot, and indirect fire effects and consequences (e.g. from fire extinguishing media, or consequential high energy arcs) should be considered and assessed. Generally, dedicated walkdowns should be undertaken in performing 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 SSCs.

7.50. The effects of fire and fire by-products (e.g. smoke, toxic gases) on human performance should be assessed. It should also be noted that overpressure resulting from fire might prevent the opening of doors needed for personnel to access recovery locations or for the fire brigade to conduct firefighting activities.

7.51. The choice of specific modelling tools for the analysis of fire growth and propagation (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 failures of SSCs, including cables. A fire scenario should be represented in the Level 1 PSA model for internal fire, for example, by fire event trees (see example in Annex II), where all the important features affecting fire development are modelled (i.e. design and quality of fire barriers, fire growth and propagation model, criteria 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 event trees.

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

7.54. Pathways that might be relevant for fire propagation (e.g. ventilation ducts or cable trays and channels, 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 occurrence frequency of a fire scenario should be complemented with additional data specific to the fire compartment, such as the presence of temporary fire loads and ignition sources and their ignitability.

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 these locations, such as the widespread effect of a fire in the control rooms across all credited systems, the potential for spurious actuation of systems and the impact of fire in control rooms on actions by operating personnel. The latter should include:

(a) The effects of fire and fire by-products (e.g. smoke, soot) on the availability of the necessary functions of instrumentation and related equipment;
(b) The capability of features for fire detection and suppression, including the potential adverse impact of indirect fire effects, typically as a result of fire suppression (e.g. from extinguishing media);
(c) The use of an alternative location for safe shutdown, taking into account aspects of accessibility, interdependencies and other possible limitations;
(d) Potential fire-induced failure modes affecting both the main and supplementary control rooms simultaneously (e.g. the spurious actuation of the switchers caused by the fire in the supplementary control room which can lead to overtaking the control from the main control room)
(e) The effects of the spread of fire by-products, such as smoke or toxic gases.

In addition, fire propagation inside a fire compartment should be taken into account, including the presence of physical segregation and separation means such as qualified fire barriers as well as spatial separation of components of redundant trains.

Analysis of fire in rooms with electrical components

7.58. Rooms with electrical components, switchgear rooms, cable spreading rooms and other rooms containing electrical instrumentation and control equipment tend to become natural centres of convergence for equipment and wiring. They contain electrical equipment and cables that might belong to more than one train of the credited system. Therefore, the potential impact of fire on redundant items important to safety or on other Level 1 PSA related equipment is likely to be higher than the impact of fire in other plant locations and this should be considered in the analysis.

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

Multicompartment fire analysis

7.60. Multicompartment fire analysis is aimed at identifying potential fire scenarios significant to risk that involve more than one fire compartment. It should be assumed that fire might spread from one compartment to another through fire barriers between the compartments, in particular via fire barrier elements with active functions such as doors or dampers, or via barrier penetrations such as cable trays or ventilation ducts. Multicompartment detailed fire analysis

should be based on a fire growth model, a model for analysis of fire propagation and a model for fire detection and suppression.

7.61. As for single fire compartments, the detailed analysis for multicompartment fires should consider the depth of propagation of the fire and the spread of direct and indirect fire effects, covering not only heat transfer between fire compartments, but also other fire by-products, such as extinguishing media.

Analysis of combined hazards

The potential for occurrence of combinations of fires and other hazards of all three combination categories mentioned above in para. 6.13 (as defined in SSG-64 [6]) should be assessed. Combinations involving fire as a consequence of other hazards should be considered in the Level 1 PSA for those hazards, whereas combinations involving fire with other consequential hazards should be considered in the Level 1 PSA for internal fire. For combinations of fires correlated with other hazards by a common cause and combinations of fires with unrelated hazards (occurring simultaneously but independently) that have not been screened out, the analysts should decide whether these combined hazards are to be considered in the Level 1 PSA for internal fire or for one of the other hazards.

7.62. A qualitative analysis of internal fires induced by other hazards (e.g. seismicity, lightning, external fire, aircraft crash) should be performed as part of the analyses carried out for the initial event (see section 6). Fire compartments where the combined impact of other hazards and fire could be important for safety should be analysed. Examples of impacts to be considered include ignition sources induced by hazards, spurious actuation or degradation of fire suppression systems and difficulties in taking manual firefighting actions (see the recommendations on Level 1 PSA for external hazards provided in Section 8).

7.63. The following effects of internal fire induced by other hazards on the performance shaping factors (or other factors, depending on the human reliability analysis method) of operating personnel should be taken into account:

(a) Accessibility of the compartments of interest after the fire has started;
(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

7.64. 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.

7.65. The final quantification of the contribution of internal fire to the core damage frequency should be performed for the fire compartments remaining after 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.

7.66. 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

7.67. In accordance with Requirement 20 of GSR Part 4 (Rev. 1) [3], the Level 1 PSA for internal fire should be documented in a manner that facilitates its review, application and update. 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, as well as partitioning of the plant into fire compartments;
(b) A description of the specific methods and data used to assess the internal fire hazard;
(c) A description of the changes made to 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 out of particular fire compartments from the analysis;
(f) The results of the detailed analyses of fire scenarios, for example for the main control room, for the electrical component room and for multicompartment fires;
(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

7.68. 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, similar aspects to those listed for internal fire in para. 7.15 should be considered.

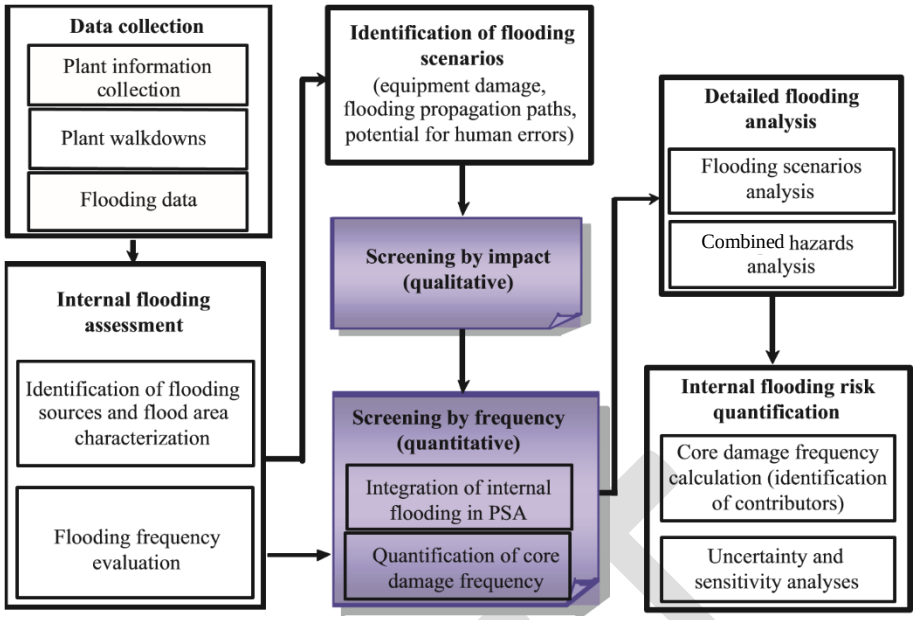

FIG. 4. Process for development of a Level 1 PSA for internal flooding

Data collection and assessment of potential for internal flooding

7.69. For operating nuclear power plants, plant walkdowns with a specific focus on 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.

7.70. Possible internal flooding events should be identified and characterized (see SSG-64 [6] for general considerations on flooding in the design of nuclear power plants). In performing this task, consideration should be given to the following:

(a) Possible sources of flooding: pipes, vessels, tanks, pools, valves, heat exchangers, connections to open-ended sources (e.g. sea, lake, river), SSCs shared by multiple units or sources (e.g. fire main ring);
(b) Possible flooding mechanisms: breaks, leaks, ruptures, spurious or desired actuation of a spray system (e.g. containment spray system, fire extinguishing system),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, 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.

7.71. When identifying potential flooding events, particular consideration should be given to plant shutdown conditions, as water pathways are frequently reconfigured manually during shutdown.

7.72. 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 and spent fuel pool aspects and to the potential for failure of flood barriers

7.73. The plant should be divided into physically separated ‘flooding areas’, each of which is viewed as generally independent of the other areas in terms of the potential effects of internal flooding and the potential for flood propagation.

7.74. 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, generic data or expert judgement may be used with appropriate justifications.

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

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

7.77. The frequency of flooding should be estimated as a mean with statistical uncertainty intervals.

Identification of internal flooding scenarios

7.78. For each flooding area, the SSCs that could be affected by 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.

7.79. The consideration of SSCs affected by internal flooding should include elevations, barriers, doors and drains. The potential for drain blockages should also be considered.

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

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

7.82. The location, including the elevation and any protection features of electrical and/or electronic components (e.g. cabinets, terminal boxes for cables for SSCs important for safety) and other components that are sensitive to humidity should be identified. In this way, the vulnerability of components with respect to flooding of certain rooms can be identified.

7.83. The potential impact of flooding on plant operation should be assessed. This assessment should include spurious actuation of components or systems owing to flooding effects, which could initiate particular accident sequences.

Screening by impact

7.84. Internal flooding scenarios should be screened on the basis of their impact. Critical flooding areas can be selected by screening out those with a negligible potential impact on plant safety. A flooding area may be screened out if one or both 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 the systems necessary for safe shutdown of the plant nor their support systems are located in the area of flood origin or in the flood propagation zone;
(b) The compartment does not contain any sources of flooding, including flooding originating from other compartments, sufficient to cause failure of equipment.

Screening by frequency

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

7.85. Internal flooding events could be further screened for their contribution to the core damage frequency. If so, 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).

7.86. The human reliability analysis performed in the Level 1 PSA for internal initiating events should be fully reviewed. 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. Human error probabilities should be reassessed and adjusted, taking into account specific procedures for the 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 plant locations where actions need to be taken by personnel to ensure the required safety functions after flooding has started;
(b) 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

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

7.88. Quantitative criteria for screening in accordance with contribution to the core damage frequency should be defined for the 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 not exceed 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) For an individual flooding area, the contribution of flooding to the core damage frequency is sufficiently low to retain all risk significant flood scenarios.

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

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

(b) A list of flooding scenarios associated with flooding areas that might represent significant contributors to risk, and which therefore 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

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

(a) Timing calculations (e.g. 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 that might failed owing to the flood, and analysis of results, including sensitivity studies and uncertainty analysis.

7.91. All potentially contributing flooding 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.

7.92. 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. 7.78). A flooding scenario can be represented by event trees 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.

7.93. 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 human failure events for internal flooding should include the following:

(a) Human failure events that are included in the Level 1 PSA for internal initiating events but are also relevant to the flooding scenario. In such cases, it might be necessary to revise the assessment of performance shaping factors as it might be more difficult for operating personnel to implement actions than in the base case scenario.
(b) Human failure events that are relevant only to flooding (e.g. those related to the isolation and subsequent restoration of electrical power supply). In such cases, the methods used to assess flood specific human failure events can usually follow the same principles as the ones used to analyse other types of human failure event. The impact of the flooding specific actions (e.g. the isolation and subsequent restoration of electrical power supply) on the plant SSCs should also be considered in the PSA model.
(c) Undesired responses by operating personnel to flood induced spurious alarms and indications.

Analysis of combined hazards

7.94. The potential for occurrence of combinations of internal flooding and other hazards of all three combination categories mentioned in para. 6.13 (as defined in SSG-64 [6]) should be assessed. Combinations involving internal flooding as a consequence of other hazards should be considered in the Level 1 PSA for those hazards, whereas combinations involving internal flooding with other consequential hazards should be considered in the Level 1 PSA for internal flooding. For combinations of internal flooding correlated with other hazards by a common cause and combinations of internal flooding with unrelated hazards (occurring simultaneously but independently) that have not been screened out, the analysts should decide whether these combined hazards are to be considered in the Level 1 PSA for internal flooding or for one of the other hazards.

7.95. A qualitative analysis of internal flooding induced by other hazards (e.g. seismicity, external flooding, aircraft crash, internal fire) should be performed as part of the analyses carried out for the initial event (see Section 6). Flooding areas where the combined impact of other hazards and flooding could be important for safety should be analysed. Examples of impacts to be considered include flood sources induced by hazards and difficulties in taking manual flood protection actions (see the recommendations on Level 1 PSA for external hazards provided in Section 8). In addition, flooding caused by the 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 flooding induced by other hazards on the performance shaping factors (or other factors depending on the human reliability analysis method) of operating personnel should be taken into account:

(a) Accessibility of plant locations where actions need to be taken by personnel to ensure the required safety functions after flooding has started;
(b) Increased stress level;
(c) Failures of indication or false indication;
(d) Other effects of flooding and initiating hazard on the behaviour of operating personnel.

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 internal 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. In accordance with Requirement 20 of GSR Part 4 (Rev. 1) [3], the Level 1 PSA for internal flooding should be documented in a manner that facilitates its review, application and update. 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 to take into account the effects of internal flooding;
(c) Justification for the screening out of particular flooding scenarios from the analysis;
(d) The results of the detailed analysis of flooding scenarios, including descriptions 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 the collapse of structures and 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, as a result of heavy loads dropping onto the vessel, spent fuel pool or systems that perform critical safety functions. The potential collapse of structures and fall of objects, in particular 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 to SSCs important to safety 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, certain individual initiators of the collapse of structures or heavy load drops may be screened out.

7.101. The probabilistic analysis should include 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 might drop down and destroy pipes connected to the vessel).

7.102. The contribution of the collapse of structures and 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 the collapse of structures or heavy load drops should be consistent with the plant response model developed for the Level 1 PSA for internal initiating events in shutdown states (see para. 9.12).

7.104. All permanent lifting equipment in the plant should be taken into consideration. Areas where a collapse of structures or 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. The calculations should take into consideration failure of mechanical equipment, human error and possible unavailability of automatic protection functions.

7.107. For combinations of structure collapse or dropped loads with other hazards, the following effects on the performance shaping factors of operating personnel should be taken into account:

(a) Accessibility of plant locations where actions need to be taken by personnel to ensure the required safety functions after the collapse or load drop;

(b) Increased stress level;

(c) Failures of indication or false indications;

(d) Spurious actuation of SSCs important to safety;

(e) Combined effects of a structure collapse or heavy load drop on the behaviour of operating personnel.

7.108. 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 drop should be analysed. The possible direction, size, shape and energy of any 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.

7.109. If a Level 2 PSA is foreseen, each structure collapse or 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

7.110. 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 owing to ignition of hydrogen or owing to oil combustion on components relevant to PSA should be considered in the context of the analysis of the impact of turbine missiles.

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

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

7.113. 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.

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

7.115. 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.

7.116. 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.

7.117. The frequencies of initiating events should be calculated in accordance with the recommendations in Sections 5 and 9.

