IAEA Safety Standards

for protecting people and the environment

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

Specific Safety Guide

No. SSG-3

IAEA
International Atomic Energy Agency

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available at the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

OTHER SAFETY RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications. Security related publications are issued in the **IAEA Nuclear Security Series**.

DEVELOPMENT AND APPLICATION OF LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

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

IAEA SAFETY STANDARDS SERIES No. SSG-3

DEVELOPMENT AND APPLICATION OF LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2010

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
April 2010
STI/PUB/1430

IAEA Library Cataloguing in Publication Data

Development and application of level 1 probabilistic safety assessment for nuclear power plants : specific safety guide. — Vienna : International Atomic Energy Agency, 2010.
p. ; 24 cm. — (IAEA safety standards series, ISSN 1020–525X ; no. SSG-3)
STI/PUB/1430
ISBN 978–92–0–114509–3
Includes bibliographical references.

1. Nuclear power plants — Risk assessment. 2. Nuclear power plants — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL 10–00612

FOREWORD

The IAEA's Statute authorizes the Agency to establish safety standards to protect health and minimize danger to life and property — standards which the IAEA must use in its own operations, and which a State can apply to its nuclear and radiation related facilities and activities. A comprehensive body of safety standards under regular review, together with the IAEA's assistance in their application, has become a key element in a global safety regime.

In the mid-1990s, a major overhaul of the IAEA's safety standards programme was initiated, with a revised oversight committee structure and a systematic approach to updating the entire corpus of standards. The new standards that have resulted are of a high calibre and reflect best practices in Member States. With the assistance of the Commission on Safety Standards, the Agency is working to promote the global acceptance and use of its safety standards.

Safety standards are only effective, however, if they are properly applied in practice. The IAEA's safety services — which range in scope from engineering safety, operational safety, and radiation, transport and waste safety to regulatory matters and safety culture in organizations — assist Member States in applying the standards and appraise their effectiveness. These safety services enable valuable insights to be shared and I continue to urge all Member States to make use of them.

Regulating safety in nuclear and radiation related activities is a national responsibility, and many Member States have decided to adopt the IAEA's safety standards for use in their national regulations. For the Contracting Parties to the various international safety conventions, IAEA standards provide a consistent, reliable means of ensuring the effective fulfillment of obligations under the conventions. The standards are also used around the world by organizations that design, manufacture and apply nuclear and radiation related technologies in power generation, medicine, industry, agriculture, research and education.

The IAEA takes seriously the enduring challenge for operators and regulators everywhere — of ensuring a high level of safety in the use of nuclear and radioactive materials around the world. Their continuing utilization for the benefit of humankind must be managed in a safe manner, and the IAEA safety standards are designed to facilitate the achievement of that goal.

THE IAEA SAFETY STANDARDS

BACKGROUND

Radioactivity is a natural phenomenon and natural sources of radiation are features of the environment. Radiation and radioactive substances have many beneficial applications, ranging from power generation to uses in medicine, industry and agriculture. The radiation risks to workers and the public and to the environment that may arise from these applications have to be assessed and, if necessary, controlled.

Activities such as the medical uses of radiation, the operation of nuclear installations, the production, transport and use of radioactive material, and the management of radioactive waste must therefore be subject to standards of safety.

Regulating safety is a national responsibility. However, radiation risks may transcend national borders, and international cooperation serves to promote and enhance safety globally by exchanging experience and by improving capabilities to control hazards, to prevent accidents, to respond to emergencies and to mitigate any harmful consequences.

States have an obligation of diligence and duty of care, and are expected to fulfil their national and international undertakings and obligations.

International safety standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection. International safety standards also promote and assure confidence in safety and facilitate international commerce and trade.

A global nuclear safety regime is in place and is being continuously improved. IAEA safety standards, which support the implementation of binding international instruments and national safety infrastructures, are a cornerstone of this global regime. The IAEA safety standards constitute a useful tool for contracting parties to assess their performance under these international conventions.

THE IAEA SAFETY STANDARDS

The status of the IAEA safety standards derives from the IAEA's Statute, which authorizes the IAEA to establish or adopt, in consultation and, where appropriate, in collaboration with the competent organs of the United Nations and with the specialized agencies concerned, standards of safety for protection

of health and minimization of danger to life and property, and to provide for their application.

With a view to ensuring the protection of people and the environment from harmful effects of ionizing radiation, the IAEA safety standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste.

Safety measures and security measures[1] have in common the aim of protecting human life and health and the environment. Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

The IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. They are issued in the IAEA Safety Standards Series, which has three categories (see Fig. 1).

Safety Fundamentals

Safety Fundamentals present the fundamental safety objective and principles of protection and safety, and provide the basis for the safety requirements.

Safety Requirements

An integrated and consistent set of Safety Requirements establishes the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objective and principles of the Safety Fundamentals. If the requirements are not met, measures must be taken to reach or restore the required level of safety. The format and style of the requirements facilitate their use for the establishment, in a harmonized manner, of a national regulatory framework. The safety requirements use 'shall' statements together with statements of

[1] See also publications issued in the IAEA Nuclear Security Series.

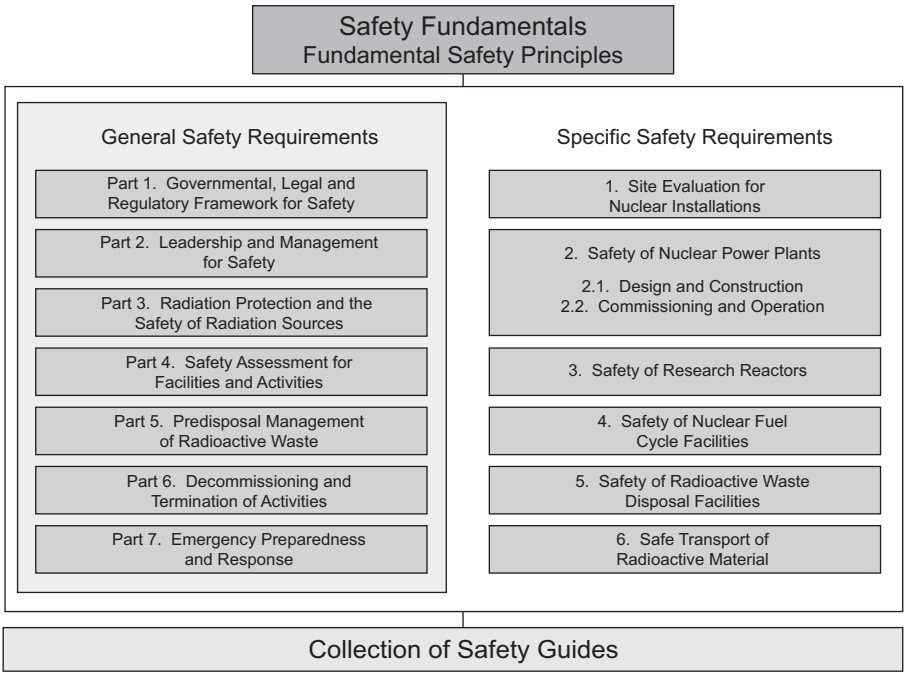

FIG. 1. The long term structure of the IAEA Safety Standards Series.

associated conditions to be met. Many requirements are not addressed to a specific party, the implication being that the appropriate parties are responsible for fulfilling them.

Safety Guides

Safety Guides provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety. The recommendations provided in Safety Guides are expressed as 'should' statements.

APPLICATION OF THE IAEA SAFETY STANDARDS

The principal users of safety standards in IAEA Member States are regulatory bodies and other relevant national authorities. The IAEA safety

standards are also used by co-sponsoring organizations and by many organizations that design, construct and operate nuclear facilities, as well as organizations involved in the use of radiation and radioactive sources.

The IAEA safety standards are applicable, as relevant, throughout the entire lifetime of all facilities and activities — existing and new — utilized for peaceful purposes and to protective actions to reduce existing radiation risks. They can be used by States as a reference for their national regulations in respect of facilities and activities.

The IAEA's Statute makes the safety standards binding on the IAEA in relation to its own operations and also on States in relation to IAEA assisted operations.

The IAEA safety standards also form the basis for the IAEA's safety review services, and they are used by the IAEA in support of competence building, including the development of educational curricula and training courses.

International conventions contain requirements similar to those in the IAEA safety standards and make them binding on contracting parties. The IAEA safety standards, supplemented by international conventions, industry standards and detailed national requirements, establish a consistent basis for protecting people and the environment. There will also be some special aspects of safety that need to be assessed at the national level. For example, many of the IAEA safety standards, in particular those addressing aspects of safety in planning or design, are intended to apply primarily to new facilities and activities. The requirements established in the IAEA safety standards might not be fully met at some existing facilities that were built to earlier standards. The way in which IAEA safety standards are to be applied to such facilities is a decision for individual States.

The scientific considerations underlying the IAEA safety standards provide an objective basis for decisions concerning safety; however, decision makers must also make informed judgements and must determine how best to balance the benefits of an action or an activity against the associated radiation risks and any other detrimental impacts to which it gives rise.

DEVELOPMENT PROCESS FOR THE IAEA SAFETY STANDARDS

The preparation and review of the safety standards involves the IAEA Secretariat and four safety standards committees, for nuclear safety (NUSSC), radiation safety (RASSC), the safety of radioactive waste (WASSC) and the safe transport of radioactive material (TRANSSC), and a Commission on Safety Standards (CSS) which oversees the IAEA safety standards programme (see Fig. 2).

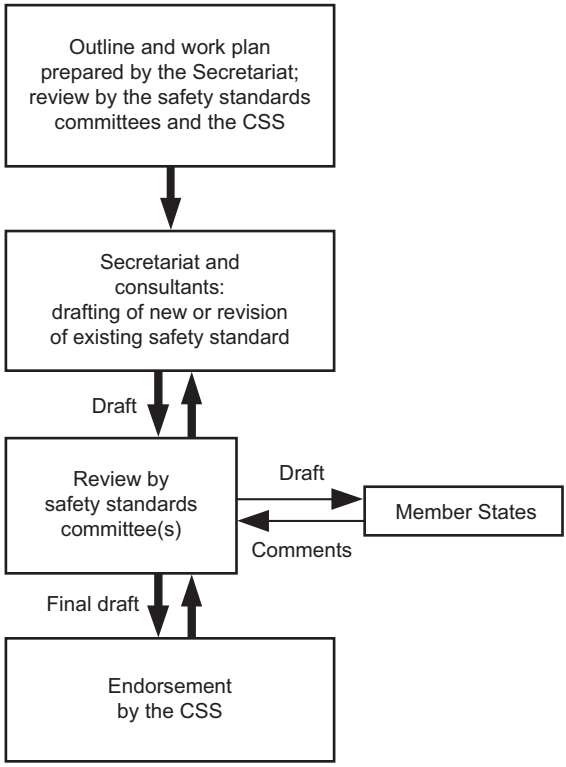

FIG. 2. The process for developing a new safety standard or revising an existing standard.