7.118. For combinations of missiles following turbine disintegration with other hazards, the following effects on the performance shaping factors of operating personnel should be taken into account:

(a) Accessibility of plant locations where actions need to be taken by personnel to ensure the required safety functions after turbine disintegration has started;

(b) Increased stress level;

(c) Failures of indication or false indications;

(d) Spurious actuation of SSCs important to safety;

(e) Combined effects of missiles following turbine disintegration on the behaviour of operating personnel.

7.119. For each turbine disintegration event, it should be conservatively assumed that the worst configuration and conditions in terms of missiles generation are in place. The possible direction, size, shape and energy of the missile or missiles generated should be characterized and the effects on the building structure and on the plant should be assessed.

7.120. If a Level 2 PSA is foreseen, each turbine disintegration 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 internal explosion

7.121. 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 designed 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.

7.122. The design of the plant building provides for the prevention and mitigation of explosions (see SSG-64 [6]). For design purposes, the systematic analysis of explosions is used to characterize the potential sources of explosions (e.g. nature and quantity of explosive materials, localization), the potential impacts of deflagrations or detonations on the plant (e.g. overpressure, impulse or drag loads, fire, 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.

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

7.124. The frequency of explosion events should be evaluated using the recommendations in Section 5. The quantification should consider the amount of explosive material located within the plant, human activities that might cause an explosion and the effectiveness of the means of prevention (e.g. hydrogen detection equipment, leakage of explosive liquid or gas detectors, ventilations).

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

Analysis of other credible internal hazards

7.126. The general process for conducting Level 1 PSA for internal hazards should be adapted for a Level 1 PSA for all other internal hazards remaining after the individual or combined hazards screening.

7.127. A plant walkdown should be performed for identification of potential sources of other credible internal hazards and for verification purposes.

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 (Rev. 1) [3] for Level 1 PSA for external hazards. Specific recommendations are given only for selected external hazards from the following list that cannot be screened out for a given nuclear power plant site:

External natural hazards:

(a) Seismic hazards;

(b) Hydrological hazards (e.g. external flooding);

(c) Meteorological hazards (e.g. high winds, precipitation)

(d) Extraterrestrial hazards (e.g. meteorites, solar flares);

(e) Biological hazards;

(f) Geological hazards;

(g) Natural fires.

External human induced hazards:

(a) Transport accidents;
(b) Aircraft crashes;
(c) Industrial and military accidents;
(d) Explosions;
(e) Fires;
(f) Releases of hazardous materials.

BOUNDING ASSESSMENT AND DETAILED ANALYSIS FOR LEVEL 1 PSA FOR EXTERNAL HAZARDS

General aspects

8.2. External hazards (see paras 6.1 and 6.8) 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 external hazards are sometimes significant contributors to the overall risk). A consistent approach should be applied for the bounding assessment and detailed analysis for Level 1 PSA for external hazards.

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

8.4. The bounding assessment 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 of the Level 1 PSA for external hazards from the Level 1 PSA for internal initiating events:
    (i) Determination of initiating events induced by the external 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 external 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).

8.5. Contributions to the core damage frequency from those external hazards that remain after the screening process should be determined using a Level 1 PSA for those hazards. A Level 1

PSA for external hazards should rely on the model of plant response developed for the Level 1 PSA for internal initiating events, both for power operation and shutdown states. The availability of a Level 1 PSA for internal initiating events should be a prerequisite for the development of a Level 1 PSA for external hazards. The results of the hazard analysis may yield further initiating events in addition to those found by performing 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.

8.6. 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.

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

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

8.9. In the bounding assessment, all potential impacts on the nuclear power plant of each external hazard not screened out should be considered.[37]

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

8.11. 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.

8.12. In the bounding assessment, applicable combinations of external hazards, as described in para. 6.11, should also be considered.

8.13. 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 occurrence 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.

Natural hazards

Seismic hazards

8.14. 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

[37] 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).

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, 26, 27, 33].

Hydrological hazards

8.15. An assessment should be made of whether the following hydrological hazards need to be considered in the Level 1 PSA:

(a) High water level (flooding) hazards:
  (i) Rapidly developing:
  - Flash flood caused by extreme local precipitation;
  - Tsunami;
  - Ice flood;
  - Riverine flooding caused by failure of water-retaining structures upstream;
  - Riverine flooding caused by blockage of river downstream;
  - Waves caused by landslides, avalanches or volcanism;
  - Seiche;
  - Flood waves caused by volcanic melting of snow and ice.

  (ii) Slowly developing:
  - Storm surge;
  - Riverine flooding caused by extreme precipitation (e.g. rain, snow) outside the plant boundary;
  - Flooding caused by changes in river channels downstream;
  - Flooding caused by tide or springtide.

(b) Low water level hazards:
  (i) Rapidly developing:
  - Riverine flooding caused by failure of water-retaining structures downstream;
  - Ice jam;
  - Flooding caused by blockage of river upstream.

  (ii) Slowly developing:
  - Drought;
  - Riverine flooding caused by changes in river channels upstream;
  - Low sea level.

(c) Local precipitation (e.g. rain, snow):
  (i) Increased roof load caused by local precipitation;
  (ii) Local flooding caused by local precipitation.

(d) Groundwater level:
  (i) High groundwater level;
  (ii) Low groundwater level.

(e) Non-biological flotsam.

8.16. Applicable combinations of hydrological hazards with other hazards, as described in para. 6.11 should also be considered, taking into account possible dependencies (e.g. high water level, consequential dam failures).

Meteorological hazards

8.17. An assessment should be made of whether the following meteorological hazards need to be considered in the Level 1 PSA:

(a) Temperature induced hazards:
  (i) Hazards from low temperature phenomena;
  (ii) Hazards from high temperature phenomena.

(b) High wind hazards:
  (i) Extratropical high winds (extratropical cyclones, thunderstorms, squall lines, weather fronts);
  (ii) Tornadoes or waterspouts;
  (iii) Downbursts or katabatic winds;
  (iv) Tropical cyclones, hurricanes or typhoons;
  (v) Salt or dust storms;
  (vi) Salt spray winds;
  (vii) Wind induced missiles.

(c) Snow hazards.

(d) Air humidity hazards.

(e) Lightning.

(f) Hail.

(g) Air pressure hazards.

(h) Fog/mist.

High winds

8.18. The following types of high wind should be considered and subjected to bounding assessment or detailed analysis, depending on the location of the site:

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

Applicable combinations of meteorological hazards with other hazards, as described in para. 6.11 should be considered, taking into account possible dependencies (e.g. high winds and high water levels).

External flooding

8.19. 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).

Applicable combinations of external flooding hazards with other hazards, as described in para. 6.11 should be considered, taking into account possible dependencies (e.g. high water levels, consequential dam failures).

8.20. 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

8.21. A comprehensive list of potential natural hazards other than seismic hazards, hydrological hazards and meteorological hazards should be considered in the bounding assessment. 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.

8.22. Applicable combinations of natural hazards with other hazards, as described in para. 6.11 should be considered, taking into account possible dependencies (e.g. severe weather conditions, transport accidents).

Human induced hazards

8.23. An assessment should be made of whether the following human induced hazards need to be considered in the Level 1 PSA:

(a) Mechanical impact from accidents:
    (i) Civil and military transport accidents, including aircraft crashes and air, rail, road and water transport;
    (ii) Industrial accidents;
    (iii) Military accidents.
(b) Human induced fires:
    (i) From transport accidents;
    (ii) From industrial accidents;
    (iii)From military accidents.
(c) Explosions (blasts):
    (i) From transport accidents;
    (ii) From industrial accidents;
    (iii)From military accidents.
(d) Releases of hazardous substances (e.g. asphyxiant, combustible, corrosive, explosive, and toxic materials):
    (i) From transport accidents;

(ii) From industrial accidents;
(iii)From military accidents;
(iv)From pipeline accidents.

(e) Other hazards:

(i) Excavation or construction work outside the plant boundary;
(ii) Grid instability;
(iii)Industrial impurities of high voltage insulations;
(iv)Electromagnetic interference;
(v) Human induced ground settlement.

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

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

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

(f) Excavation work outside the site boundary;
(g) Electromagnetic interference (e.g. magnetic or electrical fields generated by radar, radio or mobile phones) outside the site boundary.

PARAMETERIZATION OF EXTERNAL HAZARDS

General aspects

8.25. 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.

Natural hazards

Seismic hazards

8.26. Seismic hazards are characterized by following main parameters (see Refs [7, 26]):

(a) The peak ground motion (e.g. acceleration, velocity, displacement);
(b) The energy content, which is generally represented by spectral accelerations associated with the ground response spectrum but may also include other intensity measures.

8.27. Vibratory ground motion caused by earthquakes should not be eliminated from consideration as seismic waves can reach any point on the Earth's surface.

8.28. Earthquake ground motion should not be screened out.

High winds

8.29. 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 flooding

8.30. 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 flooding (see IAEA Safety Standards Series No. SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations [25]). For flooding, 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.

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

Other natural hazards

8.32. 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.

8.33. 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

8.34. 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 transport related hazards, the actual danger is from an explosion or a release of hazardous material. The key parameter is the amount of material being transported 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 (e.g. a barge colliding with a water intake, an aircraft colliding with a structure), the key parameters should be related to the impact (i.e. the mass and the velocity of the impacting object).

(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.

8.35. Each human induced hazard might result in a combination of various impact factors that need to be considered. For example, an aircraft crash might cause direct damage, explosion, fire and vibration. Similarly, a pipeline accident might result in a blast (impulsive load resulting from deflagration or detonation), fire and vibration. It might also produce missiles that 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.

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

8.37. Applicable combinations of human induced hazards with other hazards, as described in para. 6.11 should be considered, taking into account possible dependencies (e.g. chemical release, wind speed and direction).

DETAILED ANALYSIS OF EXTERNAL HAZARDS

8.38. A detailed analysis should be performed for all (single and combined) hazards for which the bounding or simplified analysis with conservative assumptions has demonstrated that the risk from the hazard might be non-negligible.

8.39. The Level 1 PSA model for internal initiating events is a prerequisite for performing a detailed analysis of external hazards.

8.40. 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.

FREQUENCY ASSESSMENT FOR EXTERNAL HAZARDS

General aspects

8.41. Paragraph 4.20 of SSR-1 [22] 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.

8.42. External hazards are characterized by multiple output parameters, some of which might 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.

8.43. 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.

8.44. Analysis of time trends (e.g. variation of hydrological or meteorological parameters in time owing to climate change) should be performed to confirm the absence of trends towards increased frequency of the hazards. If trends towards significantly increased frequency are confirmed, then hazard frequencies should be defined in order to take climate change into consideration over the time period of interest. Recent, short term trends in decreasing hazard frequencies should not be taken into account unless they are well understood as being caused by processes having a non-random nature.[38]

8.45. 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.

8.46. 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 Refs [23, 24, 25, 34].

Natural hazards

Seismic hazards

8.47. The occurrence frequency of earthquake ground motions at the site should be based on a site specific probabilistic seismic hazard assessment (see Refs [7, 26, 33]).

8.48. Probabilistic seismic hazard assessment should be conducted in accordance with the recommendations provided in IAEA Safety Standards Series No. SSG-9 (Rev. 1), Seismic Hazards in Site Evaluation for Nuclear Installations [24].

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

8.50. For the lower bound parameter value for use in the hazard analysis, it should be demonstrated that seismic events with any lower parameter value can cause only insignificant damage to structures and components, including those off the site, such as power lines and pipework carrying hazardous material.

High winds

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

8.51. The model used for calculating the frequency and intensity of 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 frequency of high winds should not dominate in the assessment of wind frequencies.

8.52. Wind hazard assessment should be conducted in accordance with the recommendations provided in SSG-18 [25].

8.53. The range of parameters used to characterize the wind hazard should cover the range of interest (e.g. from 'no failure' to 'screening limit') in order to accurately estimate the wind risk.

8.54. The high wind hazard assessment should take into consideration relevant time trends (e.g. climate change).

8.55. 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 conservatively taken into account in developing the hazard curve for high winds.

External flooding

8.56. Calculation of the frequency and consequences of external flooding 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).

8.57. External flooding hazard assessment should be conducted in accordance with the recommendations provided in SSG-18 [25].

8.58. The uncertainties in the models and parameter values should be properly taken into account and fully propagated in order to obtain a family of hazard curves from which a mean hazard curve can be derived. The analysis of frequency and consequences of extreme river floods should include flooding caused by single or cascade dam failures.

8.59. 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 taken of 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.

8.60. 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.

8.61. 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.

8.62. The external flooding hazard assessment should take into consideration relevant time trends (e.g. climate change).

Other natural hazards

8.63. 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.

8.64. 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.

8.65. 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

8.66. Human induced external hazard assessment should be conducted in accordance with the recommendations provided in [23].

8.67. 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 hazardous (e.g. combustible, explosive, asphyxiant, toxic, corrosive) material stored outside the site boundary, within a predetermined radius of the nuclear power plant, as follows:
   (i) Potential hazard sources (within a predetermined radius of the nuclear power plant) such as :
      — Oil or gas storage facilities;
      — Oil or gas transportation lines;
      — Air transportation of hazardous substances;
      — Rail transportation of hazardous substances;
      — Road transportation of hazardous substances;
      — Water transportation of hazardous substances;
      — Other facilities.

      .
   (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 other training facilities whose activities might 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).

General aspects

8.68. The fragility[39] of SSCs should be evaluated using available plant specific information to the extent necessary for the purpose of the analysis (bounding assessment or detailed analysis) and accepted engineering methods. Findings from plant walkdowns should be considered in the analyses.

8.69. 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 might result in initiating events such as loss of off-site power or a blast. Such failures might be highly correlated if the fragilities are low.

8.70. 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).

8.71. When combined hazards are considered, all the hazard specific failure mechanisms resulting in SSC failure modes should be included in the Level 1 PSA model. If the combined hazards have different failure mechanisms, the failures should be represented by the individual hazard fragilities. If the combined hazards have similar failure mechanisms, the compounded fragility should be considered.

Natural hazards

Seismic hazards

8.72. The initial list of SSCs for seismic fragility analysis should include all SSCs that are included in the Level 1 PSA model for internal initiating events. The list should be expanded to include all SSCs 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.

8.73. The seismic equipment list should be supplemented by any SSC associated with any combined hazard identified in para. 6.10 and retained in the analysis. Depending on the retained combined hazard this may include dams, tsunami walls, internal flooding sources or internal fire sources identified systematically. Details on the development of the seismic equipment list are provided in Ref. [33].

8.74. All realistic failure modes of SSCs 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. The walkdown will enable to the following:

- Screening of inherently seismically rugged equipment items from the seismic model;
- Identification of correlation considerations (e.g. identical equipment with the same configuration, orientation or anchorage on the same level of the same building;

[39] In this context, fragility is the conditional probability of failure of a system, structure or component for a given hazard input level.

- Examination of operator response pathways for potential seismically induced interference;

- Identification of equipment or structures that are not included in the seismic equipment list, but whose structural failure could potentially impact nearby items that are on the list (i.e. seismic interaction concerns);

- Consideration of issues related to seismically induced fire and seismically induced flooding.

8.75. 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 Refs [26, 33].

8.76. 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. Examples are provided in Ref. [35].

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

8.78. The potential for seismic interaction (e.g. the possibility that SSCs could fall onto a seismic equipment list item), including the potential for additional interactions with fire and flooding, should also be a focus of the walkdown.

8.79. 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.

8.80. When SSCs 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.

8.81. The seismic responses of SSCs 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).

8.82. 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 SSCs located in different buildings.

8.83. For all SSCs 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.

8.84. For structures that are not founded on rock, soil structure interaction analysis, including the embedment effect and ground motion incoherence function, is needed. Even for structures that are founded on rock, performance of soil structure interaction analyses with consideration of ground motion incoherence will have the benefit of computing realistic seismic response

and potentially lowering the response spectra peaks in the high frequency range, which are expected to arise owing to the high frequency content of the uniform hazard response spectra.

High winds

8.85. 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 might 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.

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

8.87. In evaluating wind related fragilities of SSCs, plant specific data should be used. Any structures that could fall into or onto structures that are important to safety, thereby causing damage, should be considered in the assessment. In this assessment, findings from plant walkdowns should be used as an important source of information, for example to justify any modelling parameters.

8.88. A family of fragility curves corresponding to a particular failure mode for each SSC 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 SSCs. More details on fragility analysis for high winds are given in Ref. [30].

External flooding

8.89. 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. The probability of dam failures should be calculated for different levels in the river. [40]

8.90. In assessing fragilities of SSCs in respect of external flooding, plant specific data should be used. Any structures that could fall into or onto structures important to safety, thereby causing damage, should be considered in the assessment. Findings from plant walkdowns should be used as an important source of information in the assessment. All structures located at low levels, in particular intakes and ultimate heat sinks, should be included taken into consideration.

8.91. The fragility analysis should include immersion, dynamic loads on SSCs from waves, and foundation failures (soil erosion). More details on fragility analysis for external flooding are given in Ref. [30].

Other natural hazards

[40] It is typical to assume dam failure for a river level above the dam failure design level.

8.92. The general aspects and recommendations for the fragility analysis of seismic, hydrological and meteorological hazards should be followed for other natural hazards as applicable.

Human induced hazards

8.93. The general aspects and recommendations for the fragility analysis natural hazards should be followed for human induced hazards as applicable. More details on fragility analysis and capacity analysis for aircraft impact and for explosions and releases of hazardous substances are given in Ref. [30].

INTEGRATION OF EXTERNAL HAZARDS IN THE LEVEL 1 PSA MODEL

General aspects

8.94. 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.

8.95. 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.

8.96. The assessment of type C human failure events for external hazards should include the following:

(a) Human failure events that are included in the Level 1 PSA for internal initiating events but are also relevant to the hazard scenario. In such cases, it might be necessary to revise the assessment of performance shaping factors as it might be more difficult for operating personnel to implement actions than in the base case scenario.
(b) Human failure events that are relevant only to a specific external hazard (e.g. those related to relay reset after seismic events). In such cases, the methods used to assess external hazard specific human failure events can usually follow the same principles as the ones used to analyse other types of human failure event.
(c) Undesired responses by operating personnel to spurious alarms and indications.

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

Natural hazards

Seismic hazards

8.98. 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 Refs [27, 33].

8.99. At many plants, manual shutdown of the plant 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.

8.100. 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 types 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 caused by 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.

8.101. 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 owing to the impact of a seismic event on the reactor core, should be considered.

8.102. 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.

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

8.104. 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 owing 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.

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

8.106. 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 owing to the impact of seismic events of a 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) Accessibility of plant locations where actions need to be taken by personnel to ensure the required safety functions or to rescue people;
(b) Increased stress levels;
(c) Failures of indication or false indication;
(d) Failures of communication systems;
(e) Other applicable factors impacting the behaviour of operating personnel.

8.107. In quantifying the core and/or fuel 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.

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

High winds

8.109. 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.

8.110. The consideration of accident sequences initiated by high winds should include site specific hazard curves and the fragilities of all structures for which damage might lead to the disabling of the equipment modelled in the Level 1 PSA. Other factors to be considered should include unavailability or failure 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. 8.96.

External flooding

8.111. 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 might lead to the disabling of the equipment modelled in the Level 1 PSA. Other factors to be considered should include unavailability or failure 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. 8.96.

8.112. Uncertainties, dependencies and correlations should be taken into full accounted in developing accident sequence models for initiating events induced by external flooding.

Other natural hazards

8.113. The general aspects and recommendations for model integration of seismic, hydrological and meteorological hazards should be followed for other natural hazards.

Human induced hazards

8.114. 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

8.115. In accordance with Requirement 20 of GSR Part 4 (Rev. 1) [3], the screening analysis, bounding analysis and detailed analysis for Level 1 PSA for external hazards should be documented in a manner that facilitates their peer review, as well as future updates 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 and methods used, the 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 assessment 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 also be followed.

8.116. The following major outputs of the Level 1 PSA for external hazards should be presented:

(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.

Natural hazards

Seismic hazards

8.117. 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.

8.118. 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 its technical basis 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.

8.119. The basis for screening out any SSC should be described fully.

8.120. 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.

8.121. 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

8.122. The Level 1 PSA for high winds should be documented in a manner that facilitates its review, application and update. 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 were 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 flooding

8.123. The Level 1 PSA for external flooding should be documented in a manner that facilitates its review, application and update. 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 flooding;
(b) A description of changes made in the Level 1 PSA model to take into account effects relating to external flooding;
(c) A list of all SSCs considered in the analysis along with justification for the SSCs that were screened out from the analysis;
(d) The methodology and data used to derive flooding 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

8.124. The recommendations for documenting and presenting results provided in paras 8.115–8.123 should be followed, as applicable.

Human induced hazards

8.125. The recommendations for documenting and presenting results provided in paras 8.115–8.123 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 (Rev. 1) [3] for a Level 1 PSA for shutdown states[41] 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 operation 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

[41] For low power operation, all the recommendations provided in Sections 2–8 are applicable with due account taken of the potential reduced power level and different interlocks and system configurations compared to power operation.

analysis is not necessarily the determination of core damage frequency, since fuel damage frequency and inadvertent criticality might also be risk metrics of interest.

9.2. Internal and external hazards can be as important for shutdown states as for power operation 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; external explosions and external flooding 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;
(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. [36].

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[42], during which major maintenance activities are also carried out;
(b) Planned outages, during which only specific maintenance activities are carried out;[43]
(c) Unplanned outages that follow a disturbance during power operation with and without drainage of the reactor vessel and fuel reloading.

[42] For plant operating states with refuelling outages during which the fuel is completely relocated into the spent fuel pool, the recommendations provided in Section 10 apply.

[43] All standard planned shutdown and startup conditions are generally considered among the different plant configurations.

These are reflected in the plant's technical specifications, which are usually divided in accordance with the plant's various 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 continued until a safe and stable state is reached. Termination of the analysis at a predefined sequence mission time might 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 case of an outage planned specifically for maintenance activities, a comparison of the risk associated with the planned outage against 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 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) Level of decay heat;
(c) Temperature and pressure in the reactor coolant system;
(d) Other relevant power dependent parameters (e.g. pressurizer level, water level in the primary system, steam generator level);
(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 credited systems, including support systems, and 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 outage type selected 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 showing the selection of plant operating states is included in Annex III, in which 11 different plant operating states have been differentiated. For Level 1 PSA for shutdown, however, 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 the time needed for different operations for different types of outage should be performed. This information should be verified and updated at the 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 5.13–5.22. 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 are defined with reference to 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 spent fuel pool either internal or external to the reactor building is covered separately in this Safety Guide as part of the PSA for the spent fuel pool (see Section 10). 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 state of the accident sequences in a Level 1 PSA for shutdown states; such end states are often referred to as fuel damage states or criticality events. Examples of initiating events in a PSA for shutdown states for CANDU-type reactors are provided in Ref. [36]. A decision should be made as to which of these 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. The characteristics of such 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 states:

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

9.14. Care should be taken 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 paras 5.13–5.22, 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 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 the 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.

Publicly available sources of such information include the following:

(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 such 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 following criteria form the basis for grouping initiating events in shutdown states:

(a) All initiating events in a group have a similar effect on the availability and operation of credited SSCs.
(b) All initiating events in a group have similar success criteria for credited systems.
(c) All initiating events in a group impose similar operator action requirements.

Similar initiating events can occur in different plant operating states (see Annex III), but as the availability of systems and the success criteria are generally different in these different 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. 5.34).

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 5.149–5.152. However, the quantification of initiating event frequencies for shutdown states should take into account the higher possibility of initiating events caused by human failure events, so human reliability analysis methods should also be 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 owing to events relating to the occurrence of the plant operating state, rather than its duration (e.g. some initiating events might 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. If some initiating events are screened out of further analysis owing to a low occurrence frequency attributable to the low fraction of duration of relevant plant operating states, then this assumption should be revisited and justified if the Level 1 PSA is being used for risk monitor applications.

9.22. There are basically three approaches to quantifying the frequencies of initiating events occurring in a given plant operating state (see paras 5.149–5.152), as follows:

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

9.23. 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.

9.24. 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 and success criteria

9.25. Recommendations on the general approach to accident sequence analysis are provided in paras 5.40–5.68. Although decay heat levels during shutdown are generally much lower than immediately following shutdown from power operation, the characteristics of the possible plant configurations might still give rise to events that challenge the fulfilment of safety functions. The analysis should take into account the following aspects:

(a) As a result of disabling the automatic actuation of 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.
(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.

9.26. Functional performance criteria should be used to specify success criteria for the various systems, which might differ from the success criteria specified for a Level 1 PSA for power operation.

Analysis to support the specification of success criteria

9.27. 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.

9.28. 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, so the 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, at a minimum, take into account the following factors:

(a) 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;
(j) Availability of protection systems for actuation of safety functions.

9.29. 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

9.30. Event trees (see paras 5.58–5.62) 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.

9.31. 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.

9.32. 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 states and plant damage states

9.33. For shutdown states, 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.

9.34. 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. 5.65). 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 (based on time since shutdown from power operation);

(b) Containment state, especially when the containment is open;
(c) Conditions that determine the time taken to restore containment isolation and the potentially reduced effectiveness (leaktightness) of the containment during this time;
(d) Integrity of the primary system pressure boundary with vessel head removed, nozzle dams installed, safety valves removed and primary system vent open;
(e) Water inventory in the primary circuit.

9.35. Appropriate specification of the plant damage state will be decisive for the results and their interpretation.

SYSTEMS ANALYSIS

9.36. 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 5.71–5.82) 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 might be configured differently to accommodate maintenance or the specific alignment of the system might change the 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 mission times needed for different systems are 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 it was not necessary for power operation.
(i) Interconnection of particular systems is necessary to establish a configuration for a safety function that is used only in shutdown states, for example, using the spent fuel cooling system for core cooling; account should be taken of the procedure to be followed for such interconnection.
(j) A particular system was not modelled as this would only be necessary for the Level 2 PSA for power operation.

Examples of specific system modelling requirements are given in Annex III.

ANALYSIS OF DEPENDENT FAILURES

9.37. As described in paras 5.86–5.91 for power operation, the objective of this analysis is to identify dependencies that might 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 all be included in the analysis.

9.38. 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 might create new sources of dependencies, such as coincident repairs or maintenance of redundant components that should be taken into account. Examples are presented in Annex III.

9.39. Revisions to the dependency models for power operation should be implemented as necessary, especially if the success criteria are different for shutdown states, or the conditions for support systems (e.g. ventilation systems, power supply systems) are different.

9.40. The alignment of systems and component outages should also be reviewed.

9.41. 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

9.42. In paras 5.96–5.121, 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 consistent both with one another and with the analysis performed in other portions of the Level 1 PSA.

9.43. Typical aspects during shutdown, such as extensive use of maintenance staff from external organizations, frequent overtime work and increased control room work, should be adequately considered in the analysis. Account should also be taken of difficulties in work supervision and pressures owing to tight schedules.

9.44. For human reliability analysis, close interaction between the human reliability analysts and 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 analysts should attempt to gain knowledge on the basis of practical experience from the operation of similar plants.

Type A human failure events — pre-initiator human failure events

9.45. Type A human failure events (see para. 5.102) consist of actions associated with testing, maintenance, repair and calibration that, if not performed 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 time constraints, leading to a high potential for human errors.

(b) There might be reduced availability of automatic realignment functions (e.g. no automatic closure signal for a valve left open after a test).

Type B human failure events — human failure events that might cause an initiating event

9.46. 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 owing 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 might 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 5.114–5.118.

Type C human failure events — post-initiator human failure events

9.47. 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.

9.48. 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. Such aspects as the following might differ from the PSA for power operation:

(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 shutdown states.

9.49. Values generated by the use of time reliability correlations specific to power operation should be adopted with caution, since the time windows in shutdown states might be well outside the applicable ranges of such correlations.

9.50. 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.

9.51. As in a Level 1 PSA for power operation, dependencies between human failure events in the same accident sequence should be taken into account (see paras 5.119 and 5.120). 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 might lead to increased failure probability compared with the case where loss of function was a result of mechanical failure.

DATA ASSESSMENT

9.52. The data necessary for quantification of the Level 1 PSA for shutdown conditions include 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) Unavailability owing to maintenance, including overlapping maintenance based on operating history;
(g) Assessment of common cause failures.

The basic needs and approaches for data acquisition described in Section 5 also apply to shutdown states. Since data for the quantification of component reliability parameters specific to shutdown are less widely available than data for power operation, however, a widely used approach is to adapt data from power operation. This should not be done without transparent justification as regards the applicability of such data.

9.53. Data assessment in relation to maintenance and testing activities should be reviewed for the different configurations; while certain activities might be conducted throughout the outage, others might only be conducted in certain configurations. Also, maintenance and testing frequency might change depending on the configuration.

9.54. A major objective of testing during planned outages is to verify the correct functioning of equipment that has undergone maintenance, before it is put back into operation. The unavailability of this equipment should be determined on the basis of the average test duration and the duration of the plant operating state during which the component is being tested.

9.55. Possible human interactions and probability of human errors in overriding alignments resulting from test and maintenance activities should be assessed.

9.56. The possibility of repair should be considered because it can significantly increase the availability of credited systems in plant operating states for shutdown conditions. Neglecting repair might, 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.

9.57. Dependency of repair times on the plant operating state should be taken into account. Such dependencies might be related 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.

9.58. An appropriate reliability model should be selected in shutdown states to take into account that the components on standby during power operation might be in operation during an outage.