All IAEA Member States may nominate experts for the safety standards committees and may provide comments on draft standards. The membership of the Commission on Safety Standards is appointed by the Director General and includes senior governmental officials having responsibility for establishing national standards.

A management system has been established for the processes of planning, developing, reviewing, revising and establishing the IAEA safety standards. It articulates the mandate of the IAEA, the vision for the future application of the safety standards, policies and strategies, and corresponding functions and responsibilities.

INTERACTION WITH OTHER INTERNATIONAL ORGANIZATIONS

The findings of the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) and the recommendations of international

expert bodies, notably the International Commission on Radiological Protection (ICRP), are taken into account in developing the IAEA safety standards. Some safety standards are developed in cooperation with other bodies in the United Nations system or other specialized agencies, including the Food and Agriculture Organization of the United Nations, the United Nations Environment Programme, the International Labour Organization, the OECD Nuclear Energy Agency, the Pan American Health Organization and the World Health Organization.

INTERPRETATION OF THE TEXT

Safety related terms are to be understood as defined in the IAEA Safety Glossary (see http://www-ns.iaea.org/standards/safety-glossary.htm). Otherwise, words are used with the spellings and meanings assigned to them in the latest edition of The Concise Oxford Dictionary. For Safety Guides, the English version of the text is the authoritative version.

The background and context of each standard in the IAEA Safety Standards Series and its objective, scope and structure are explained in Section 1, Introduction, of each publication.

Material for which there is no appropriate place in the body text (e.g. material that is subsidiary to or separate from the body text, is included in support of statements in the body text, or describes methods of calculation, procedures or limits and conditions) may be presented in appendices or annexes.

An appendix, if included, is considered to form an integral part of the safety standard. Material in an appendix has the same status as the body text, and the IAEA assumes authorship of it. Annexes and footnotes to the main text, if included, are used to provide practical examples or additional information or explanation. Annexes and footnotes are not integral parts of the main text. Annex material published by the IAEA is not necessarily issued under its authorship; material under other authorship may be presented in annexes to the safety standards. Extraneous material presented in annexes is excerpted and adapted as necessary to be generally useful.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. It is generally recognized that facilities and activities dealing with radioactive material provide many benefits, but at the same time give rise to radiation risks. The Safety Fundamentals, Fundamental Safety Principles [1], establish 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, Principle 5 of Ref. [1] (para. 3.22) on optimization of protection states:

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

1.2. Several IAEA Safety Requirements publications establish more specific requirements for risk assessment for nuclear power plants. The Safety Requirements publication on Safety of Nuclear Power Plants: Design [2] (para. 5.69) establishes that:

> "A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied. On the basis of this analysis, the design basis for items important to safety shall be established and confirmed."

It is also emphasized further in Ref. [2] (para. 5.73) that:

> "A probabilistic safety analysis of the plant shall be carried out in order:
>
> (1) to provide a systematic analysis to give confidence that the design will comply with the general safety objectives;
> (2) to demonstrate that a balanced design has been achieved such that no particular feature or PIE[1] makes a disproportionately large or

[1] PIE: postulated initiating event.

significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety;

(3) to provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behaviour ('cliff edge effects') will be prevented;

(4) to provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;

(5) to provide assessments of the probabilities of occurrence and the consequences of external hazards, in particular those unique to the plant site;

(6) to identify systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences;

(7) to assess the adequacy of plant emergency procedures; and

(8) to verify compliance with probabilistic targets, if set."

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

1.4. The Safety Requirements publication on Safety Assessment for Facilities and Activities [3] (para. 4.13) emphasizing the need for a comprehensive safety analysis states:

> "The safety assessment has to include a safety analysis, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety in various operational states, anticipated operational occurrences and accident conditions, by means of deterministic and also probabilistic methods."

It is also stated in Ref. [3] (para. 4.55):

> "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.

1.5. 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 damage and the core damage frequency is estimated. Level 1 PSA provides insights into the strengths and weaknesses of the safety related systems and procedures in place or envisaged as preventing core damage.
(2) In Level 2 PSA, the chronological progression of core damage sequences identified in Level 1 PSA is evaluated, including a quantitative assessment of phenomena arising from severe damage to reactor fuel. Level 2 PSA identifies ways in which associated releases of radioactive material from fuel can result in releases to the environment. It also estimates the frequency, magnitude and other relevant characteristics of the release of radioactive material to the environment. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures and the physical barriers to the release of radioactive material to the environment (e.g. a containment building).
(3) In Level 3 PSA, public health and other societal consequences are estimated, such as the contamination of land or food from the accident sequences that lead to a release of radioactivity to the environment.

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

1.7. Level 1 PSAs have now been carried out for most nuclear power plants worldwide. In recent years, a trend has emerged for Level 2 PSAs or limited Level 2 PSAs (e.g. Level 2 PSAs in which the large early release frequency is estimated) to be carried out for many types of nuclear power plant. In addition, Level 3 PSAs have been carried out in several States.

1.8. 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, an International Nuclear Safety Advisory Group (INSAG) report [4] and other publications that address the safety of nuclear power plants.

OBJECTIVE

1.9. The objective of this Safety Guide is to provide recommendations for meeting the requirements of Ref. [3] in performing or managing a Level 1 PSA project for a nuclear power plant and using it to support its safe design and operation. This Safety Guide is applicable to existing nuclear power plants and to evolutionary designs of nuclear power plants, but may not be fully applicable to revolutionary designs. 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.

1.10. 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 [5].

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

SCOPE

1.12. This Safety Guide addresses the necessary technical features of a Level 1 PSA and applications for nuclear power plants, on the basis of internationally recognized good practices. The scope of a Level 1 PSA addressed in this Safety Guide includes all operational conditions of the plant (i.e. full power, low power and shutdown) and all potential initiating events and potential hazards, namely: (a) internal initiating events caused by random component failures and human error, (b) internal hazards (e.g. internal fires and floods, turbine missiles) and (c) external hazards, both natural (e.g. earthquake, high winds, external floods) and of human-induced (e.g. airplane crash, accidents at nearby industrial facilities).

1.13. This Safety Guide is focused on the reactor core; it does not cover other sources of radioactive material on the site, e.g. the spent fuel pool. However, while considering Level 1 PSA for low power and shutdown modes (Section 9), the risk from the fuel removed from the reactor is also addressed.

1.14. The consideration of hazards arising from malicious actions does not lie within the scope of this Safety Guide.

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

1.16. The recommendations of this Safety Guide are intended to be technology neutral to the extent possible, and it is expected that the vast majority of the recommendations will be applicable to different types of nuclear power plant. However, examples, where deemed necessary, are mainly provided for light water cooled nuclear power plants. Interpretation or judgement may be necessary when applying some recommendations to other types of nuclear power plant.

STRUCTURE

1.17. Section 2 provides recommendations on the general issues concerning the performance and use of PSA, including the scope of the PSA, validation of the PSA and a living PSA. Section 3 provides key recommendations on project management and organization for PSA and general aspects of PSA documentation. Section 4 addresses the task of familiarization of the team

carrying out the PSA with the nuclear power plant. Sections 5–8 provide recommendations on the methodology of a Level 1 PSA for full power operating conditions for various initiating events and hazards. Section 5 provides recommendations on Level 1 PSA for internal initiating events. Section 6 summarizes key recommendations on the general aspects of Level 1 PSA for internal and external hazards, and Sections 7 and 8 address the specifics of Level 1 PSA for internal hazards and external hazards, respectively. Section 9 provides key recommendations for Level 1 PSA for low power and shutdown modes. Section 10 sets out key recommendations for applications of Level 1 PSA. Three annexes provide an example of a generic list of internal and external hazards, an example of a fire propagation event tree and a seismic event tree, and supporting information on PSA for low power and shutdown modes.

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

SCOPE OF THE PSA

2.2. Paragraphs 2.2–2.4 provide recommendations on meeting Requirement 1 on a graded approach and Requirement 14 relating to the scope of the safety analysis for a PSA [3]. The scope of the PSA to be undertaken should be correlated with the national safety goals or criteria, if the latter have been set. At a high level, quantitative results of PSA are often used to verify compliance with safety goals or criteria, which are usually formulated in terms of quantitative estimates of core damage frequency, frequencies of radioactive releases of different types and societal risks and which therefore may necessitate performance of a Level 1 PSA, Level 2 PSA or Level 3 PSA, respectively. Safety

goals or criteria do not usually specify which hazards and plant operational modes have to be addressed. Therefore, in order to use the PSA results for the verification of compliance with existing safety goals or criteria, a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operational modes should be performed unless the 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 operational modes that are not in the model does not threaten compliance with the safety goals or criteria.

2.3. If the PSA is carried out only to Level 1, then the reactor core is usually the focus of the analysis. If the PSA is carried out to Level 2 or Level 3, where the impact of radioactive releases has to be assessed, then the scope of the PSA may include contributions to risk arising from other radioactive material on the site, such as spent fuel and radioactive waste. Such sources of radioactivity outside the core should be included in the PSA whenever the intention is to address the total risk from the plant to members of the public near the site.

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

VALIDATION AND REVIEW OF THE PSA

2.5. Paragraphs 2.5 and 2.6 provide recommendations on meeting Requirement 18 on the use and validation of computer codes for a PSA and Requirement 21 on the independent verification of PSA [3]. PSA involves a number of analytical methods. These include the development of event tree and fault tree logic models used for analysis of accident sequences, the methods for solution of the logic models, the models of phenomena that could occur, for instance, within the containment of a nuclear power plant following core damage, and the models for the transport of radionuclides in the environment to determine their effects on health and the economy, depending on the scope of the analysis (Level 1, 2 or 3). Prior to their application, it should be demonstrated that these analytical methods provide an adequate representation of the processes taking place. The computer codes that support these analytical methods 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 (Ref. [3], para. 4.60).