9.59. Component 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. Component mission times can have a significant impact on the calculated probabilities of system failure. Assumptions regarding the mission times of components should be consistent with the modelling of accident sequences (i.e. with the sequence mission time and system mission times), as well as with reliability data, as these might reveal a sensitivity to operation time.

9.60. If foreseeable changes in outage procedures are to be incorporated in the analysis, this might have implications for 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

9.61. For a Level 1 PSA for shutdown states, the quantification of accident sequences should be performed using the same techniques as for a Level 1 PSA for power operation. The use of other techniques, such as Markovian techniques instead of standard fault tree and event tree evaluation methods, might yield more realistic results for shutdown states in which long sequence mission times make it possible to credit recovery actions.

9.62. When reviewing the results of the quantification, as in the case of a Level 1 PSA for power operation, the minimal cutsets obtained should be carefully reviewed. In a Level 1 PSA for shutdown states, the system models might have to be modified to reflect the conditions of the different plant operating states. If the system models are modified, the minimal cutsets obtained for similar accident sequences or systems in different plant operating states should be cross-checked to ensure that any differences in them do indeed reflect the different plant operating states or sequence characteristics and do not stem from modelling errors.

IMPORTANCE ANALYSIS, SENSITIVITY STUDIES AND UNCERTAINTY ANALYSIS

9.63. For the uncertainty analysis for shutdown states, the same techniques should be used as for a Level 1 PSA for power operation (see paras 5.179–5.181).

9.64. Importance analysis and sensitivity studies should also be performed using the same techniques as for a Level 1 PSA for power operation (see paras 5.171 and 5.174–5.178).

9.65. 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 the PSA for shutdown states. For example, the specific conditions that were selected to characterize a plant operating state might represent a wider range of conditions that can actually occur during the plant operating state. Compared with PSA for power operation, there might be different

combinations of systems that are unavailable; some combinations might result from more conservative analysis and some from less conservative analysis. The plant operating state might have a longer or shorter duration. The 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

9.66. In accordance with Requirement 20 of GSR Part 4 (Rev. 1) [3], the Level 1 PSA report should include the procedures for performing a Level 1 PSA for power operation, along with sections on aspects that are particular to Level 1 PSA for shutdown conditions, such as a section describing in detail the process used for identification of outage types, plant operating states and initiating events.

9.67. The results obtained at 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.

9.68. Frequently, written maintenance or operating procedures are improved or introduced in response to preliminary analysis findings. Any such changes should also be outlined in the documentation.

9.69. 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 — 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.

9.70. The presentation of the engineering insights and the recommendations should be such that they provide clear input to the decision making process.

9.71. 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.

9.72. 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.

9.73. 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.

9.74. In addition to core damage frequency, other undesired end states, for example, involving criticality or damage to the fuel pool and their frequencies should be assessed and the results documented.

9.75. 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.

9.76. Documentation should be drawn up in accordance with regulatory review requirements.

10. SPECIFICS OF LEVEL 1 PSA FOR THE SPENT FUEL POOL

10.1. In principle, the Level 1 PSA for the spent fuel pool is based on the same methodology as the 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 in this section are relevant to both the PSA for the reactor and the PSA for the spent fuel pool.

UNDESIRED END STATES

10.2. The undesired end states of interest regarding the Level 1 PSA for the spent fuel pool should be clearly defined. If they have been specified in national regulations or guidelines, the national probabilistic safety goals or criteria applicable to the spent fuel pool should be the basis for specifying the undesired end states of interest.

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 the absence of detailed thermohydraulic analyses, fuel uncovering (i.e. when the water level in the spent fuel pool

drops below the top of the active part of the fuel assemblies stored or handled in the spent fuel pool as a result of boiling or draining) may also be applied as a criterion to assume fuel damage.

10.4. Beyond fuel damage, fuel uncovering 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 state.

10.5. If necessary for risk assessment, the damage of fuel assemblies to a predefined degree should be considered to determine the main end point of interest. Mechanical damage of a limited number of fuel rods or of one single fuel assembly during refuelling operations may be screened out from further assessment, if it can be justified that these events will not lead to a large radioactive release.

10.6. Gross mechanical fuel damage owing to internal hazards such as heavy load drops or falling objects (including as a consequence of hazard induced structural failures) or hazard combinations should also be considered as an undesired end state, since such events can challenge the design basis limits for the fuel.

PLANT OPERATING STATES

10.7. The modelling of all risk relevant plant operating states may need to cover a large variety of spent fuel pool configurations together with the associated scheduled maintenance activities and changes in residual heat levels. Similar plant operating states should be grouped together to limit the number of 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 operating states:

(a) The water inventory of the spent fuel pool;
(b) The residual heat of the fuel assemblies stored in the spent fuel pool;
(c) The spent fuel pool system configuration (i.e. whether the pool is isolated from or connected to the reactor);
(d) The storage position of fuel assemblies in the spent fuel pool (e.g. in a lower rack or an upper rack, depending on the design);
(e) The handling activities performed;
(f) The availability and scheduled maintenance of credited systems;
(g) Potential recovery actions and repairs;
(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 Level 1 PSA for the spent fuel pool are as follows:

(a) Loss of cooling (i.e. failure of spent fuel pool heat removal system);
(b) Loss of coolant (e.g. pipe rupture in the spent fuel pool heat removal circuit);
(c) Loss of off-site power;
(d) Inadvertent draining (e.g. owing to erroneous human intervention);
(e) Reactivity accidents (e.g. boron dilution, fuel loading errors)

(f) Initiating events induced by internal hazards that might lead to failure of the spent fuel pool heat removal system (including pipe ruptures as sources of internal flooding in systems other than the heat removal circuit), loss of spent fuel pool inventory or falling of objects onto the fuel assemblies in the spent fuel pool as a result of lifting activities;
(g) Initiating events induced by external hazards that might lead to failure of the spent fuel pool heat removal system, loss of spent fuel pool inventory or falling of objects onto the fuel assemblies in the spent fuel pool as a result of hazard induced structural failure;
(h) Initiating events induced by combinations of hazards that might lead to the consequences described in (f) and (g) above.

ACCIDENT SEQUENCE ANALYSIS

10.10. In the accident sequence analysis, the possibility of actions by operating personnel aimed at recovering the spent fuel pool cooling system 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 activities involved in recovering the spent fuel pool cooling system, recovery from pipe ruptures and recovery from loss of off-site power (e.g. repair of the failed component) should be taken into account in the assessment. For estimating the time to recovery, the initial water inventory in the spent fuel pool, the residual heat of the fuel assemblies stored in the spent fuel pool and 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 components or resources of credited systems (including water inventories) and shared human resources in the case of common initiating events. Interactions between the spent fuel pool and the reactor core should also be considered, for example flooding effects, structural loads owing to external hazards or other phenomena and draining events when spent fuel pool and reactor are connected.

10.13. When modelling loss of coolant accidents in the spent fuel pool, flooding should be considered as a consequential hazard. The timely isolation of isolable piping can then be credited to avoid a flooding impact (e.g. the long lasting failure of the spent fuel pool heat removal system). The failure (including the break) of siphons should also be considered in accident sequence analysis for loss of coolant initiating events.

10.14. The accident sequence analysis should consider that boiling can cause pump cavitation which might prevent successful restart of the cooling system(s) and/or might disable local actions owing to degraded ambient environmental conditions (including air temperature and radiation level) in the vicinity of the spent fuel pool.

10.15. For spent fuel pool accident sequences involving a large water inventory and low power level, slow accident progression should be considered in defining the sequence mission time, which can then be relatively long to allow for reliable recovery actions and repairs. Termination of the analysis at a predefined sequence mission time might prevent meaningful results from being obtained.

HUMAN RELIABILITY ANALYSIS

10.16. The slow accident progression in the case of loss of cooling events in the spent fuel pool enables the participation of multiple actors in the diagnosis and decision making processes and in the execution of recovery actions and repairs. This should be taken into consideration when defining performance shaping factors that mostly affect the failure probability of recovery actions[44] in these situations.

10.17. The emergency operating procedures may be developed to a different level of detail for spent fuel pool accidents than for reactor core accidents. This difference might influence human reliability when responding to an accident and should be considered when carrying out human reliability analysis for the Level 1 PSA for a spent fuel pool.

10.18. Potential dependencies between human actions to prevent undesired end states for the spent fuel pool as well as for the reactor core should be considered. In addition, the aggravating effects of increased workload on operating personnel mitigating concurrent accidents simultaneously should be considered when assessing the relevant human error probabilities.

QUANTIFICATION OF THE ANALYSIS

10.19. All the recommendations provided in paras 5.160–5.170 are applicable to a Level 1 PSA for the spent fuel pool. In addition, the PSA models for fuel in the reactor core and in the spent fuel pool should be integrated in order to correctly model dependencies of any shared systems. This is particularly important for initiating events that affect both the reactor core and the spent fuel pool simultaneously and for a subsequent Level 2 PSA (in particular for plants with the spent fuel pool inside the containment).

INTERPRETATION OF THE RESULTS

10.20. The combined or separate interpretation of risk from accidents involving the spent fuel pool and the reactor core should be consistent with the probabilistic safety goals or criteria specified in national regulations or guidelines.

10.21. There is no international consensus on whether or not to aggregate the results of the Level 1 PSA for the spent fuel pool with those of the reactor.[45]

10.22. 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 those of the reactor should be considered, rather than simply summing these estimates (i.e. similar to the method used for aggregating multi-unit or site core damage frequencies, see Section 11).

[44] Recovery actions can be credited only in the case of slow accident progression, with a sufficient time window and information available for operators to implement these actions.

[45] 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 (see, e.g., paras 5.7, 5.20, 7.37, 7.72). The recommendations provided in this section are related to the development of a Level 1 multi-unit PSA (MUPSA) which is aimed at quantifying multi-unit risk metrics.

11.2. The MUPSA model is typically developed on the basis of single unit PSA models and takes into account the specifics of each unit under consideration.

MUPSA SCOPE

11.3. As described for PSA in general in para. 2.2, the scope and the need for MUPSA should also be correlated with the probabilistic safety goals or criteria, if they have been specified in national regulations or guidelines.

11.4. The scope of MUPSA should include all risk significant multi-unit initiating events[46] and hazards, as well as all 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, screening may be performed if necessary, on the basis of the review of single unit PSA results.[47]

MUPSA RISK METRICS

11.5. Risk metrics additional to those used in single unit PSA (e.g. core damage frequency) should be developed in order to express the risk profile in the context of multi-unit nuclear power plants, for related decision making purposes. For example, the following risk metrics 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 to only one reactor on a multi-unit site;
(b) Multi-unit core damage frequency: frequency per site-year of an accident involving core damage to two or more reactors on a multi-unit site;
(c) Site core damage frequency: frequency per site-year of an accident involving core damage to one or more reactors on a multi-unit site;
(d) Multi-source fuel damage frequency: the frequency per site-year of an accident involving fuel damage in two or more sources (e.g. 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.

[46] 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.

[47] Depending on the scope of the PSA, for risk aggregation, multi-unit aspects as well as potential effects from other sources of radiation collocated on the site (e.g. interim fuel storage facilities, nuclear waste treatment facilities) might be also considered within the PSA.

PLANT OPERATING STATES

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 in power operation and shutdown states, as well as spent fuel pools in different plant operating states. Some combinations may be eliminated on the basis of plant operating practices, for example not refuelling two units 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, the various plant operating states should be grouped. This grouping should be done in such a way 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. In a MUPSA, multi-unit initiating events should be screened, taking into account their risk significance. 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 grouped initiating events could potentially have a different impact on a multi-unit plant.

11.12. For a MUPSA, event frequencies that are dependent on the combination of plant operating states should be calculated, taking into account the probability of the combination (see also para. 11.9).

SYSTEMS ANALYSIS

11.13. SSCs and resources that are shared among the units should be explicitly modelled in MUPSA.

11.14. The availability of 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 the MUPSA systems analysis.

HUMAN RELIABILITY ANALYSIS

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 owing to site level

accident conditions, shared human resources, work in the shared control rooms (as 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 dependency 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 accidents in one or more units on site simultaneously, the adverse effects on the control and accident management of the other units should be considered, taking into account factors connected with severe accidents at other units on the site (e.g. radiological releases, 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 hazard 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 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 takes into account aspects of multi-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 LEVEL 1 PSA

GENERAL ASPECTS OF PSA APPLICATIONS

12.1. This section discusses a number of PSA applications practised in individual States on the basis of their national safety policies and regulations, and provides recommendations on meeting the following requirements:

— Requirement 23 of GSR Part 4 (Rev. 1) [3] in relation to the general use of PSA;

— Requirements 6, 10, 16, 42 of SSR-2/1 (Rev. 1) [2] in relation to the use of PSA in the design of nuclear power plants;

— Requirement 22 of SSR-2/1 (Rev. 1) [2] in relation to the use of 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 [37] in relation to the use of PSA for testing and maintenance optimization;

— Requirement 12 of SSR-2/2 (Rev. 1) [37] in relation to the use of Level 1 PSA for periodic safety review;

— Requirement 8 of SSR-2/2 (Rev. 1) [37] in relation to the use of Level 1 PSA 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 related to the safety of the plant in order to prioritize and optimize design and safety related activities so that they focus on areas with 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 goals 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. It should be fully documented so that the analysis can be traced back to details of the design and supporting analysis.[48]

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 performed 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. The PSA models and, if necessary, the PSA applications should be periodically updated throughout the lifetime of the plant to consider attributed changes in design, operational practices, operational experience and other issues that influence the parameters modelled in the PSA.

12.7. 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 (i.e. internal initiating events, internal hazards and external hazards) and plant operating states to the PSA results. In particular, it should be recognized that the aggregation of various risk contributors (e.g. hazards, plant operating states, facilities) implies a certain level of heterogeneity in terms of the level of details, resolution, inherent conservatism and uncertainties for individual contributors. Such heterogeneity might lead to misleading insights from the PSA and should therefore be taken into consideration during decision making.[49] This is of particular importance for PSA applications that rely on the evaluation of importance measures and for risk monitor type applications. Therefore, it is highly recommended to calculate the risk importance of the various equipment separately for each risk contributor. As an example, risk importance

[48] The quality attributes of Level 1 PSA models essential for particular PSA applications are provided in Ref. [38].

[49] 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 might be significantly larger than those associated with internal events.

measures for seismic events and internal events should be calculated separately.

12.8. In deriving risk insights from the PSA, care should be taken to consider major sources of uncertainties, and a sensitivity analysis of the main assumptions might need to be conducted.

12.9. For Level 1 PSA applications at operating plants, the techniques involved and the implications of the PSA should be adequately communicated to plant management so that they develop an integral understanding of their associated management responsibilities.

12.10. The Level 1 PSA results, along with 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 applications would build an awareness of how to manage the risks.

12.11. How well the PSA model reflects the as built and as operated plant so that the management might have confidence in the PSA results, is one of the most important attributes for many PSA applications (see Refs [38, 39]).

12.12. Paragraph 4.32 of SSR-2/2 (Rev. 1) [37] states that "If a probabilistic assessment of risk is to be used for decision making purposes, the operating organization shall ensure that the risk analysis is of appropriate quality and scope for decision making purposes." The risk analysis should therefore 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 PSA concepts and methods so that the results can be interpreted properly.

SCOPE OF LEVEL 1 PSA APPLICATIONS

12.13. In accordance with Requirement 4 of GSR Part 4 [3] the safety assessment should include 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, power operation, 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 Level 3 PSA might be necessary.

12.14. In many cases, the scope of the PSA that is necessary to support a specific application might 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.[50]

12.15. 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

[50] For example, if the Level 1 PSA does not contain an analysis of internal fire, it is not feasible to use the PSA insights in relation to cable routing.

should be identified and the impact on the results of the PSA should be assessed.

12.16. For multi-unit nuclear power plants, the national safety policy or regulations might require the risk associated with multiple units to be used in risk informed decision making. In such cases, either the insights from a MUPSA should be used (if available) or the insights from a PSA which appropriately considers multi-unit interactions from single unit perspectives (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

12.17. 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 (see Refs [9, 13]):

(a) Any mandatory requirements that relate to the PSA application under consideration (e.g. legal requirements or regulations);
(b) The insights from deterministic safety analysis (e.g. whether the provisions of defence in depth requirements are being met, whether there are adequate safety margins, whether lower level requirements such as the provision of sufficient levels of redundancy and diversity in the SSCs that perform safety functions are being met, whether the equipment in the plant has been qualified to a sufficient level that it can withstand the harsh environments that would follow initiating events);
(c) Any other applicable insights or information (e.g. a cost–benefit analysis, details of the remaining lifetime of the plant, inspection findings, operating experience, doses to workers from making changes to the plant).

12.18. When applying PSA in a risk informed approach, any decisions should be made in a balanced manner, with all relevant factors are taken into account. The remainder of this section does not cover all possible PSA applications; only those most commonly used in individual States.[51]

USE OF PSA FOR DESIGN EVALUATION

12.19. The PSA should be used to provide 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 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. To meet Requirement 20 of SSR-2/1 (Rev. 1) [2], when applicable, the Level 1 PSA model for internal initiating events should be used to confirm the set of design extension conditions without significant fuel degradation that should be deterministically derived

[51] Examples of publications providing additional information on PSA applications 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].

as per para. 3.40 of SSG-2 (Rev. 1) [5].

(c) The PSA should be updated throughout the 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 lifetime extension, and to provide insights into whether proposed design modifications and operating changes are adequate.

(e) The PSA should be used in 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, Safety Assessment for the Decommissioning of Facilities Using Radioactive Material [40])

Use of PSA to support decisions made during the design of a nuclear power plant

12.20. To obtain maximum benefit, the PSA used for design evaluation should be a full scope PSA as specified in para. 12.13. 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.

In accordance with para. 5.76 of SSR-2/1 (Rev. 1) [2], the design is required to take due account of the PSA for establishing that a balanced design has been achieved, preventing cliff edge effects and comparing the results of the analysis with the acceptance criteria for risk. The cliff edge effects should be tested in the analysis results in the form of sensitivity studies by varying a set of analysis input data that have the potential to be risk significant.

12.21. Insights from the PSA allow the design of a new plant to be optimized in terms of risk metrics and cost. The results of the PSA should be used to provide an approach for determining the following:

(a) Whether the credited systems have adequate levels of diversity and redundancy;

(b) Whether there are sufficient levels of equipment qualification for SSCs that experience harsh environments 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.

12.22. The results of the PSA should also be used to determine the need for additional measures to be incorporated to reduce risk.

12.23. The PSA includes an investigation of variants and exploratory design options, the sufficiency of the redundancy and diversity of systems and, to a certain extent, reflects emergency arrangements and accident management measures. The results of the PSA should

be used to provide an input to enhance the emergency arrangements[52] and accident management measures. The PSA results should also be used to allocate reliability and availability targets for SSCs to meet probabilistic safety goals or criteria, thereby forming part of the design specification. In addition, the PSA should be used as a support tool to select or modify design basis accidents and design extension conditions and to define general design criteria. The PSA may also be used to provide an input to cost–benefit analysis.

12.24. When applying PSA to the design of a nuclear power plant, particular effort should be made to correctly reflect new design features that might not be addressed in previous PSAs (e.g. unique initiating events, failure modes, common cause failures, specific event sequences, dependencies).

12.25. In a PSA conducted at an early design stage, the for the fact that additional assumptions are needed owing to lack of design and operating details should be documented, and the validity of these assumptions should be checked at a later stage in the design (e.g. at the construction or pre-operational stage).

12.26. Uncertainties in input information, data 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.

12.27. 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 should be done for the minimal cutsets that make significant contributions to core or fuel damage frequency in order to identify the initiating event groups, component failures and human failures events that make the greatest contribution 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.

12.28. The contribution of individual groups of initiating events to the core damage frequency or fuel damage frequency, and the contribution of minimal cutsets for individual groups to the core damage frequency or fuel damage frequency should be used to determine whether the design of the plant is balanced, i.e. to ensure that no particular group of initiating events and no particular accident sequence within the group makes an unduly large contribution to the core damage frequency or fuel damage frequency.[53]

12.29. 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 (excluding configurational basic events used to control system configurations in a particular plant operating mode), which might indicate that the single failure requirement is not being met for the design.

12.30. The list of dominant minimal cutsets should be reviewed to determine whether

[52] It is understood that the PSA might not be able to address the entire spectrum of aspects related to the effectiveness of emergency arrangements. The input expected from the PSA is related to aspects such as the timing and dynamics of accident sequences, the most risk significant scenarios and detailed information about the context during the scenario (e.g. devastation on site, release details).

[53] International practice shows that it can be difficult to achieve this objective for external hazards, especially for new designs, where the core damage frequency values could be relatively low for internal initiating events.

there are opportunities to enhance defence in depth if any deficiencies are identified.

12.31. Importance measures for basic events, groups of basic events, credited systems and initiating event groups, should be calculated and used to interpret the results of the PSA.[54] A high Fussell–Vesely importance value or Birnbaum importance value for an independent failure event might 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 might 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 might indicate insufficient diversity of 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 a complementary manner to support decisions during plant design.

12.32. Where multiple units and/or sources are collocated at a site, the impact of one of these on nuclear power plant units on the others should be considered in risk informed design optimization process to support reduction of the risk significance of such impact.

12.33. PSA results and insights are dependent on design features and provisions (including human interactions and associated procedures) that are credited in the PSA. The actual use of these features and provisions to achieve acceptably low risk estimates at the pre-construction stage should be verified in the PSA performed before applying for an operating licence. If any discrepancies leading to higher risk are identified they should be reflected in the PSA and proposals for changes to reduce the risk should be made.

Use of PSA in the licensing process

12.34. An assessment of the overall plant safety is necessary for obtaining an operating licence and usually involves a full scope Level 1 PSA.[55] As part of this application, the results of the PSA should be compared with the probabilistic safety goals or criteria (where these have been defined). A safety evaluation for applying for a pre-construction licence may involve a limited scope PSA (e.g. using data from similar plants).

12.35. The overall results of the Level 1 PSA (usually the core damage frequency or fuel damage frequency) should be compared with the 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 whether a sufficient level of safety has been achieved for the plant, that is, whether sufficient credited systems have been incorporated in the plant design and whether adequate emergency, operating, maintenance and testing procedures are available to prevent core or fuel damage during operation.

12.36. The comparison of the results of the Level 1 PSA with probabilistic safety goals or criteria should begin at the concept design and be repeated at various points in the design, construction and operation stages to assist in safety, technical and organizational decision making and to check that the design remains adequate.

[54] For an explanation of the various importance measures, see para. 5.171.

[55] Different Member States have different requirements with regard to the scope of the PSA for licensing purposes, depending on the hazards and initiating events being considered and the location of the fuel (e.g. in the reactor, in the spent fuel pool, in fresh or irradiated fuel storage facilities).

12.37. In making the comparison described in para. 12.36, account should be taken of the results of the sensitivity studies and uncertainty analysis performed. These results will indicate the degree of confidence in meeting the criteria and/or goals and the likelihood that they have been met.

12.38. This application should include the provision of information during the pre-licensing process aimed at obtaining public acceptance for the construction and operation of the nuclear power plant.

Comparison of design options

12.39. When modifications are being considered for a nuclear power plant, there are usually a number of options available. The PSA should be used to provide an input into the comparison of these options. The way that this is done depends on the complexity of the modification being considered but could range from revising the PSA model to incorporate a proposed new credited system (for complex changes) to post-processing the minimal cutsets (for simpler changes). The PSA should provide an input to the integrated risk informed decision making process to determine which of the options to choose (see Refs [9, 13]).

12.40. 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 is always preferable.

Use of PSA in periodic safety review

12.41. Paragraph 4.46 of SSR-2/2 (Rev. 1) [37] states that "probabilistic safety assessment can be used for input to the [periodic] safety review to provide insight into the contributions to safety of different safety related aspects of the plant." The Level 1 PSA should be reviewed following the recommendations on safety factor 6 provided in IAEA Safety Standards Series No. SSG-25, Periodic Safety Review for Nuclear Power Plants [41].

12.42. The safety assessment process for this application should consist of identifying safety issues, assessing their safety significance and making decisions on the need for corrective measures.

12.43. In a periodic safety review, the PSA should be used to create an up to date overview of the whole nuclear power plant and to help in identifying cost-effective improvements to safety.[56] Consequently, the PSA should use plant specific data, model as built and as operated plant conditions and address the possible impact of ageing 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

[56] As a part of periodic safety review, the PSA could be used to support the extension of the lifetime of the plant, to support a cost–benefit analysis 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).

replaced.[57].

Optimization of protection against internal hazards and external hazards

12.44. The PSA for internal hazards and external hazards 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.

12.45. The PSA supporting optimization of the design against internal hazards and external hazards should be used to provide input for the following:

(a) Checking the robustness of the SSCs against internal hazards and external hazards, including containment (based on the results of PSAs for internal hazards and external hazards);

(b) Establishing criteria for equipment separation, cable tracing and plant layout (e.g. on the basis of the results of the PSAs for fire and flooding);

(c) Understanding hazard occurrence factors (e.g. critical locations of high energy lines, critical fire sources) and designing protective features (e.g. fire detection, fire mitigation, flood or fire barriers, external flooding protective measures);

(d) Establishing criteria for drainage, flood detection and isolation, and isolation of fire compartments;

(e) Identifying and reducing maintenance activities that can lead to fire or flooding events.

12.46. Uncertainties related to aspects important for the PSAs for internal hazards and external hazards 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, TESTING AND MAINTENANCE OPTIMIZATION

12.47. This section provides recommendations on meeting Requirement 31 of SSR-2/2 (Rev. 1) [37], which 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.

[57] Currently, the modelling of SSC ageing in the context of PSA is at an exploratory stage; ageing effects are typically addressed qualitatively.

"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.

[…….]

"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."

Risk informed technical specifications

12.48. The PSA should be used to provide a consistent basis for risk informing technical specifications, which specify the limits and conditions for plant operation and maintenance related to the risk significance of the affected plant features.[58]

12.49. If the PSA alone is being used to develop the technical specifications, then it should also be used to identify the equipment to be included in the technical specifications. In this way, equipment of high safety significance will not be left out from the technical specifications without limiting conditions for operation[59].

12.50. Insights from the PSA should be used as follows, as an input to establishing or verifying the measures to be implemented if an abnormal event that does not lead to immediate reactor scram occurs:

(a) At the design stage, the Level 1 PSA facilitates the quantification of risk associated with different allowed outage times (or other corresponding measures) and with any additional actions taken in response to the same abnormal event. These risks should be compared and the most risk beneficial option should be proposed for inclusion in the technical specifications. When quantifying such risks, the risks for continued operation during the allowed time and the risks after the measure has been implemented should both be taken into account.

(b) For an operating plant where the technical specifications and limiting conditions for operation are already available, the Level 1 PSA should be used to justify their appropriateness and to suggest revisions of allowed outage times (or other corresponding measures) where justification is not sufficient.

In both cases, a full scope Level 1 PSA should be used and modified as appropriate to take into consideration all aspects associated with a particular abnormal event or plant configuration. If the Level 1 PSA is of limited scope, it can 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

[58] The technical specifications determine the measures to be implemented if an abnormal event that does not lead to an immediate reactor scram occurs, along with the allowed outage times (or other corresponding measures) before implementation of these measures, and any additional actions necessary (e.g. additional testing requirements for redundant equipment, reduction of power level, disconnection of affected equipment, immediate repair of failed components). If the allowed outage times (or other corresponding measures) are exceeded, the technical specifications set out further actions to be taken by operating personnel. The technical specifications are typically based on deterministic requirements and engineering judgement.

[59] The 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 (referred to as configuration control).

negligible.

12.51. When 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.

12.52. The insights provided by the PSA should include the information necessary for comparison with the decision criteria or guidelines used to support the risk informing of the technical specifications. Examples of such information include 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

12.53. The surveillance test intervals determine the frequency of testing and sometimes the testing strategy for SSCs important to safety. PSA based evaluation of surveillance test intervals considers the risk from unavailability owing to undetected failures, and the risk from unavailability owing to tests and test induced failures.

12.54. The goal of this application is to optimize the surveillance testing strategy and intervals with respect to their impact on equipment reliability and overall risk estimates. Potential human errors that could occur during surveillance testing that might have an adverse impact on safety, for example by leading to plant trips and initiating events, are normally taken into consideration in optimizing the test intervals.

12.55. At the design stage, all SSCs that are included in the PSA model should be taken into consideration 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 human failure events during and after testing that can lead to unavailability of equipment or cause initiating events are reduced;

(d) The service test intervals do not lead to excessive unavailability of equipment owing to potential excessive wear of the tested components.

12.56. For an operating plant where service testing strategies are already available, the PSA should be used to justify their appropriateness and to suggest changes in service test intervals for the components that have the highest risk contribution and high risk importance values.

12.57. When quantifying such risks, the uncertainty in both mathematical models and data for tested components should be taken into account.

12.58. In providing input from the PSA for the optimization or justification of the service test 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 owing to frequent tests);

(b) Common cause failures with due account taken of the type of testing (i.e. staggered or non-staggered);

(c) The potential for human failure events, including errors of commission, during and after testing, leading to component unavailability and/or an initiating event.

12.59. For both new and operating nuclear power plants, a full scope PSA should be used to consider the impact of different service test interval strategies. If the PSA is of limited scope, it should only be used if it is demonstrated that changes in the service test interval strategy have a negligible impact on the risks associated with missing parts of the PSA.