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

LIVING PSA

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

2.8. Data should be collected throughout the lifetime of the plant to check or update the analysis. Such data should include data on operational experience, in particular data on initiating events, data on component failures and unavailability during periods of testing, maintenance and repair, and data on human

performance. The results from the analysis should be periodically reassessed in the light of new data.

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

REFERENCE VALUES (SAFETY GOALS OR CRITERIA)

2.10. Paragraphs 2.10–2.20 provide recommendations on meeting Requirement 4 for the purpose of conducting a PSA [3]. 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, operators, 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 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 safety systems;
(b) The frequency of core damage[2] (Level 1 PSA);
(c) The frequency of a specific release (specified, for example, in terms of its quantity, isotopes, timing) of radioactive material from the plant or the

[2] For the concept of core damage, specific criteria have to be specified, as described in Section 5 of this Safety Guide. These criteria may be different for different reactor designs.

frequency of a 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. One possible framework for the definition of probabilistic safety criteria is given in Ref. [6], which defines a 'threshold of tolerability' above which the level of risk would be intolerable, and a 'design target' below which the risk would be broadly acceptable. Between these two levels there is a region where the risk would be acceptable only if all reasonably achievable measures have been taken to reduce the risk. Although this approach has been adopted in some States, it is more usual to find probabilistic safety criteria identified as targets, goals, objectives, guidelines or reference values for orientation. In addition, the numerical values for the levels of risk, which correspond to the threshold of tolerability and the design targets, differ from State to State.

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

2.14. On the basis of current experience with the design and operation of nuclear power plants, INSAG, in 1999, proposed numerical values that can be achieved for current and proposed designs of nuclear power plants.

2.15. INSAG (see Ref. [4]) has proposed the objectives for core damage frequency separately for existing plants and future plants.[3]

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

2.16. Core damage frequency is the most common measure of risk since most nuclear power plants have undergone at least a Level 1 PSA and the methodology is well established. In many States, numerical values of this type are used either formally or informally as probabilistic safety goals or criteria.

2.17. **Large off-site release of radioactive material**: A large release of radioactive material, which would have severe implications for society and would require off-site emergency arrangements to be implemented, can be specified in a number of ways, including the following:

(a) As absolute quantities (in bequerels) of the most significant nuclides released;
(b) As a fraction of the inventory of the core;
(c) As a specified dose to the most exposed person off the site;
(d) As a release incurring 'unacceptable consequences'.

In some cases, criteria are specified that relate to the timing of the release, in particular whether the release occurs early or late. In such cases, the term 'early' needs to be defined.

2.18. The objectives have also been proposed by INSAG for a large off-site release of radioactive material requiring short term off-site response.[4]

2.19. Although there is no international consensus on what constitutes a large off-site release, similar probabilistic criteria have been specified in a number of States.

2.20. **Health effects to members of the public**: INSAG has given no guidance on targets for health effects for members of the public.[5]

[4] The objective for large off-site releases requiring short term off-site response is 1×10^{-5} per reactor-year for existing plants. Reference [4] does not specify a numerical value for a large off-site radioactive release for future plants, but states the following qualitative objective: "Another objective for these future plants is the practical elimination of accident sequences that could lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time."

[5] In some States, the target for the risk of death of a member of the public is taken to be 1×10^{-6} per reactor-year.

USE OF PSA IN DECISION MAKING

2.21. Paragraphs 2.21–2.31 provide recommendations on meeting Requirement 23 of Ref. [3] on the use of a Level 1 PSA. The PSA should be used during the lifetime of the plant to provide an input into decision making in combination with the results and insights of deterministic safety analyses and considerations of defence in depth.

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

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

2.23. 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. 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.

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

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

2.26. In addition, the results of the PSA should be compared with the probabilistic safety goals or criteria if these have been specified in national

regulations or guidelines, etc. This should be done for all probabilistic criteria defined for the plant, including those that address system reliability, core damage, releases of radioactive material, health effects for workers, health effects for the public and off-site consequences such as land contamination and food bans.

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

2.28. The results of the Level 1 PSA should be used to identify weaknesses in the design or operation of the plant. Weaknesses can be identified by considering the contributions to the risk from groups of initiating events, the importance measures of the safety systems and the contributions of human error to the overall risk. Where the results of the PSA indicate that changes could be made to the design or operation of the plant to reduce risk, the changes should be incorporated where reasonably achievable, taking the relative costs and benefits of any modifications into account.

2.29. The results of the Level 2 PSA should be used to determine if sufficient provision has been made to prevent or mitigate the effects of postulated core damage sequences. In Level 2 PSA, it should be considered whether the containment is adequately robust and whether the protection systems such as hydrogen mixing and recombining systems, containment sprays and containment venting systems provide an adequate level of protection to prevent a large release of radioactive material to the environment. Furthermore, containment bypassing events such as a loss of coolant accident in interfacing systems should be addressed. In addition, Level 2 PSA should be used to identify and optimize accident management measures that could be carried out to mitigate the effects of the damaged core. This could include determining additional measures, for example, measures that could be taken to introduce water into the reactor containment.

2.30. When available, the results of Level 2 PSA and Level 3 PSA should be provided to civil authorities as a technical input for off-site emergency planning.

2.31. Section 10 provides detailed recommendations on specific applications of PSA for the regulatory body and for operating organizations. However, for the sake of convenience and continuity in covering the general aspects of PSA, a summary of the main recommendations relating to application of PSA is provided in the following:

(a) The results of the PSA should be used in developing emergency procedures for accidents and to provide inputs into the technical specifications of the plant. In particular, the results of the PSA should be used to investigate the increase in risk after the removal from service of items of equipment for testing or maintenance and the adequacy of the frequency of surveillance or testing. The PSA should be used to confirm that the allowed outage times do not contribute unduly to risk and to indicate which combinations of equipment outages should be avoided.

(b) The PSA should be used throughout the design and operation of the plant to assist in the decision making process on the safety of the plant:
   (i) For a new plant, the PSA should be initiated in the conceptual design stage to check that the level of redundancy and diversity provided in the safety systems is adequate. The PSA should be continued through the more detailed design stage to assess more detailed design issues and should be used to support operation of the plant. In the design stage, an iterative process should be put in place to ensure that the insights gained from the PSA are fed back into the design process.
   (ii) For an existing plant, the PSA should be carried out either as part of a periodic safety assessment or to support the safety case for proposed modifications. Although the requirements for the PSA remain the same, the data used may vary with the experience accumulated. Moreover, depending on the age of the facility, the remaining operational lifetime, the cost of proposed modifications and other related considerations, there will be differences in what changes could reasonably be implemented to reduce risk. Such considerations should take account of the possibility of plant life extension, irrespective of whether such a life extension has been applied for or is only being considered.

(c) The PSA should be used to determine if the safety systems contain an adequate level of redundancy and diversity and if the overall design is balanced. As indications of a balanced design, the results of the PSA should show that:
   (i) No particular feature of the design or of the group of initiating events makes a disproportionately large contribution to risk;
   (ii) The achievement of an overall low level of risk does not rely on contributors that have significant uncertainty.

A lack of balance in the design is often an indication that there are opportunities for implementing reasonably practicable measures to reduce risk.

3. PROJECT MANAGEMENT AND ORGANIZATION FOR PSA

DEFINITION OF OBJECTIVES AND SCOPE OF THE PSA PROJECT

3.1. Paragraphs 3.1 and 3.2 provide recommendations on meeting Requirement 4 of Ref. [3] on purpose of the Level 1 PSA and Requirement 14 relating to the scope of a Level 1 PSA [3]. Determination of the objectives of the PSA together with its intended and potential uses is an important step to undertake prior to starting the process of performing a PSA. The scope of the PSA is defined by the analysis level (Level 1, 2 or 3), the initiating events and hazards considered, and the operational modes (i.e. full power, low power or shutdown states[6]) addressed. The scope of the PSA should be compatible with both the objectives of the study and the available resources and information, i.e. the necessary procedures and methods, personnel, expertise, funding and the time needed for the analysis. For example, if the objective of a PSA is to verify the risk arising from plant operation against specified safety goals, thus implying a complete risk assessment, a full scope PSA comprising a comprehensive listing of initiating events and hazards and all plant operational modes should be performed, and adequate resources should be provided for the analysis. In addition, other sources of radiation (e.g. the spent fuel pool) may need to be analysed, depending on the formulation of the safety goals.

3.2. It should be recognized that the intended applications of PSA may impose additional requirements on the scope of the PSA, on the modelling approaches and on the level of detail. If such additional requirements are taken into account at the planning stage of the PSA project, it will help to avoid inconsistencies in the results and insights obtained. For instance, if it is planned to use the PSA for the development of a severe accident management programme, a Level 2 PSA should be performed. As another example, if it is planned to use the PSA model as a basis for a risk monitor, the PSA model should be 'symmetrical' in terms of the modelling of initiating events. The common simplification of modelling an

[6] PSA for low power and shutdown states is usually performed as part of the same study.

initiating event as always occurring in one particular train should not be used. For example, loss of coolant accidents should be modelled for each loop with an appropriate probability that a specific loop is affected (i.e. 1/2 for a two train plant, 1/3 for a three train plant) rather than a single event in one of the loops. More details on the features of PSA necessary for various applications of PSA are provided in Section 10.

PROJECT MANAGEMENT FOR PSA

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

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

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

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

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

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

3.5. It is generally considered desirable to start the process of performing the PSA as early as possible in the lifetime of the plant. Design weaknesses or

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

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

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

SELECTION OF METHODS AND ESTABLISHMENT OF PROCEDURES

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

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

TEAM SELECTION AND ORGANIZATION

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

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

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

ESTABLISHMENT OF A QUALITY ASSURANCE PROGRAMME FOR PSA

3.13. The quality assurance[7] programme for a PSA encompasses activities that are necessary to achieve the appropriate quality of the PSA and activities that are necessary to verify that the appropriate quality is achieved. For a PSA, appropriate quality means an end product that is correct and usable and one which meets the objectives and fulfils the scope of the PSA. The quality assurance programme should provide for a disciplined approach to all activities affecting the quality of the PSA, including, where appropriate, verification that each task has been satisfactorily performed and that necessary corrective actions have been implemented.