12.60. The PSA model should explicitly model the unavailability of SSCs owing to testing and make it possible to predict the impact of changes to a service test interval on each affected SSC.

12.61. Risk importance measures should be used to prioritize and rank SSCs that are candidates for a change of service test 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 test interval.

12.62. 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 owing to human failure to properly restore normal alignments after testing should be taken into account. If it is known that a test might lead to a higher probability of an initiating event (initiating event frequency is related to test frequency) then this should be taken into account if the test frequency is changed.

Risk informed in-service testing

12.63. The current approach to in-service testing is to perform it in accordance with 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.

12.64. 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. A risk informed approach to in-service testing can allow the operating personnel to prioritize the components of various risk significance and has the potential to prevent undue adverse effects of testing on components and increase the availability of components while still maintaining a very high level of safety.

12.65. 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.

12.66. The risk information from the PSA should be derived using the Fussell–Vesely importance together with 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.

12.67. 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 multi-unit nuclear power plants.

12.68. 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.

12.69. 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-service and in-service inspection

12.70. The overall aim of the programme for pre-service and 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 inspections programme typically implemented is based on a traditional deterministic approach and engineering judgement. In the risk informed pre- and in-service inspection approach, it is assumed that the risk significance of the piping segment is determined through a combination of the assessment of qualitative or quantitative degradation potential and the assessment of the potential consequences of the piping segment failure (e.g. conditional core damage probability), which might be presented in the form of a risk matrix.

12.71. The risk informed approach should be used to provide insights from the PSA to revise the inspections programme (in terms of inspection frequency, methods used and sample size) to focus on those segments of pipework that have the highest risk significance and reduce the inspections performed on segments of pipework with a low risk significance. This is expected to lead to a reduction in the overall number of pipework inspections that are performed and a reduction in the associated occupational exposure, without increasing the risk estimates.[60]

12.72. At the design stage, the risk informed approach should be used to support the development of the inspection programme to prevent failures of the risk significant pipework. For operating plants, this programme should be maintained and updated on the basis of feedback from operating experience.

12.73. Insights from the PSA should be used as an input in determining the following:

(a) The pipework segments to be assessed by the risk informed pre-service and 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;

[60] Several approaches to carrying out risk informed in-service inspection have been developed; see Ref. [42]. Examples include methods recommended by the Electric Power Research Institute, the Pressurized Water Reactor Owners Group and the European Network for Inspection and Qualification.

(d) The change in the risk resulting from changes to the pre-service and in-service inspection programme.

12.74. 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 system train (or the whole system) being unavailable to perform its safety function;
(c) As a failure of a system train (or the whole system) when it operates on demand owing to the loads imposed on the pipework segment.

12.75. Pipework failures that lead directly to initiating events would normally already be included in a full scope PSA. It should be checked that this is the case and that conditional core or fuel damage probability is assessed for all initiating events induced by pipework failure. The ranking of these probabilities should be used for identification of the most risk significant pipework.

12.76. For pipework failures leading to the unavailability of credited systems or failure of credited systems 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[61], so the model should be revised correspondingly for this PSA application. A surrogate approach is often adopted, whereby 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.

12.77. The more rigorous way of determining the risk significance of all segments of pipework included in the risk informed pre-service and in-service inspection programme 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 pre-service and in-service inspection programmes that have been implemented in various Member States [42].

12.78. When the revised pre-service and 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 the guidelines used to assess the acceptability of the changes to the 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 pre-service and in-service inspection programme and by requantifying the PSA with these revised values, or by performing 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.

12.79. 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

[61] Sometimes such failures are screened out if the contribution to the failure probability of credited systems from a failure of the pipework is negligible in comparison to that from a failure of active components.

shared systems should be given additional consideration to determine how the inspection strategies should be adjusted using a risk informed approach.

RISK INFORMED CLASSIFICATION OF SSCS

12.80. 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;
>
> (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."

12.81. In addition, IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [43] provides the following recommendations on the use of PSA for safety classification:

> "2.3 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.
>
> […….]
>
> "2.14 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.
>
> […….]
>
> "3.27 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.
>
> "3.28 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."

12.82. The aim of the application of a risk informed classification is to provide an input

to the process of assigning safety classes to SSCs in accordance with their risk significance.[62] The 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. The analysis, to be conducted by a group of experts with various related expertise (e.g. in PSA, deterministic safety analysis, operation and maintenance, technology or licensing), might result in a final proposal to upgrade or to downgrade the classification of the investigated item. In the case of a resulting upgrade, previously hidden design imbalances affecting nuclear safety might be eliminated. In the case of a resulting downgrade the resources needed by operating personnel to implement the surveillance programme might be reduced and unnecessary regulatory burdens might be removed, without increasing risk.

12.83. The Level 1 PSA should be used to determine the risk significance of SSCs used to prevent core or fuel damage. The risk significance should be derived using both the Fussell–Vesely importance (or a measure providing equivalent information, such as the risk reduction worth or the fractional contribution) 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. Risk significance parameters should then be compared to thresholds defined to be consistent with the conventional (i.e. deterministic) classification methodology.

12.84. 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 having low or high safety significance.

12.85. Consideration should be given to 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.

12.86. When a large number of SSCs are reclassified and their treatment (e.g. testing and maintenance) is adjusted based on risk significance, the estimated failure probabilities of a large number of SSCs modelled in the PSA might change. Therefore, the cumulative impact of risk should be assessed to determine the conservative upper bound of cumulative impact and ensure that any cumulative potential risk increases are acceptable.

MONITORING AND MANAGING RISK CONFIGURATION

12.87. The risk monitor is a real time analysis tool that should be used to generate risk information based on the actual plant configuration (through a number of factors that typically include the plant operating state, the components that have been removed from service and the choice of operating trains and standby trains for normally operating systems) and on the current environmental operating conditions (e.g. the contribution from high snowfall or extremely low temperatures should not appear in the risk profile during summer).

12.88. The risk monitor can be used for the planning of future maintenance outages, long

[62] The historical approach for safety classification is to apply a high level of quality assurance to all SSCs identified as important to safety. However, the results of many PSAs performed to date have shown that some safety classified SSCs show a relatively low safety significance whereas some non-safety classified SSCs show a relatively high safety significance.

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).

12.89. 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.

12.90. 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 other aspects (e.g. the plant's technical specifications, defence in depth). Even though risk monitors are only used at operating plants, it is good practice to begin their development at the design stage, once the plant's design is already fixed.

12.91. The risk monitor should provide both quantitative risk information (e.g. 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 (e.g. the status of safety functions and systems).

PSA model and software for a risk monitor

12.92. The PSA model for the risk monitor should be amended so that it calculates the point in time risk for each of the plant's configurations rather than the average risk generally calculated by the PSA.

12.93. The PSA model should be amended to remove any simplifications made to reduce the amount of analysis needed for the PSA (e.g. modelling asymmetries) that could lead to the risk monitor giving incorrect results for some of the plant configurations that could arise.

12.94. 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 made symmetrical to account for all possible configurations (e.g. of operating systems) and it has to be possible to set the status of basic events to TRUE or FALSE to show component unavailability owing to testing or maintenance and thus reflect the current component configuration. The PSA model developed should also be compatible with the software used for the risk monitor.[63]

12.95. The risk monitor should be designed for use by nuclear power plant personnel knowledgeable about plant design and operations, rather than just PSA specialists.

12.96. The changes that a PSA practitioner or a risk monitor user may make should be commensurate with the level of expertise of those individuals and should be well documented.

12.97. 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.

[63] It might be necessary to change the event tree and fault tree models developed in the PSA into one logically equivalent large fault tree model (usually referred to as a 'top logic model') or change the way that NOT logic and logical switches are used in the model.

12.98. The software should be capable of providing results within a time frame that meet the needs of its primary users (e.g. work planners, control room operators) to meet its intended functions (e.g. to assess and manage the configuration risk of planned or emergent conditions).

12.99. The risk monitor should present information in a way that can be understood by its 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.

12.100. The risk monitor validation process should be aimed at providing a high level of confidence that the quantitative results produced 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

12.101. Users of the risk monitor should be aware of important limitations in the scope and 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 might fail to capture the significance of credited systems that are dedicated to mitigating the events caused by these hazards. The risk monitor model should therefore 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

12.102. The PSA results should be used to determine an appropriate set of performance indicators to provide retrospective or current indications of plant safety performance.

12.103. Risk based indicators that focus on past plant behaviour, taking into account events that have occurred and failures and unavailability of SSCs, should be used to identify trends and make comparisons between expected and calculated risk values so that decision makers can pinpoint ageing effects on SSCs.

12.104. 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.

12.105. Once risk based safety performance indicators have been established and agreed upon between the regulatory body and the operating organization, they should be used to increase the efficiency of inspections.

12.106. Risk based indicators should be derived using a risk monitor or a PSA that is based on plant specific data and actual operating experience.

PSA BASED EVENT ANALYSIS

12.107. Operating events which might initiate a plant trip and/or degrade or disable 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 performed to determine root causes.

12.108. 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 the event so that the response to the event is in accordance with its risk significance[64].

12.109. PSA based event analysis should be performed for events at the plant (also referred to as direct events) and relevant events at other plants (also referred to as transposed events). PSA based event analysis should include the analysis of initiating events and of conditional events (where the likelihood of an initiating event is increased or the availability of the credited systems needed to respond to initiating events is reduced).

12.110. 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 probability.

12.111. 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 or fuel damage probability, taking into account the unavailability of the affected SSCs and the duration of the event (e.g. using the risk monitor).

12.112. The PSA model should be capable of evaluating the potential impacts applicable for the event.

12.113. PSA based event analysis should be performed for events with high potential safety significance. To this end, screening criteria should be developed that can screen out events with low safety significance and rank events according to their significance.

12.114. The condition of the plant, failures that have occurred and actions taken by operating personnel during the event should be determined and accurately mapped in the PSA model. The PSA model should be requantified to generate the results necessary for comparison with the screening criteria mentioned in para. 12.113. The results necessary for comparison are typically the conditional core or fuel damage probabilities.

12.115. When conducting PSA based event analysis, known adverse occurrences should be modelled, setting associated basic events to TRUE, whereas known success occurrences should be modelled keeping associated basic events to their nominal probability.

12.116. The analysis of the event should be supplemented by sensitivity studies to provide the answer to ‘what if?’ questions (e.g. 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.

12.117. PSA based event analysis should be performed to complement deterministic analysis by allowing multiple failures 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.

12.118. Care should be taken in using the results of the PSA based event analysis to identify 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

[64] By performing risk based extrapolation of minor operational events to accident scenarios with serious consequences, valuable insights into accidents can be gained without any of the real consequences.

unless the analysis uses the same models, methods and assumptions throughout.

12.119. If a MUPSA model is available, it should be used to support PSA based event analysis by taking into account the degradation of shared systems and the impact of an initiating event on the behaviour of operating personnel and shared resources if several units might be affected.

RISK INFORMED REGULATIONS

12.120. The PSA should be used to identify plant specific or generic risk insights and design or operating changes that could enhance safety. PSA insights should also be used to guide long term prioritization of regulatory objectives and requirements, and of related safety research. Changes in risk metrics are used to evaluate possible changes to regulatory requirements needed to implement the risk management strategy.

12.121. Regulatory bodies should consider using PSA insights to promulgate risk informed regulations that enhance public safety or issue plant specific orders in accordance with national safety policies and regulations.

12.122. In some situations, PSA insights might 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 in accordance with national safety policies and regulatory requirements.

12.123. In developing and updating regulations and regulatory guides, regulatory bodies should employ a risk informed approach that takes account of the risk information and insights provided by the PSA, as follows:

(a) To use insights from the 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.

12.124. The scope and level of detail of the PSA should be commensurate with the issue under investigation and the PSA should be able to take into account all aspects of dealing with the issue.

RISK INFORMED OVERSIGHT AND ENFORCEMENT

12.125. The activities conducted by a regulatory body in relation to an operating plant include issuing, amending, suspending or revoking authorizations or licences; performing regulatory oversight; ensuring that corrective actions are taken and taking enforcement actions when necessary. Qualitative or quantitative risk insights derived from the PSA should be used to prioritize and 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 the areas of plant design and operation with high risk significance and that inspections are reduced or not performed in areas with 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 regulatory body should take risk significance into consideration in determining the magnitude of follow-up activities (e.g. the need for follow-up regulatory actions and enforcement);

(c) For assessing the significance of the failure by the operating organization to meet regulatory expectations and comply with enforcement actions;

(d) For assessing changes in risk measures associated with inspection findings; changes in risk metrics and conditional risk metrics can be used to evaluate the risk impact of degradations or issues that are found during inspections and to evaluate possible corrective actions;

(e) For developing and evaluating corrective measures regarding safety issues identified in the oversight process, including exploratory investigations into different variants to resolve a particular issue when changes in risk metrics are used to determine the risk significance and risk acceptability of the proposed measures based on risk characterization; changes in risk metrics should be used to determine the risk significance and risk acceptability of the proposed measures based on risk characterization.

12.126. The PSA should be used to evaluate and rank 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. Safety issues identified outside the PSA can be evaluated as part of 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.

12.127. The PSA can also be used to make interim decisions to alleviate a regulatory concern, while the longer term solutions are being evaluated. Examples of issues that might need an interim decision are as follows:

(a) The need for regulatory action in response to an event at a plant;

(b) One-time exemptions from technical specifications or other licensing requirements;

(c) Temporary modifications to hardware configuration or procedures.

12.128. The scope of the 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 could be used initially to perform a conservative screening evaluation and, if the results are significant, a more realistic and detailed evaluation could be performed. The evaluation should be extended as necessary for specific areas of concern.

USE OF PSA INSIGHTS TO DEVELOP OR ENHANCE EMERGENCY OPERATING PROCEDURES

12.129. 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 scope of) emergency operating procedures by providing assurance that a broad scope of vulnerabilities is addressed in a realistic, appropriately detailed and consistent manner.

12.130. At the design stage, the 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 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.

12.131. For operating plants, information from accident sequence analysis in Level 1 PSA performed using existing emergency operating procedures, and assessment of the associated human interactions, should be used to identify emergency operating procedures that need improving in the light of PSA insights.

12.132. The Level 1 PSA results should be reviewed to identify plant event sequences making an excessive risk contribution and for which credited systems are still available but cannot be credited because of a lack of adequate emergency operating procedures. For such plant event sequences, emergency operating procedures should be further developed.

12.133. 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 for the purpose of restoring the function of credited systems and for preventing degradation of events into severe accidents. The integral view of plant response utilized in the PSA methodology should be used in determining the potential for negative effects of certain measures.

12.134. Risk importance measures[65] of the affected or proposed actions and associated accident sequences should be used to help prioritize possible changes in procedure. Changes in core damage frequency or fuel damage frequency should be used to justify acceptable risk impacts and to determine risk significance.