[7] Instead of the term ‘quality assurance’, the term ‘management system’ is used in Ref. [7]. The term ‘quality assurance’ is left in this Safety Guide in order to comply with widely accepted current practices and terminology used in the area of PSA.

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

GENERAL ASPECTS OF PSA DOCUMENTATION

Objectives and content of documentation

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

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

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

3.16. PSA documentation includes work files, computer inputs and outputs, correspondence, interim reports and the final report of the PSA. The documentation of PSA should be complete, well structured, clear and easy to follow, review and update. It should be presented in a traceable and sequential manner, i.e. the order of appearance of analysis in the final documentation should follow, as far as possible, the order in which it was actually performed. In addition, means should be provided for possible extensions of the analysis,

including integration of new topics, use of improved models, broadening of the scope of the PSA in question and its use for alternative applications. Explicit presentation of the assumptions, exclusions and limitations for extending and interpreting the PSA is also of critical importance to users.

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

Organization of documentation

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

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

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

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

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

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

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

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

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

4. FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION

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

(a) The safety analysis report for the plant;
(b) Technical specifications for the plant;
(c) System descriptions;
(d) As built (as is) system drawings (piping and instrumentation diagrams);
(e) Electrical line drawings, including circuit diagrams and trip criteria for the electrical bus protection system;
(f) Control and actuation circuit drawings;
(g) Normal operating procedures, emergency procedures, test procedures and maintenance procedures;

(h) Analyses pertinent to the determinants of mission success criteria of systems;
(i) Operational 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.

The plant documents containing the information necessary for the analysis should be collected and made available to the PSA team. Depending on the scope of the PSA, more specific information may be required, for example, plant layout and topography of the site and surroundings for PSA for external hazards. Interaction with operating personnel who are not part of the PSA team might be necessary for clarification and additional information.

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

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

5. LEVEL 1 PSA FOR INTERNAL INITIATING EVENTS FOR FULL POWER OPERATING CONDITIONS

5.1. This section provides recommendations on meeting Requirements 6–13 of Ref. [3] for Level 1 PSA for internal initiating events. This section provides recommendations on the technical issues that need to be addressed in carrying out a Level 1 PSA for internal initiating events caused by random component failures and human errors occurring at full power.

5.2. The recommendations on Level 1 PSA cover:

(a) General aspects of Level 1 PSA methodology;
(b) Initiating event analysis;
(c) Accident sequence analysis;
(d) Systems analysis;
(e) Analysis of dependent failures;
(f) Analysis of common cause failures;
(g) Human reliability analysis;
(h) Modelling of passive systems and computer based systems;
(i) Data required for a Level 1 PSA;
(j) Integration and quantification of the PSA model;
(k) Sensitivity studies and importance and uncertainty analysis.

The general framework for analysis is illustrated in Fig. 1.

GENERAL ASPECTS OF LEVEL 1 PSA METHODOLOGY

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

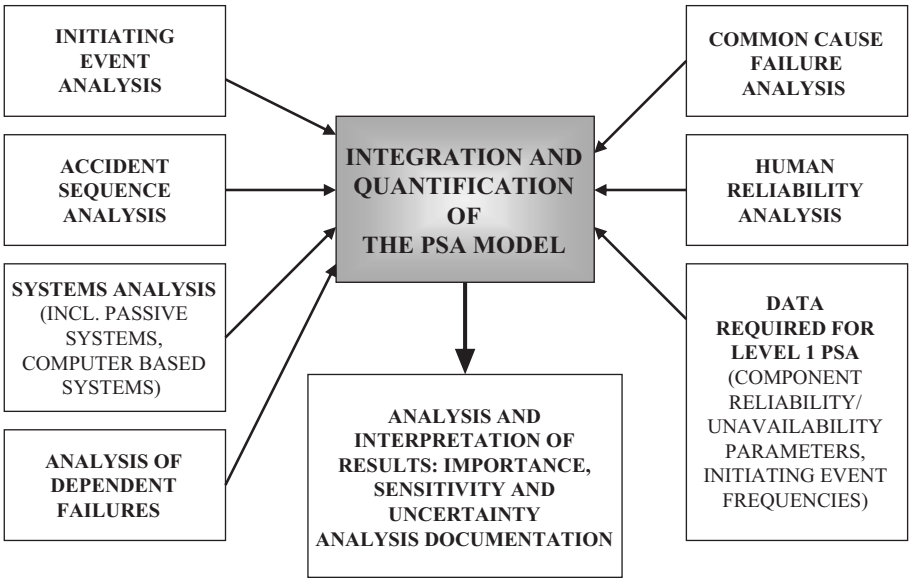

FIG. 1. General analysis framework of a Level 1 PSA for internal initiating events.

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

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

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

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

5.7. 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 bias the results unnecessarily. Hence, the Level 1 PSA should be based on best estimate models, assumptions and data. However, some conservatism may be necessary where there is a high level of uncertainty, in order to avoid unjustifiable optimism.

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

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

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

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

INITIATING EVENT ANALYSIS

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

5.12. This section deals with the identification of internal initiating events that could arise during full 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 low power and shutdown modes are provided in Section 9.

Identification of initiating events

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

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

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

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

events) that could arise through failure to operate, partial failure to operate or inadvertent operation.

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

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

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

5.19. The set of initiating events should include events of very low frequency with potentially large consequences, for example, rupture of the reactor pressure vessel, or loss of coolant accidents in interfacing systems. Inclusion of loss of coolant accidents in interfacing systems is particularly important if the Level 1 PSA is intended to be used as the basis for a Level 2 PSA (and possibly a Level 3 PSA).

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

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

5.22. A review of the operating experience of the nuclear power plant (if it is already operating) and of similar nuclear power plants should be carried out to

ensure that any initiating events that have actually occurred are included in the set of initiating events addressed in the Level 1 PSA.

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

Transients

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

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

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

5.26. When losses of off-site power that could occur due to internal hazards (such as a fire in the plant) and external hazards (such as extreme environmental conditions or an earthquake) are modelled explicitly in a PSA for those hazards, the definition of the loss of off-site power for the model for internal initiating events should exclude these causes so as to avoid double counting in the Level 1 PSA.

5.27. The set of initiating events should also include failures of support systems, for example, electrical power systems, instrument air, cooling water systems, room cooling systems and the instrumentation and control systems. This is

particularly important where the failure of a support system could lead to a reactor trip and the support system in question also has a role to play after a reactor trip.

Loss of coolant accidents

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

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

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

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

Grouping of initiating events

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

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

screening is performed, it may still need to be revisited for specific PSA applications.

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

(a) The accident progression following the initiating event;
(b) The success criteria for the mitigating systems;
(c) The effect of the initiating event on the availability and operation of safety systems and support systems, including the presence of conditions for signals that will actuate protection actions or block actuation of systems;
(d) The response expected from plant operators.

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

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

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

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

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

ACCIDENT SEQUENCE ANALYSIS

5.40. The next step in the analysis is to determine the response of the plant to each group of initiating events (as identified in accordance with the foregoing

procedure) that requires the operation of safety systems to carry out the safety functions to prevent core damage. Such safety functions typically include shutting down the reactor and keeping it subcritical, removal of heat from the reactor core, etc. (see para. 5.45).

5.41. The events that are identified in the accident sequences will relate to the success or failure of the safety systems and human actions taken in carrying out the safety functions required for the groups of initiating events. The end points of the accident sequence models will correspond either to a safe stable state where all required safety functions have been performed successfully or to core damage.

Core damage

5.42. A criterion (or criteria, if appropriate) should be developed for what constitutes core damage or a particular degree of core damage.[8] For example, for light water reactors, it is often assumed that core damage occurs if any of the fuel parameters (such as the clad temperature) exceeds its design basis limit or a higher limit if this can be justified.

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

Safety functions, safety systems and success criteria

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

5.45. The safety functions that need to be performed to prevent core damage should be identified for each initiating event group. The safety functions required

[8] Several core damage states can be specified, depending on the degree of the damage, for example, in channel type reactors, damage to different numbers of channels is usually considered depending on the severity of the consequences. Another factor in specifying the degree of core damage can be timing, e.g. delayed core damage.

will depend on the reactor type and the nature of the initiating event and will typically include:

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

5.46. The safety systems and operator actions that will need to be available to perform each of these safety functions should be identified, along with the success criteria for the safety systems used in performing these safety functions.

5.47. The success criterion for each safety system should be defined as the minimum level of performance required to achieve the safety function, taking into account the specific features of each sequence. Where redundant trains of the safety system are involved, the success criteria should be defined as the number of trains that are required to operate. Where diverse safety systems are involved, the success criteria should account for the performance required from each of the diverse systems. This could include partial operation of each of the diverse systems as supported by the best estimate safety analysis.

5.48. The safety systems that 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, for example, the electrical power and cooling water systems, or where the initiating event produces a harsh environment in an area where safety related equipment is located. In either case, this can lead to failure of the required safety systems. Another example arises in the case of a large or intermediate loss of coolant accident in a pressurized water reactor where, if the break occurs in a cold leg, the flow would be lost from the trains of the emergency core cooling system connected to that leg; this would need to be recognized in defining the success criteria.

5.49. The success criteria should specify the mission times for the safety systems, that is, the time that the safety systems will need to operate so that the reactor reaches a safe, stable shutdown state and that will allow for long term measures to be put in place to maintain this state. In many cases, this has been taken to be 24 or 48 h for most initiating events. For new designs that provide the features to delay core damage, consideration of a longer mission time may be necessary.

5.50. The success criteria should also specify requirements for support systems, based on the success criteria for the front line systems, which are performing safety functions directly.

5.51. The success criteria should define the operator actions required to bring the plant to a safe, stable shutdown state as defined by the plant procedures. It is good practice to specify operator actions in a cooperative effort between plant operators, systems analysts and human reliability analysts.

5.52. The Level 1 PSA documentation should include a list of the safety functions, safety systems, support systems and operator actions that are required for each initiating event to bring the reactor to a safe, stable shutdown state.

Analysis to support the specification of success criteria

5.53. The success criteria for the safety systems and the support systems used in the Level 1 PSA should be justified by supporting analysis. Supporting analysis would include the thermohydraulic analysis for decay heat removal following transients and loss of coolant accidents, neutronics analysis for reactor shutdown and hold-down, etc.

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

5.55. However, if conservative success criteria that are based on conservative design basis analyses have been used in the Level 1 PSA for some of the safety 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.

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

Modelling of accident sequences

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

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

5.59. The structure of the event tree should take account of the time sequence of the headings on the event tree representing operator actions 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 the operators.

5.60. The event tree structure should take into account functional and physical dependencies (see para. 5.87) that may occur as a result of equipment failures and human errors. Dependencies between safety systems (usually referred to as systems interactions) should also be represented on the event tree.

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

End points of accident sequences and plant damage states

5.62. The accident sequence analysis will identify accident sequences where all the required safety functions have been carried out in a satisfactory manner so that core damage will not occur, and accident sequences where one or more of the

safety functions have not been carried out so that core damage is assumed to occur. This distinction will generally be sufficient if the analysis is to stop at a Level 1 PSA. However, if the intent is to use the results of the Level 1 PSA as input to a Level 2 PSA, it is general practice to group the accident sequences that lead to core damage into plant damage states, which will form the interface between the Level 1 PSA and the Level 2 PSA. It is more useful if the plant damage states are specified as a part of the Level 1 PSA (rather than postponing the specification of plant damage states to the first step of the Level 2 PSA).

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

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

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

The list above is appropriate only for a PSA for full power operating conditions; for the low power and shutdown states, a different set of characteristics will be appropriate.

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

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

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

5.68. 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 system failures that are identified in the accident sequence analysis. This is usually done by means of fault tree analysis, where the top event of the fault tree is taken as the system failure state(s) identified by the event tree analysis. The fault trees extend the analysis down to the level of individual basic events, which typically include component failures (that is, failures of pumps, valves, diesel generators, etc.), 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.[9]

Fault tree analysis

5.71. The fault trees should be developed to provide a logical failure model for the safety 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 system function should be the logical inverse of the accident sequence success criterion, as specified in paras 5.47–5.56. In some cases, more than one fault tree model may be necessary for the same safety 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 (pumps, valves, diesel generators, etc.) and individual human errors and should include all the basic events that could lead, either directly or in combination with other basic events, to the top event of the fault tree. The level of the analysis is generally left to the discretion of the analyst, but it should be consistent with the available data on component failures and the proposed applications of the Level 1 PSA.

5.75. The set of basic events to be modelled in the fault trees should be identified by means of systematic analysis (for example, by means of a failure mode and

[9] 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).

effects analysis that has been carried out as part of the design assessment to identify important component failure modes) and a review of operator actions supported by task analysis to identify potential human errors.

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

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

5.78. 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 has the same effect on the system as the composite event itself. In addition, all the composite events included in the model should be functionally independent, i.e. no individual component should appear in more than one composite event, or elsewhere as a basic event.

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

5.80. The way that the unavailability of systems due to maintenance is modelled should be consistent with plant technical specifications[10] 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 safety systems, and all running and standby trains of normally operating systems. The development of a symmetrical model will allow the importance measures[11] calculated by the Level 1 PSA code to be used in a straightforward manner.

Required systems information

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

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

[10] 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.

[11] See para. 5.151 for examples of importance measures.

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 normal configurations of the components;
(c) The pipe segments or wiring segments connecting the components;
(d) The support system interfaces (power, electrical, cooling, etc.).

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

ANALYSIS OF DEPENDENT FAILURES

5.86. 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:

(1) **Functional dependencies** include dependencies resulting from plant conditions, for example, failure to depressurize leads to unavailability of low pressure injection, and dependencies due to shared components, common actuation systems, common isolation requirements or common support systems (power, cooling, instrumentation and control, ventilation, etc.).
(2) **Physical dependencies** (also referred to as **spatial interaction dependencies**) due to an initiating event that can cause failure of safety system equipment. This can occur due to pipe whip, missile impact, jet impingement or environmental effects.
(3) **Human interaction dependencies** due to errors made by the plant staff that either contribute to, or cause, an initiating event, or lead to the unavailability or failure of one or more items of safety system equipment so that they do not operate when required following an initiating event.
(4) **Component failure dependencies** due to errors in design, manufacture or installation or errors made by plant personnel during plant operation. These are addressed by a common cause failure analysis (see paras 5.92–5.95).

5.88. A systematic review should be carried out of the design and operation of the plant to identify all the potential dependencies that could arise, leading to the unavailability of safety 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 in the event tree or fault tree model. Human interaction dependencies and component failure dependencies should also be modelled; these are discussed further in paras 5.96–5.113 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 account of in the fault tree model. These should be identified and modelled explicitly in the fault tree analysis. It is good practice for the analysts to tabulate all these dependencies in a matrix of system dependencies, which can be used as a basis for constructing the fault trees and which is helpful to the reviewers in checking them. Functional dependencies should not be included among the component failure dependencies in the common cause failure probabilities of the system. Rather, component failure dependencies are reserved for the more uncertain dependencies that have not been explicitly identified and that are quantified by means of beta factors and similar models.

5.91. The intersystem functional dependencies that could arise due to shared components or support systems should be identified and modelled explicitly in the fault tree analysis. It should be noted that, in the linked event tree approach (see para. 5.6), intersystem functional dependencies can be addressed using the boundary condition method. Such dependencies could arise in separate safety 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 by the collection of data. Addressing both intrasystem and intersystem common cause failure events is considered a 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 the important 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 should take account of the level of redundancy in the system, the design aspects of the components, the layout of the system in terms of the levels of separation, segregation, equipment qualification, etc., 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 take account of data from the operation of similar plants and generic data. If generic common cause failure parameters are to be used for the calculation of common cause failure probabilities, the applicability of these values should be analysed and justified. The component boundaries, failure modes and failure root causes in the generic data sources to be used should be consistent with those assumed in the PSA. If expert judgement is to be used for the assignment of common cause failure parameters (when neither plant specific data nor generic data are available), an appropriate justification should be provided for the data and error factors assigned should be commensurate with the uncertainty in the process of specifying the common cause failure parameters.

HUMAN RELIABILITY ANALYSIS

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

frequency. A useful starting point would be to check the approach applied against one of the approaches generally used to ensure that all the necessary steps for a human reliability analysis are carried out.

5.97. The recommendations provided in paras 5.98–5.113 relate to the classical static representation of human behaviour in a Level 1 PSA, which is the most common approach used. More recently, the cognitive aspect of human behaviour in dynamic interaction with the working environment has been taken into consideration using more advanced methodologies, but this is not addressed here.

5.98. Although the techniques used for human reliability analysis have improved in recent years, there is a wide variety of methods available and the state of the art in this area is still evolving. The method chosen should be applied and documented consistently and correctly.

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

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

Identification of human interactions

5.101. A structured and systematic procedure should be applied for the identification of the human interactions that need to be included in the Level 1 PSA. This should include all types of human interaction, as indicated in paras 5.102–5.105, where errors can make a contribution to the core damage frequency.

5.102. The human reliability analysis should include human errors made before the occurrence of the initiating event that have the potential to lead to the failure or unavailability of safety related equipment or systems (usually referred to as Type A human interactions). These can occur during repair, maintenance, testing or calibration tasks. If such errors remain undetected, the component or component groups affected will be unavailable when required after an initiating

event. Particularly important are interactions that have the potential to result in the simultaneous unavailability of multiple trains of safety 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 carried out to identify the repair, maintenance, testing and calibration tasks carried out by the plant operators for the systems modelled in the Level 1 PSA and thereby to identify Type A human interactions. The review should determine the potential for errors to occur and the effect of these potential errors on the unavailability or failure of safety system equipment.

5.104. A systematic review should be carried out to determine potential human errors that could lead to an initiating event (Type B human interactions). As a minimum, a check should be carried out to ensure that human errors that could cause initiating events are 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 carried out to identify the critical actions that will need to be carried out by plant operators after the occurrence of an initiating event (Type C human interactions). The review should determine the potential for errors to occur and the effect of these potential errors on the unavailability or failure of a component or system. Type C human interactions usually provide a significant contribution to the core damage frequency and hence are often the most important human interactions identified in the Level 1 PSA.

5.106. To represent the impact of human errors, human failure events should be either incorporated as basic events in fault trees or used as event tree headings.

Derivation of human error probabilities

5.107. The human error probabilities derived should be scenario specific and should reflect the factors that can influence the performance of operators, including the level of stress, the time available to carry out the task, the availability of operating procedures, the level of training provided, the environmental conditions, etc. These factors (often called ‘performance shaping factors’) should be identified by task analysis.

5.108. The method used for the derivation of the human error probabilities should be consistent with the methods generally used in Level 1 PSAs or its use should be explicitly justified.

5.109. Qualitative descriptions should be drawn up for each of the key human interactions. These descriptions should specify all the significant aspects associated with the actions of the plant personnel and should typically include:

(a) The timing of the action.
(b) The relevant plant procedures.
(c) The environment in which the action is carried out.
(d) Operational practices, e.g. the structure of the operating crew and their responsibilities.
(e) The effect of prior actions on the action at hand.
(f) Information available to the operators, training they have undergone, etc.

5.110. The modelling of specific human interactions should be checked using appropriate techniques, for example, walk-through or talk-through procedures. Furthermore, observation of operator performance and human interactions in simulator exercises will provide useful information in support of the human reliability analysis.

5.111. 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.

Treatment of dependencies between human failure events

5.112. There are likely to be 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, incorrect procedures, an incorrect diagnosis or a plan of action in carrying out response actions, etc. 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.

5.113. All measurable cutsets (see para. 5.9) involving multiple human failure events should be identified. Such cutsets can be identified by setting the human error probabilities to a high value (e.g. 0.9) and recalculating the core damage frequency; the cutsets involving multiple human failure events will then appear at the top of the list of cutsets. The set of human failure events that are combined in

the same cutset 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.

OTHER MODELLING ISSUES

Passive systems

5.114. The current trend is to incorporate passive systems into the design of evolutionary plants to carry out safety functions such as decay heat removal and emergency core cooling. Passive systems are considered to have a higher reliability than active systems since they do not rely on support systems (such as electrical power and cooling water) and may not require active initiation by the protection system.