12.135. A Level 1 PSA review of actions by operating personnel should support the enhancement of emergency operating procedures for those actions aimed at preventing severe core or fuel damage.

12.136. The level of detail of the Level 1 PSA model in the areas affected by the procedural changes involving accident sequences should be increased if the 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.

12.137. The human reliability analysis method used in the Level 1 PSA should be capable of predicting the impact of procedural changes to support this application; otherwise it should be reconsidered.

12.138. The Level 1 PSA should also provide feedback on potential revision of the specified decision points for transition to severe accident management guidelines.

[65] Typically, Fussell–Vesely importance together with Birnbaum importance (or risk achievement worth)

USE OF PSA INSIGHTS TO RISK INFORM THE TRAINING OF OPERATING PERSONNEL

Improvement of the training programme for operating personnel

12.139. 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 design) 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.

12.140. Descriptions of dominant accident sequences for core or fuel damage frequency in which human failure events play a significant role, risk importance measures of human failure events 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 human failure events and the PSA results should be used to select those actions on which enhanced training would be beneficial[66].

12.141. The human reliability analysis methods used in the PSA should be capable of measuring the affected changes. The change in risk metrics should allow analysts to evaluate the significance and acceptability of the proposed change.

12.142. Operating personnel at nuclear power plants spend a significant proportion of their time being trained on plant procedures; consequently, the risk insights should be used to risk inform this training and ensure that operating personnel have sufficient time to learn about risk significant actions.

12.143. The training should, at a minimum, inform operating personnel about risk significant actions. It might be further enhanced by making adjustments to the frequency of simulator training on certain scenarios, adding risk significant scenarios to qualification programmes for operating personnel, and using risk significant scenarios in drills.

Improvement of the training programme for maintenance personnel

12.144. The training of maintenance staff should be enhanced on the basis of insights and information derived from the PSA, focusing on potential risk significant impacts of maintenance activities such as common cause failure and maintenance induced failure of multiple system trains.

12.145. 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.

12.146. The same risk importance measures as recommended in para. 12.133 should be used to identify risk significant SSCs, pre-accident human failure events and basic events related to maintenance and common cause failures and to rank them with a view to identifying

[66] The risk achievement worth of a human failure event is representative of the ratio by which the fuel damage will increase if an individual fails to perform an action. Conversely, the Fussell-Vesely 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.

potential maintenance programme changes.

12.147. Changes in risk metrics (e.g. fuel damage frequency) should be used to evaluate the significance and acceptability of the proposed change to the maintenance training programme.

USE OF PSA TO ADDRESS EMERGING ISSUES

12.148. As operating experience is amassed, various issues might emerge that were unknown during the design, construction, and early operation of the plant (e.g. age-related failure mechanisms of passive SSCs).

12.149. Qualitative and/or quantitative insights from the PSA should be used to assess the risk significance of emerging issues.

12.150. Many of the issues that emerge are likely to be related to age-related degradation of passive SSCs and the replacement of obsolete components, which cannot be explicitly modelled in the PSA. Therefore, careful consideration should be given to how the issue should be accurately modelled (e.g. without overly conservative assumptions) using the PSA model (e.g. the degraded condition of a subset of control rods should not be modelled as a failure to insert the rods). Since emerging issues in general provide limited information, sensitivity analyses should be used to glean PSA insights.

12.151. The operating organization should use insights from the PSA to determine the priority of resolving the emerging issue within the construct of national safety policies and regulations.

12.152. The regulatory body should use insights from the PSA to set an appropriate timeline for the operating organization to resolve the emerging issue, 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, IAEA Safety Standards Series No.SSG-64, IAEA, Vienna (2021).

[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 NUCLEAR SAFETY GROUP, A Framework for an Integrated Risk Informed Decision Making Process, 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, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Hierarchical Structure of Safety Goals for Nuclear Installations, IAEA-TECDOC-1874, IAEA, Vienna (2019).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on Performing Integrated Risk Informed Decision Making, IAEA-TECDOC-1909, IAEA, Vienna (2020).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Human reliability analysis for nuclear installations, Safety Report Series (draft).

[16] US NUCLEAR REGULATORY COMMISSION, EPRI/NRC-RES Fire Human Reliability Analysis Guidelines – Final Report, NUREG-1921, Electric Power Research Institute, Palo Alto, CA (2012).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors, IAEA-TECDOC-1752, IAEA, Vienna (2014).

[19] OECD NUCLEAR ENERGY AGENCY, Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis, NEA/CSNI/R(2014)16, OECD/NEA, Paris (2015).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Dependability Assessment of Software for Safety Instrumentation and Control Systems at Nuclear Power Plants, Nuclear Energy Series No. NP-T-3.27, IAEA, Vienna (2018).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSR-1, IAEA, Vienna (2019).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Hazards Associated with External Human Induced Events in Site Evaluation for Nuclear Installations, IAEA Draft Safety Guide No. DS520, IAEA, Vienna (December 2020)

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-9 (Rev. 1), IAEA, Vienna (2022).

[25] 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).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodologies for Seismic Safety Evaluation of Existing Nuclear Installations, Safety Report Series No. 103, IAEA, Vienna (2020).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Nuclear Installations Against External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-68, IAEA, Vienna (2021).

[28] ELECTRIC POWER RESEARCH INSTITUTE, Identification of External Hazards for Analysis in Probabilistic Risk Assessment: Update of Report 1022997, EPRI, Technical Report 3002005287, Palo Alto, CA (2015).

[29] DECKER, K., BRINKMAN, H., List of External Hazards to be considered in ASAMPSA_E, Technical Report, ASAMPSA_E /WP21/D21.2/2017-41, University Vienna, Vienna (2016).

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Vulnerabilities of Operating Nuclear Power Plants to Extreme External Events, IAEA-TECDOC-1834, IAEA, Vienna (2017).

[31] US NUCLEAR REGULATORY COMMISSION, EPRI/NRC-RES Fire PRA

Methodology for Nuclear Power Facilities, Final Report, NUREG/CR-6850, EPRI 1011989, Electric Power Research Institute, Palo Alto, CA (2005).

[32] 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).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-1937, IAEA, Vienna, (2020).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Volcanic Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-21, IAEA, Vienna (2012).

[35] ELECTRIC POWER RESEARCH INSTITUTE, Methodology for Seismically Induced Internal Fire and Flood Probabilistic Risk Assessment, EPRI Technical Report 3002012980, EPRI, Palo Alto, CA (2018).

[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Level 1 Probabilistic Safety Assessment Practices for Nuclear Power Plants with CANDU-Type Reactors, IAEA-TECDOC-1977, IAEA, Vienna (2021).

[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).

[38] 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).

[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, IAEA, Vienna (2001).

[40] 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).

[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-25, IAEA, Vienna (2013).

[42] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed In-service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues and Development, IAEA Nuclear Energy Series No. NP-T-3.1, IAEA, Vienna (2010).

[43] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

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 owing to strong winds. It includes both direct damage from wind pressure and indirect damage owing to wind-borne missiles.	The hazard does not include tornado (A2) or downburst (A3) owing to the unique characteristics of these hazards. The hazard does not include the effects of snowstorm (included in A8), salt storm (A13) or sandstorm (A14). However, the wind effects of these hazards are included. Effects of storm surges are covered by the high water level hazard (W3).
A2	Tornado	The hazard is defined in terms of damage to the plant owing to tornadoes.	The hazard is addressed separately from other strong winds owing to its special characteristics (e.g. duration, wind speed, frequency of occurrence).
A3	Downburst	The hazard is defined in terms of impact on the plant of a downburst.	The hazard is addressed separately from other strong winds owing to its special characteristics (e.g. wind speed vertical profile). During a downburst, wind speed does not decrease at lower levels from the ground, as it does with strong winds.
A4	High air temperature	The hazard is defined in terms of impact on the plant of high air temperature.	Plant impact owing to high water temperature is addressed separately (W4).
A5	Low air temperature	The hazard is defined in terms of impact on the plant of low air temperature.	Plant impact owing to low water temperature (W4) or ice impact (W7, W8, W9) is addressed separately.
A6	Extreme air pressure (high/low gradient)	The hazard is defined in terms of impact on the plant of high or low air pressure or of rapid pressure changes.	
A7	Extreme rain	The hazard is defined in terms of damage to the plant owing to extreme rain.	Includes both damage owing to rain load on structures and damage owing to rain induced flooding.

A8	Extreme snow (including snowstorm)	The hazard is defined in terms of damage to the plant owing to extreme snow, including snowstorms.	Wind effects owing to snowstorms are covered by the strong wind hazard (A1). Flooding effects owing to melting of snow are covered by flooding effects owing to extreme rain (A7).
A9	Extreme hail	The hazard is defined in terms of damage to the plant owing to extreme hail. It includes damage owing to hail load on structures.	Flooding effects owing to melting of hail are covered by flooding effects owing to extreme rain (A7). Any possible effects on the ultimate heat sink are covered by ice hazards (W7, W8, W9).
A10	Mist	The hazard is defined in terms of impact on the plant of mist.	
A11	White frost	The hazard is defined in terms of impact on the plant of white frost.	
A12	Drought	The hazard is defined in terms of impact on the plant of an extended drought period that lowers the water level of lakes, rivers and open water basins.	Possible plant impacts owing to high air temperature (A4) 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).
A13	Salt storm	The hazard is defined in terms of impact on the plant of a storm involving salt covering of plant structures.	Wind effects from salt storms are covered by the strong wind hazard (A1).
A14	Sandstorm	The hazard is defined in terms of impact on the plant of storm-borne sand.	Wind effects from sandstorms are covered by the strong wind hazard (A1).
A15	Lightning	The hazard is defined in terms of damage to the plant owing 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.	Fire started by lightning is covered by external fire (G7) and by the internal fire analysis.
A16	Meteorite	The hazard is defined in terms of damage to the plant owing 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.	The impact of fish, mussels and other animals in the intake water is covered by the organic material in water hazard (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 an 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 addressed separately (M15). Fires resulting as secondary effects of other external hazards are addressed 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 owing 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 owing to strong water current.	The effects of underwater landslide are addressed separately (W6).
W2	Low water level	The hazard is defined in terms of impact on the plant of low water level.	Level decrease owing to land rise is addressed separately (G1).
W3	High water level	The hazard is defined in terms of impact on the plant of high water level owing 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 owing to high air temperature is addressed separately (A4).
W5	Low water temperature	The hazard is defined in terms of impact on the plant of low water temperature.	Plant impact owing to low air temperature (A5) or ice impact (W7, W8, W9) is addressed separately.

W6	Underwater landslide	The hazard is defined in terms of impact on the plant of an underwater landslide. An underwater landslide may be owing to above water causes, such as prolonged and intense precipitation.	Plant impact owing to underwater erosion is addressed as part of the strong water 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 owing 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 (e.g. algae, seaweed, fish, mussels, jellyfish) in the intake water.	
W11	Corrosion (from salt water)	The hazard is defined in terms of impact on the plant of corrosion from salt water.	
W12	Solid or fluid (non-gaseous) 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 owing to a ship accident but may also originate on land.	The hazard does not include effects owing to release of solid or fluid (non-gaseous) impurities (W12).
W14	Tsunami	The hazard is defined in terms of damage to the plant owing to high water level and pressure from the tsunami 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 the consequences of releases in connection with a ship accident , which are addressed separately in M2, M3, W12 and W13.

M2	Explosion after transport accident	The hazard is defined in terms of damage to the plant resulting from explosion after ground transport accidents outside the site or owing to sea, lake or river transport accidents. The damage may be caused by pressure impact or impact from missiles.	The hazard does not include damage owing to an aircraft crash (M20), pipeline accident (M5) or chemical release (M3).
M3	Chemical release after transport accident	The hazard is defined in terms of intake clogging or toxic impact on the plant resulting from chemical release after ground transport accidents outside the site or owing to sea, lake or river transport accidents.	Explosion effects from transport 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 caused by pressure impact or impact of missiles.	The hazard does not include explosions in connection with transport accidents outside the site (M2) or pipelines (M5) or toxic effects of a chemical release (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 caused by 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 transport 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 of a chemical release outside the site. Such 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 of a 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 are assumed to be covered 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 transport within the site	The hazard is defined in terms of damage to the plant resulting from direct impact of heavy transport within the site, but outside the plant buildings. This also includes transport of the containment external maintenance platform.	Heavy transport 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 caused by pressure impact or impact of missiles.	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 caused by pressure impact or impact from missiles.	
M13	Chemical release within the site	The hazard is defined in terms of toxic impact on the plant of a chemical release within the site. Such releases may originate from process accidents inside the plant or from leakages of substances stored within the site, but outside the plant buildings.	Chemical releases from substances stored inside plant 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 of a 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 of other external hazards are addressed 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 the plant resulting from an aircraft crash within the site area. The aircraft may be commercial, private or military.	
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 water level 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 (2003).

ANNEX II

EXAMPLES OF FIRE EVENT TREES AND SEISMIC EVENT TREES

ILLUSTRATION OF THE USE OF THE EVENT TREE TECHNIQUE FOR ANALYSIS OF FIRE MITIGATION AND PROPAGATION

II–1. The example of a fire 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.