5.115. The boundary conditions for the operation of each passive system should be established by thermohydraulic analysis, experiment and testing. These boundary conditions will relate to the temperature, pressure, inventory, etc., for the system. If these boundary conditions are met, it can be assumed that the passive system will operate. If these boundary conditions are not met, it is assumed that the passive system will fail to carry out its function.

5.116. Failure of the passive system should be modelled in the analysis and the failure probability should be assessed. The modelling of the passive system should account for the probability of failure to meet the boundary conditions for system operation and should use the standard fault tree modelling techniques to address component failures (failure of non-return or relief valves to open, pipework blockage, etc.), human errors in setting up the system and failure of initiation (if external initiation is required). The uncertainties in the supporting analysis should also be accounted for.

Computer based systems

5.117. Computer based systems are increasingly being used in the control and protection systems for nuclear plants and this trend is expected to continue. Computer based systems rely on both hardware and software components. The reliability of the hardware can be assessed using standard techniques and the reliability of the software can be addressed to some extent through verification and validation programmes. However, it is more difficult to model the reliability

of a computer based system in the Level 1 PSA than it is for a hardware system, since there is no consensus on how to model failure of the software.

5.118. Since the overall probability of failure could be dominated by software failures, and at present it is not possible to derive a probabilistic model of software failure[12], a judgement needs to be made on the quality of production of the software, that is, whether adequate procedures have been followed to minimize the likelihood of errors being made in the production of the software, whether adequate checks have been made to detect errors in the code (static analysis) and whether adequate testing has been carried out for the completed code (dynamic testing).

5.119. Software reliability is currently an active area of research. However, if a judgement is made on the reliability of the software that takes account of all the relevant factors relating to the design, production and testing of the software, it may be incorporated into the Level 1 PSA model.

5.120. Where a control and protection system or two diverse systems carrying out the same safety function are both computer based systems, consideration should be given to whether there are any dependencies in the hardware and software of the two computer systems and, if so, this should be taken into account in the Level 1 PSA.

DATA REQUIRED FOR A LEVEL 1 PSA

5.121. Paragraphs 5.121–5.139 provide recommendations for the required data for initiating event frequencies, component failure probabilities, and component outage frequencies and durations. The required data for common cause failure probabilities and human error probabilities are discussed in paras 5.95 and 5.107, respectively. The recommendations for meeting Requirement 19 of Ref. [3] on use of operating experience data are also provided in paras 5.121–5.139.

[12] In this context, a 'probabilistic model of software failure' is taken to mean both the probability that, following an initiating event, the correct parameter values are input into the computer system but the correct output is not generated due to an error in the software and the consequences of that error.

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

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

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

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

5.126. 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 judgement.

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

Frequencies of initiating events

5.128. A frequency should be assigned to each initiating event group modelled in the Level 1 PSA. In determining this frequency, account should be taken of all the causes identified for the initiating event.

5.129. In addition to the techniques mentioned in paras 5.123–5.127, 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.

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

5.131. The frequency should be calculated for the initiating event groups. The frequency for the initiating event group should be the sum of the frequencies for all the individual initiating events assigned to that group.

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

Component failure probabilities

5.133. 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 operational regime, the boundaries defined for the component in the Level 1 PSA model and its failure modes.

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

5.135. For components such as pumps that are required to operate for some time post-trip, the mission time should be specified. Determination of mission times should take account of the time taken to reach a safe, stable long term shutdown state and for long term recovery actions to be established. Mission times can be very long for some initiating events such as a loss of coolant accident.

5.136. 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

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

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

5.139. 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

5.140. The logic model developed in the Level 1 PSA should be quantified using the data indicated in paras 5.121–5.139. The accident sequence frequencies are then calculated using the data for the initiating event frequencies, component failure probabilities, component outage frequencies and durations, common cause failure probabilities and human error probabilities.

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

5.142. Paragraphs 5.142 and 5.143 provide recommendations on meeting Requirement 18 of Ref. [3] on use of computer codes for a Level 1 PSA. The quantification of the Level 1 PSA should be carried out using a suitable computer code that has been fully validated and verified. A number of sophisticated Level 1 PSA computer codes that can be used to carry out this analysis are available commercially or have been developed in various States.

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

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

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

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

5.146. The analyst should provide a definition of the term ‘a significant contribution to the risk’ as used in para. 5.145. This could take the form of an absolute criterion or a relative criterion (e.g. relative to total core damage frequency).

5.147. A check should be made that any post-processing that has been carried out on the 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.

5.148. 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 cutsets (for the fault tree linking approach) and any post-processing that has been carried out.

5.149. The analyst should provide definitions of the terms 'significant sequence' and 'significant cutset' as used in para. 5.148. These could take the form of absolute criteria or relative criteria (e.g. relative to total core damage frequency).

5.150. 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 cutsets with a lower frequency are not included in the analysis. (It is also possible to specify an order cut-off so that 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

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

(a) The Fussell–Vesely importance[13];
(b) The risk reduction worth[14];

[13] 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.

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

(c) The risk achievement worth[15];
(d) The Birnbaum importance[16].

The various importance measures provide a perspective on which basic events, etc., 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).

Types of uncertainty

5.152. Paragraphs 5.152–5.160 provide recommendations on meeting Requirement 17 of Ref. [3] on uncertainty and sensitivity analysis for a Level 1 PSA. It is recognized that there will be uncertainties in the models developed and in the data used in the Level 1 PSA. These uncertainties should be addressed when using the results of a PSA to derive risk insights or in support of a decision. This can be done by carrying out sensitivity studies or an uncertainty analysis, as appropriate. The uncertainties in the Level 1 PSA are normally classified into three general categories as follows:

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

[15] The risk achievement worth is the relative increase in the frequency of core damage if the failure of the particular item of equipment is considered to be certain. The risk achievement worth is a measure of the importance of the function performed by the equipment. It identifies the equipment playing a major role with regard to safety, even if the failure rate of such equipment is very low.

[16] The Birnbaum importance measure is a measure of the increase in risk when a component is failed compared with when the component is operating.

(3) **Parameter uncertainty**: This arises due to the uncertainties in the parameters used in the quantification of the Level 1 PSA. This is the type of uncertainty that is usually addressed by an uncertainty analysis through specifying uncertainty distributions for all the parameters and propagating them through the analysis.

5.153. Consideration needs to be given as to how to use the uncertainty information in the design evaluation and decision making process. However, it should be noted that the risk criteria or targets for core damage frequency often relate to point estimates[17] rather than to uncertainty distributions. The way that the Level 1 PSA is used for the identification of weaknesses also relates to point estimates rather than to uncertainty distributions.

Sensitivity studies

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

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

5.156. The analyst should provide a definition of the term 'significant impact on the results of the Level 1 PSA' as used in para. 5.155. This could take the form of a numerical criterion in an absolute or a relative form (see para. 5.146), a qualitative criterion (e.g. introduction of a new accident sequence), or a combination of both quantitative and qualitative criteria (e.g. introduction of a new significant accident sequence).

5.157. The results of the sensitivity studies should be used to indicate the level of confidence that may be placed in the insights obtained from the PSA, that is, whether the core damage criterion or target has been met, whether the design is balanced and whether there are possible weaknesses in the design and operation

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

of the plant that have not been highlighted in the base case Level 1 PSA with which the sensitivity cases are compared.

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

Uncertainty analysis

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

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

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

INTRODUCTION

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

(a) **Internal hazards** originating from the sources located on the site of the nuclear power plant, both inside and outside plant buildings. Examples of internal hazards are internal fires, internal floods, turbine missiles, on-site

transportation accidents and releases of toxic substances from on-site storage facilities.

(b) **External hazards** originating from the sources located outside the site of the nuclear power plant. Examples of external hazards are seismic hazards, external fires (e.g. fires affecting the site and originating from nearby forest fires), external floods, high winds and wind induced missiles, off-site transportation accidents, releases of toxic substances from off-site storage facilities and severe weather conditions.

Such hazards can damage plant components and thus generate accident sequences that might lead to core damage (or to other end states as appropriate, if these are to be considered in the Level 1 PSA). Often, these hazards have the potential to affect many different pieces of equipment simultaneously and adversely impact plant personnel. Both internal and external hazards should be included in the Level 1 PSA.[18]

ANALYSIS PROCESS

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

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

The overall analysis approach is illustrated in Fig. 2.

6.3. While the stages of hazard identification and screening are similar for internal and external hazards, the bounding assessment and detailed analysis for each hazard may involve tasks that may be unique for the hazard considered, for

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

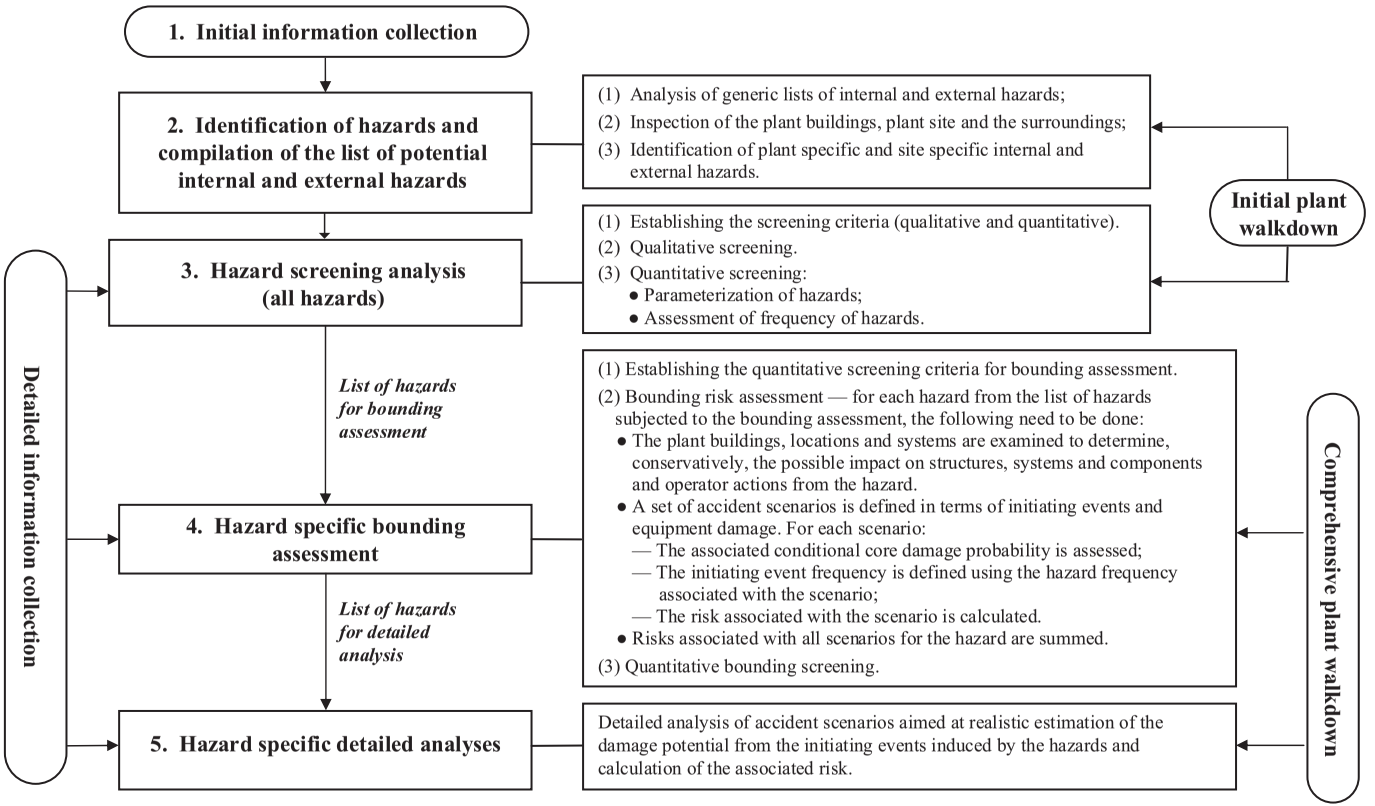

FIG. 2. Overall analysis approach for Level 1 PSA for internal and external hazards.

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

6.4. All potential internal and external hazards that may affect the plant should be considered and should be subjected to screening analysis, bounding assessment or detailed analysis, as appropriate.

6.5. As explained in para. 5.141, in Level 1 PSA for internal initiating events, in order to eliminate logic loops, reduced fault tree models are developed by removing submodels representing random failures of components. For example, to eliminate the logic loop between service water and power supply, the links to fault trees of specific buses are removed. Dependent failures of these components (whose random failures have been eliminated from the logic model) resulting from damage due to internal and external hazards should be incorporated in the Level 1 PSA models for internal and external hazards.

COLLECTION OF INITIAL INFORMATION

6.6. At the starting point of Level 1 PSA for internal and external hazards, all available information specifically relating to the internal and external hazards should be collected. This information should include, as 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, structures, systems and components.
(c) Plant layout and topography of the site and surroundings.
(d) Information on the location of pipelines, transportation routes and on-site and off-site storage facilities for hazardous materials.
(e) Location of industrial facilities in the vicinity of the site.
(f) Historical information on the occurrence of any internal and external hazards at the site, in the region, etc.

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

IDENTIFICATION OF HAZARDS

6.8. The task of hazard identification should aim to generate a comprehensive list of potential internal and external hazards. Examples of specific hazards are:

Internal hazards inside plant buildings:

(a) Internal fires;
(b) Internal floods;
(c) Internal missiles;
(d) Internal explosions;
(e) Heavy load drops.

External natural hazards:

(a) Seismic hazards;
(b) External fires;
(c) External floods;
(d) High winds;
(e) Biological phenomena, for instance, abnormal fish population in the cooling pond;
(f) Extreme meteorological conditions[19].

External human-induced hazards:

(a) Off-site explosions;
(b) Off-site toxic substance releases;
(c) Aircraft crashes.

[19] According to Ref. [8], extreme meteorological conditions include extreme temperature, extreme atmospheric moisture, snow precipitation (also blizzards) and ice pack, and lightning. Other hazards may be connected to these, such as frazil ice, frost and hail.

6.9. To ensure that the process of identification of hazards is comprehensive and traceable, a two step approach should be applied as follows:

(1) Use of the methods for internal and external hazard analysis available internationally. As a starting point, the hazards listed in various related IAEA publications (e.g. Refs [8–10]) and examined in past studies should be included in the list. Annex I provides an example of a generic list of potential internal and external hazards.
(2) Identification of site specific and plant specific internal and external hazards in a structured framework that makes possible a comprehensive check.

6.10. For existing plants, an integral part of the process of identification of internal and external hazards should be site survey and plant walkdown.

6.11. A list of potential combined hazards should be developed. Combinations of hazards may have a significantly higher impact on plant safety than each individual hazard considered separately, and the frequency of occurrence of a combination of hazards may be comparable to that of the individual hazards, e.g. high level water due to storm precipitation and dam failure caused by storm precipitation. The process of identification of hazards should include the identification of all combinations of hazards that may be significant for risk.

6.12. The possible combinations of hazards should be identified on the basis of the list of individual internal and external hazards. The entire list of potential hazards should be used for this purpose before any screening analysis is carried out. Usually, combined hazards involve only natural hazards (e.g. a combination of heavy 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).

6.13. The general approach used for the identification of a realistic set of combinations of hazards should be based on a systematic check of the dependencies between all internal and external hazards. The following causes for combinations of hazards should be considered:

(a) Hazards have the potential to occur under the same conditions and at the same time (e.g. high winds and snow precipitation).
(b) One external hazard can induce other hazards (e.g. a seismically induced external flood accompanied by dam failure).

(c) External hazards can induce internal hazards (e.g. seismically induced internal fires or floods).
(d) One internal hazard can induce other internal hazards (e.g. internal floods induced by internal missiles).

The impact of combinations of hazards on safety functions should be reassessed as they may affect different safety functions or the same function in a more severe manner than a single hazard.[20]

SCREENING OF HAZARDS

6.14. A successive screening process is generally established to minimize the emphasis on internal and external hazards whose significance to risk is low and to focus the analysis on hazards that are risk significant. The successive screening process should be applied consistently and screening criteria should be specified in a manner that ensures that none of the significant risk contributors from any internal or external hazard relevant to the plant and the site are omitted. The results from the screening process should be presented in the Level 1 PSA documentation.

6.15. The following screening criteria, which can be used either individually or in combination, are typically applied:

(a) On the basis of qualitative arguments, the hazard will not lead to an initiating event. For external hazards, this criterion is generally applied when the hazard cannot occur close enough to the plant to affect it. 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 that there will be sufficient time to eliminate the source of the threat or to provide an adequate response.
(c) The hazard is included within the definition of another hazard.

---

[20] The following are examples of some potential combined external hazards:
(a) Drought (due to high air temperature) and strong wind and smoke from forest fire;
(b) Strong wind and lightning;
(c) High air temperature and high water temperature;
(d) Snowfall and strong wind;
(e) Drifting snow and strong wind;
(f) Drifting snow and strong wind and frazil ice.

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

6.16. The quantitative criteria for screening out hazards should depend on the overall objective of the Level 1 PSA and should correlate with the core damage frequency from internal initiating events and from internal and external hazards. 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.

6.17. None of the criteria listed in para. 6.15 are applicable to internal hazards that originate inside plant buildings. These hazards should not be screened out as an entire hazard category and should always be the subject of either bounding or detailed analysis.

6.18. 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).

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

(a) Seismic hazards;
(b) Human-induced hazards;
(c) Wind hazards.

6.20. In order to eliminate specific hazards from the high wind category, it should be proven that the climatic conditions specific to the location of the plant support the assumption that these hazards are not sufficient to damage the plant (e.g. hurricanes in a non-coastal area). Wind hazards with a certain potential for damage should be screened out only when it is demonstrated that the frequency of exceedance of a particular wind velocity is negligible. The combination of wind with other hazards, such as rainfall or flooding, should be considered. When screening is performed, it is necessary to include in the analysis the possibility of

objects being picked up by the wind (mainly in the case of tornadoes and hurricanes) and turned into missiles.

6.21. For the screening process for external flood hazards, the following should be taken into consideration:

(a) The location of the nuclear power plant with respect to distance to a river, sea or lake, and the possibility of any flood reaching the site.
(b) The warning time[21]:
    (i) This can be long enough to allow shut-off operations in plants located at river sites (e.g. more than one day in advance).
    (ii) For plants located at coastal sites, in general, the warning time is shorter and may sometimes be only a matter of hours or minutes in the case of a local tsunami.
    (iii) In addition to the warning time, the time dependent likelihoods of success in receiving the warning and of the success of potential preventive actions should also be considered.
(c) The type of structure in place for retaining water.
(d) It is possible that other, adjacent areas will be inundated as the flooding occurs and that the flood level will be higher than expected. A plant at the edge of a narrow flood plain is more likely to be flooded than a plant located in a wide delta area.

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

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

6.24. Initiating events occurring at the plant may be the result of the impact of a single hazard or a combination of two or more hazards. While using the screening

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

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.[22]

6.25. A review of the actual status of the plant and the surroundings should be performed while applying screening criteria, in order to verify that changes in the original design conditions are not significant or are taken into account in the PSA. In particular, changes that have the potential to cause new hazards or to lead to an increased frequency of hazards of a certain magnitude should be thoroughly investigated.[23]

7. SPECIFICS OF LEVEL 1 PSA FOR INTERNAL HAZARDS

INTRODUCTION

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

---

[22] An example of such a combination of hazards is high winds and external floods. Even if each hazard could be screened out, the combination of hazards may have much higher impact on the risk to the plant, for example, when external floods are accompanied by, or even caused by, high winds.

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

(a) Changes in military and industrial facilities within a 30 km radius around the site or changes in nearby transport routes (i.e. railways, aircraft, roads and rivers) leading to changes in the range and magnitude of human-induced external hazards.
(b) Changes in dam construction on rivers above the plant site leading to an increase in the damage potential of the external flood hazard.
(c) Changes in environmental conditions (average annual wind speed and maximum annual wind speed, water level, temperature, local precipitation, etc.) leading to an increase in the frequency of natural external hazards with higher damage potential, etc.

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

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

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

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

7.3. Some internal hazards (internal explosions, fires, floods, etc.) can occur in a variety of different locations in the plant (rooms, buildings or elsewhere on the site). In such cases, the hazard characterization should specify:

(a) First, a global plant analysis boundary so that all locations that could contribute to the hazard risk are considered;
(b) Second, enclosed plant areas, assuming that the existing protection features (physical separation, barriers, isolation equipment, etc.) in the plant design will effectively contain the damage inside the areas.