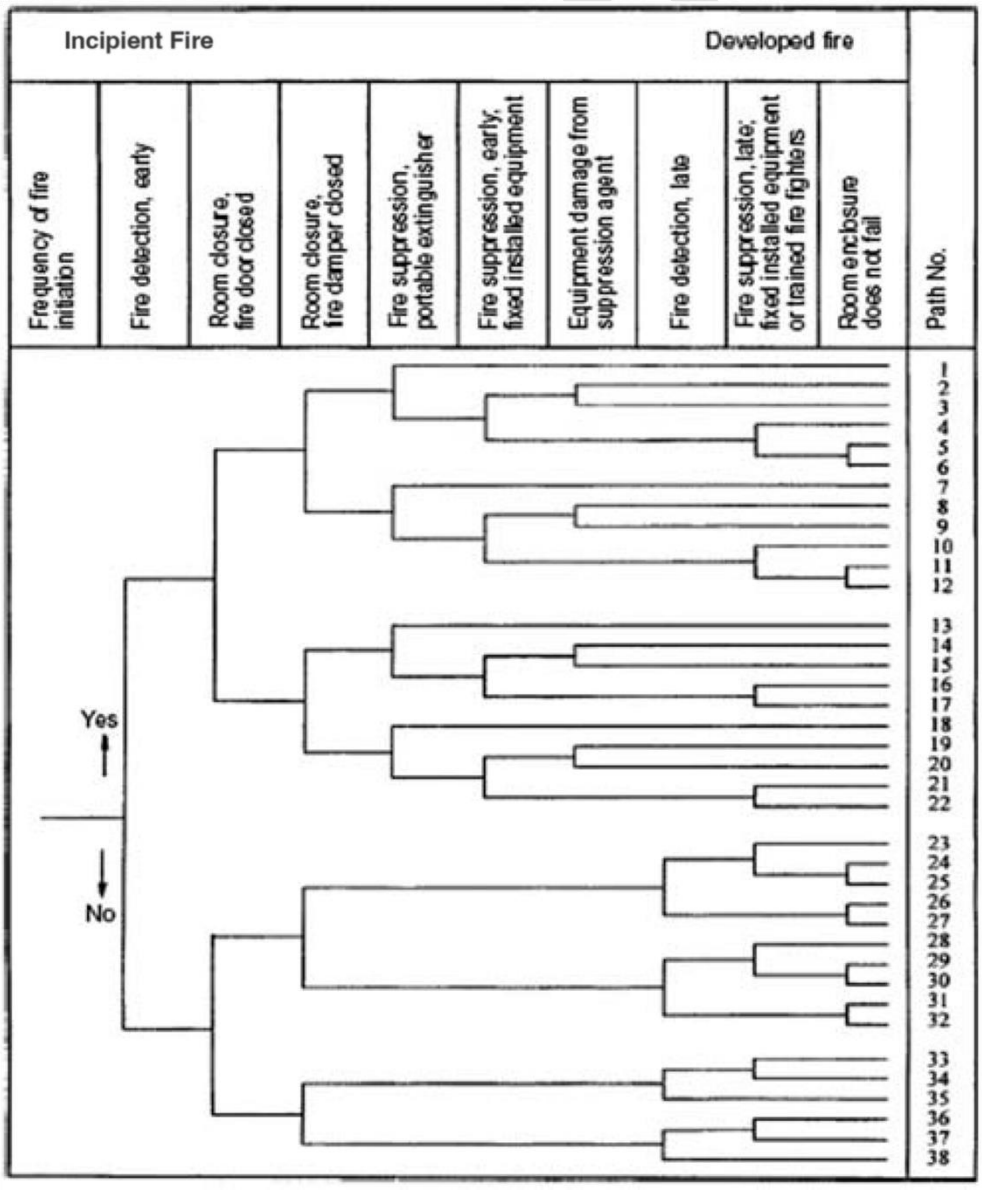

FIG. II–1. Example of a generic fire event tree.

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.

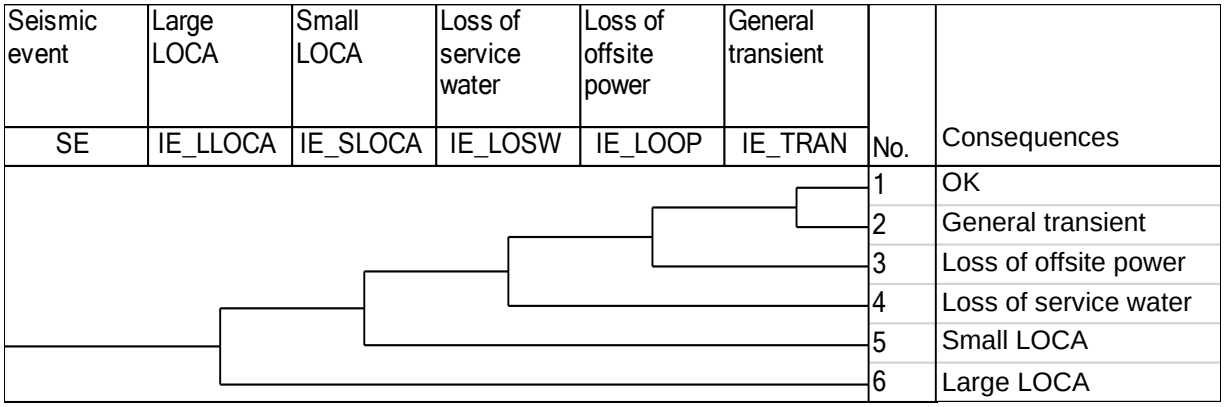

FIG. II–2. Example of an event tree for the modelling of a seismically induced initiating event. LOCA: loss of coolant accident.[67]

[67] Whilst the event tree in Fig II-2 appears to be logically correct, the labelling convention is potentially confusing. Normally, the top event descriptors are written as positive statements, with the up branch being positive and the down branch being negative (as correctly used in Fig II-1).

ANNEX III

SUPPORTING INFORMATION ON PSA FOR SHUTDOWN STATES

EXAMPLES OF PLANT OPERATING STATES AND ASSOCIATED INITIATING EVENTS

III–1. A probabilistic evaluation of shutdown states was performed in the framework of a PSA for an SWR 69 type German boiling water reactor[III–1]. A similar example for a pressurized water reactor plant is provided in Ref. [III–2].

III–2. On the basis of Ref. [III–1], the information presented in this Annex illustrates how the plant operating state can be specified and how initiating events can be associated with the various plant operating states. In order to describe the changes in system related and physical states, the outage was divided into different stages (see Fig. III–1 and Table III–1). The stages have been chosen in such a way that the system availability and the physical states are as constant as possible. Normally, during the outage (stages 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 identify 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 initiating events and their assignment to the plant operating states in which they might 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. 9.13, the end states to be included have to be decided on the basis of national probabilistic safety goals or criteria.

III–6.Corresponding information for a pressurized water reactor 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.

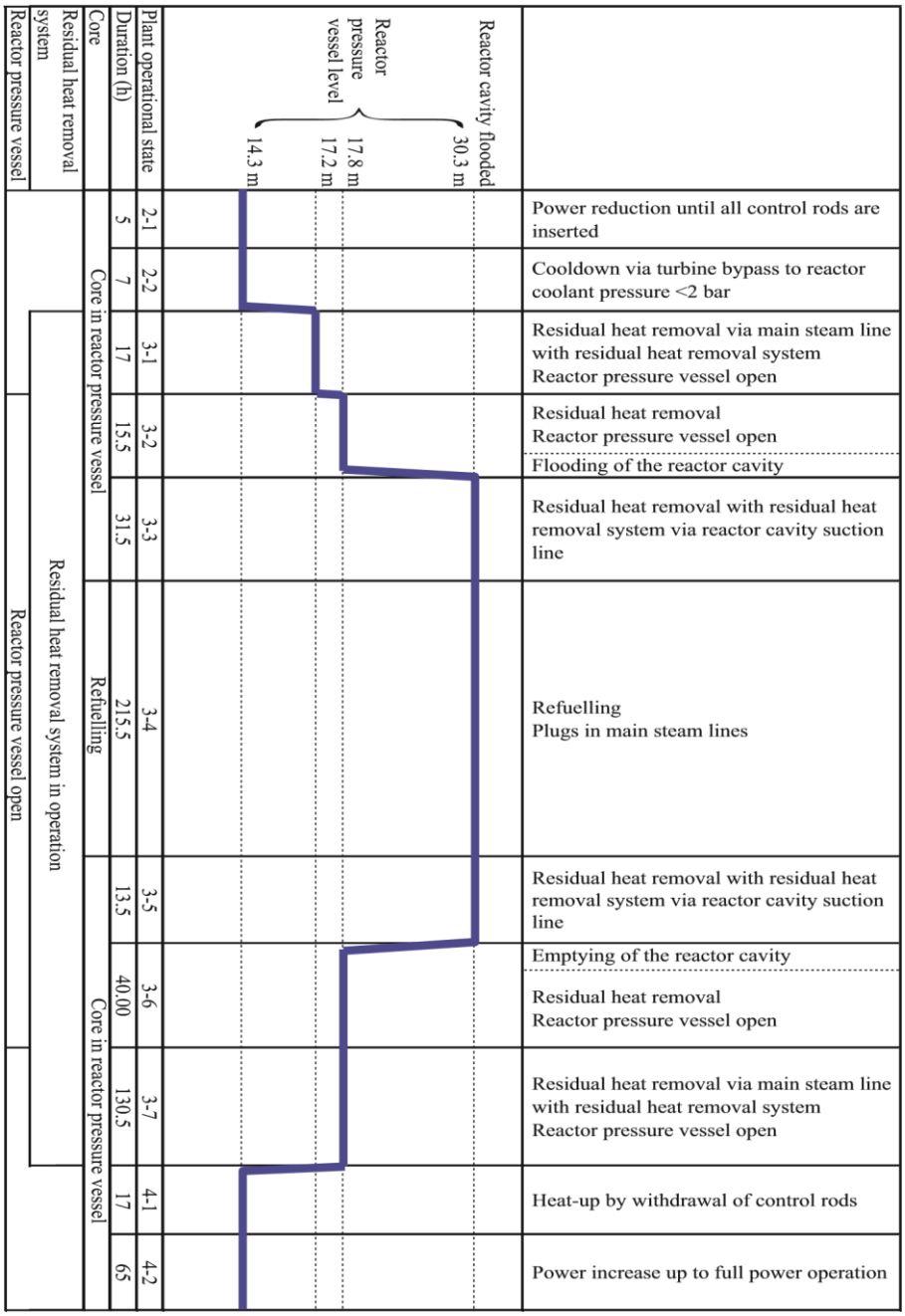

FIG. III–1. Reactor coolant level during outage.

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 in 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 in the reactor pressure vessel inside containment											
S1.1	Owing 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	Owing 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 in the residual heat removal system			X	X	X	X	X	X	X		
S3	Leak in 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 in 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 FOR 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 the 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 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	Deboration of coolant and taking reactor to critical condition / *Withdrawal of control rods and/or deboration*
(2)A0	Power increase up to specified level / *Reactor protection signals and availability of safety systems the 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
	Reactor pressure vessel closed				Reactor pressure vessel open					Reactor pressure vessel closed			
Transients													
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 owing 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									
Loss of coolant accidents													
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-bdV owing 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					

	Plant operating state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Leak into an affiliated system			x	x	x	x	x	x	x	x			
Unexpected deboration													
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	

P-bdV: pressurizer blow down valve.

EXAMPLES FOR SPECIFIC SYSTEM MODELLING REQUIREMENTS

III–7. Reference [III–8] is 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 in shutdown conditions. Certain operating states of the residual heat removal system that are only used during outages might also 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, might 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 might be bypassed during shutdown conditions in order to prevent an inadvertent start. For example, safety injection systems might 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 an outage owing to activities being undertaken as a result of the outage. For exampl**e**, although the cross-connection of low pressure systems might be an appropriate action during power operation, this might be locked, or a system train might be entirely disabled during an outage. 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 availability of the various systems during outage complicates 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 might 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, the working environment and the tasks performed are assessed to identify potential human errors and consequences. The significance of each potential error is then judged. In determining possible consequences, a distinction is made between unavailability of components or system parts on the one hand and initiating events on the other.

III–14. In the first case, an assessment is made of how the failure could be detected, for which time interval unavailability or latent faults would result and for which initiating events the unavailability or latent faults would become evident. Finally, possible countermeasures and consequences are described.

III–15. In the second case, the initiating event is classified (e.g. loss of coolant accident). Again, possible countermeasures 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 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, 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 for a boiling water reactor at the Laguna Verde nuclear power plant. In Fig. III–3, for plant operating states 1–4 at the same plant, 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.

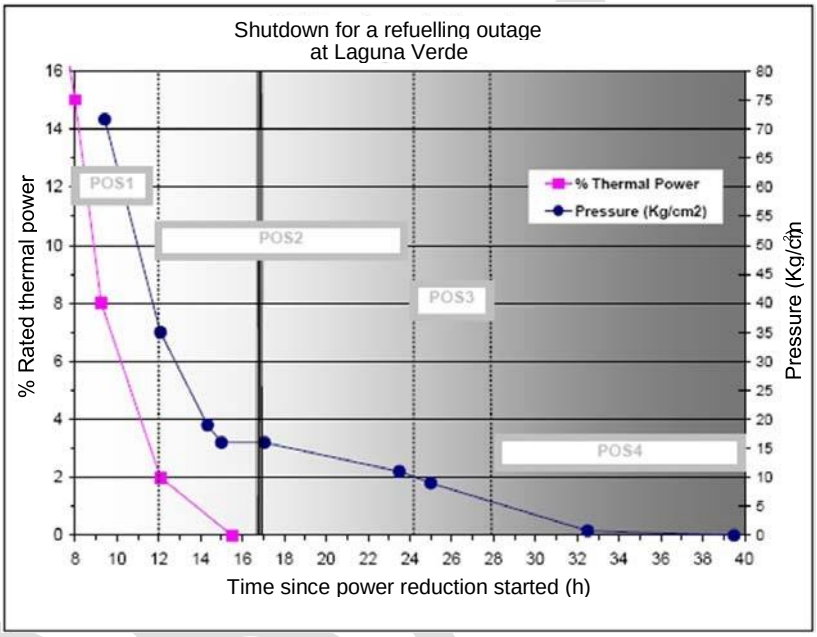

FIG. III–2. Plant operating states in PSA for shutdown states at Laguna Verde nuclear power plant. POS: plant operating state.

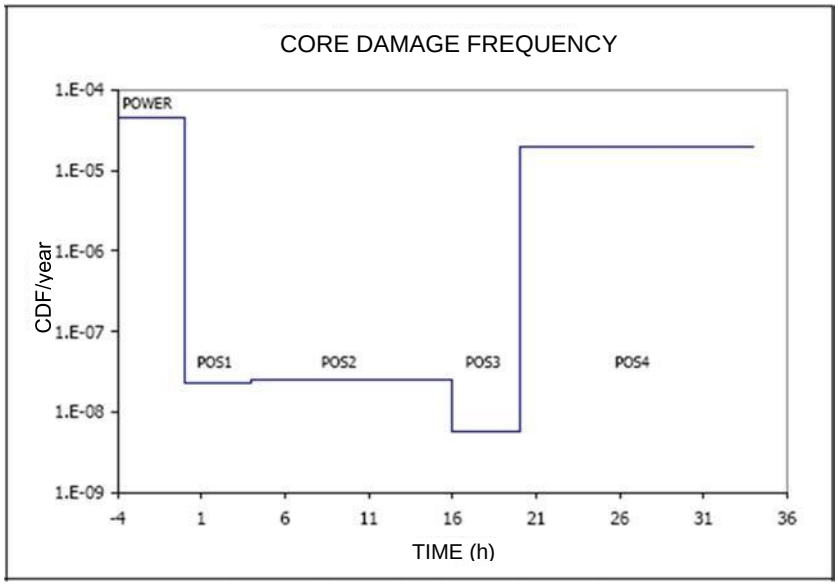

FIG. III–3. Comparison of core damage frequency per year for PSA for power operation and shutdown states. POS: plant operating state. CDF: Core damage frequency.

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, ID (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, ID (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] FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Methoden und Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: Mai 2015, BfS-SCHR-61/16, Bundesamt für Strahlenschutz (BfS), Salzgitter, Germany (September 2016)
[III–9] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA-TECDOC-1144, IAEA, Vienna (2000).
[III–10] 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).