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

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

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

where:

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

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

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

7.6. The impact analysis should consider the effect of hazard induced component failures on initiating events included in the PSA and on associated mitigatory safety functions. Detailed analysis based on physical studies

(e.g. simulations of fire scenarios or flooding propagation scenarios) should be carried out to reduce undue conservatism leading to overestimation of the risk posed by the hazard.

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

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

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

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

7.11. The combination of the probabilities of hazard induced failures of safety related components 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:

(a) The possibility of a fire at any location in the plant.
(b) The potential spread of fire to other locations.
(c) Fire detection, fire suppression and confinement of fire.
(d) The possibility of damage to equipment due to actuation of fire suppression systems (e.g. spray and flood caused by fire suppression systems may

damage equipment that would otherwise survive a fire, or the failure mode of such equipment may be altered).

(e) The effects of fire on pieces of equipment (components as well as their associated instrumentation and control and power cables). The effects considered should include new failure modes resulting from spurious actuation of equipment caused by 'hot shorts'.

(f) The possibility of damage to such equipment and, in the case of severe fires, to the integrity of the structures of the plant (walls, ceilings, columns, roof beams, etc.).

(g) The impact of random equipment failures and human errors.

(h) The effects of the fire, both direct (e.g. the need to evacuate the control room) and indirect (e.g. confusing information resulting from spurious indications), on operator actions.

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

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

(a) Smoke may cause electronic devices to fail.

(b) The human error probability may be higher due to unusual environmental conditions (smoke, which may be toxic as well as merely irritating, and heat) imposed by the fire event.

(c) The presence of smoke may necessitate evacuation of the main control room.

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

(a) The specific items of the methodology for a Level 1 PSA for internal initiating events for low power and shutdown conditions, as presented in Section 9.

(b) The screening should be performed separately to take account of the greater fire loads and higher number of potential ignition sources, particularly transient combustibles associated with maintenance operations performed during low power and shutdown modes.
(c) The fire protection means available.
(d) The potential for further paths for fire propagation (e.g. some doors may be open during low power and shutdown modes).
(e) The increased occupancy of different plant locations during outages may improve the fire detection capabilities.
(f) The fire related plant operational and configuration changes that are implemented to control combustibles and those that are performed to provide compensatory measures for system or component outages.

7.16. Deterministic fire hazard analysis carried out during the design (see Ref. [9]) and the operation (see Ref. [11]) of the plant should be used to provide an important input to the Level 1 PSA for internal fire, for example, the list of components and cables and their locations, the partitioning of the plant into fire compartments taking into account functional and detailed fire impact analyses performed for designing the fire protection features.

7.17. The approach to the Level 1 PSA for internal fire should be based on a systematic analysis of all locations within the plant boundary. To facilitate this examination, the plant should be subdivided into distinct physical units ('fire compartments'[24]), which are then scrutinized individually. The plant partitioning carried out in the design may be useful as an initial point for division of these physical areas. Criteria applied for specifying fire compartments should be justified and documented. Some flexibility may be exercised by the analyst in defining fire compartments for use in Level 1 PSA. For instance, the analyst may prefer to consider several fire compartments as one compartment, if this facilitates the screening analysis. Division of the plant into a large number of small locations may not be necessary, at least at the early stage of the PSA analysis.

[24] In Ref. [9], a fire compartment is defined as a building or part of a building that is completely surrounded by fire resistant barriers, i.e. all walls, the floor and the ceiling. In contrast to this, in the context of a PSA for internal fires, a fire compartment could be a well-enclosed room that is not necessarily surrounded by fire resistant barriers.

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 7.19–7.65. 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. According to 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

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

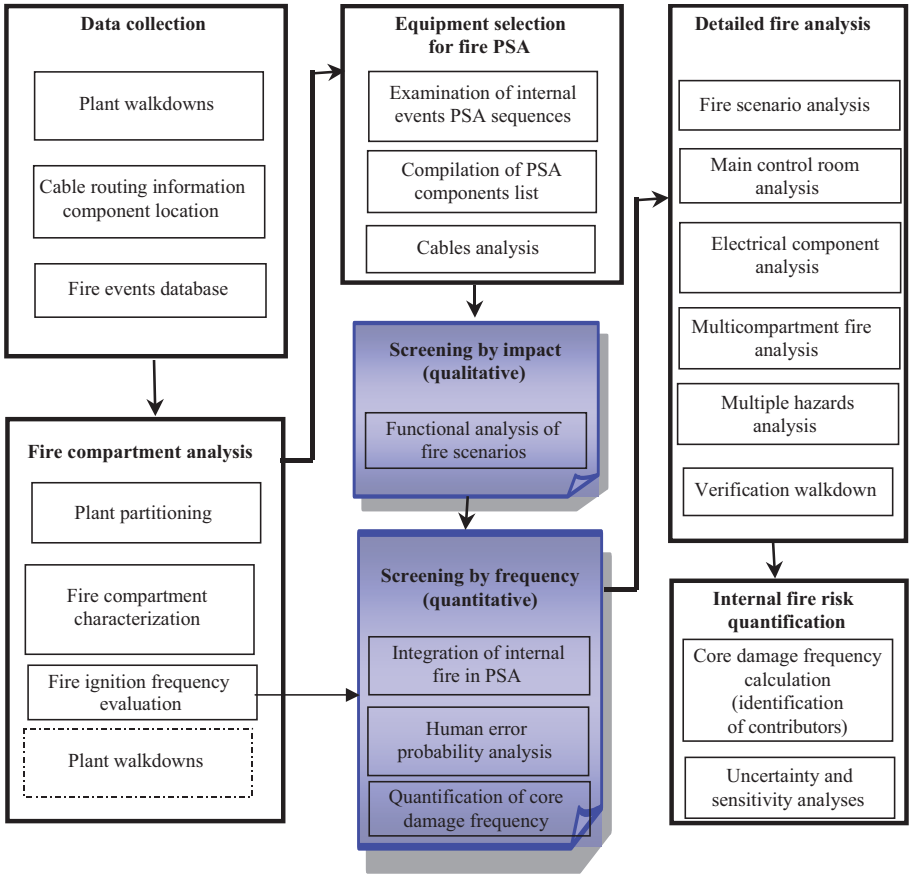

FIG. 3. Process for development of a Level 1 PSA for internal fire.

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 account for fire induced conditions.

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

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

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

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:

(a) Their physical boundaries (walls, doors, dampers, penetrations, etc.);
(b) The fire protection features;
(c) The fire resistance (fire rating) of the barriers surrounding the compartment;
(d) The components and cables located inside the fire compartment;
(e) Adjacent fire compartments and the connections to these;
(f) Ventilation paths (ducts) that may connect the fire compartment to be analysed with non-adjacent fire compartments;

(g) The fire load (e.g. type, amount, whether protected or unprotected, location, local distribution and whether permanent or temporary);
(h) Potential ignition sources (e.g. type, amount, location);
(i) Procedures for control of combustible material;
(j) Occupancy level (i.e. the possibility of detection of the fire by personnel);
(k) Accessibility of the location (e.g. for the fire brigade).

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

7.24. Estimation of the frequency of ignition of fires for fire compartments is an important part of the Level 1 PSA for internal fire and should be performed either before screening for all fire compartments, or at the beginning of the quantitative screening process for the most important fire compartments that survive the qualitative screening process (see para. 7.41). The frequency of ignition associated with fire ignition sources should be evaluated using the recommendations in Section 5, as far as feasible with plant specific data. When plant specific data are insufficient, generic data should be used for estimation of the fire ignition frequency along with the available plant specific data, adjusted in respect of the actual sources of fire ignition (including sources resulting from hot work), and the amounts of permanent and temporary combustible material in the fire compartments.

Selection of equipment for Level 1 PSA for internal fire

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

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

Failures such as these may 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.

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

7.27. Identification of all related cables and circuits associated with the components specified in paras 7.25 and 7.26 and analysis of cable routes should be an integral part of this examination. In addition, non-electrical circuits such as instrument air control lines should be considered for potential damage due to fire.

7.28. 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

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

7.30. If screening by impact is performed, it should be based at least on the following criteria or on combinations of these criteria. A fire compartment may be screened out on the basis of negligible potential impact on plant safety if:

(a) The fire load density is below a specified accepted threshold; OR
(b) All of the following conditions hold:
    (i) No equipment is present in the compartment that can cause an initiating event or can require manual shutdown; AND
    (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; AND
    (iii) The potential for spreading of fire effects to other fire compartments containing safety related equipment is very low.

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

7.32. Screening by impact should also cover multicompartment fire scenarios developed under pessimistic assumptions for fire spreading. For each fire compartment, complexes of compartments where fire could propagate are defined by adding to that compartment all adjacent compartments (in all directions) and by adding all connected compartments that share ventilation without their necessarily being adjacent to the compartment. Then all possible combinations of fire compartments should be analysed with regard to the potential for spread of fire to adjacent (or connected) fire compartments. To limit the number of combinations that require consideration, general assumptions could be made regarding the reliability and effectiveness of fire barrier elements (e.g. simultaneous independent failures of barriers may be considered very unlikely).

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

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

Screening by contribution to core damage frequency

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

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

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

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

Human error probability analysis

7.38. In determining the contribution of fire to the core damage frequency or calculating the conditional core damage probability, human error probabilities credited in the Level 1 PSA for internal initiating events should be reviewed, considering deviations from the emergency operating procedures and specific procedures for fire mitigation. Any deviations from the approaches used for human reliability analysis for the Level 1 PSA for internal initiating events, as presented in Section 5, should be justified and documented.

7.39. 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, potential existence of contradictory signals, smoke, loss of lighting and difficulty in entering or passing through the affected fire area.

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

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

7.41. For the quantitative screening task, the contribution of fire to the core damage frequency should be assessed for each fire compartment, considering the corresponding frequency of the fire scenario, according to the general formula given in para. 7.5.

7.42. 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:

(1) 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).
(2) The criterion for screening individual fire compartments should be set to a value high enough to allow some screening, but sufficiently low as to retain all risk significant fire scenarios.

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

7.44. The result of the entire screening process (by impact and by frequency) will be a list of fire scenarios associated with fire compartments that may represent significant contributors to risk and which need further consideration. For each fire scenario on this list, a quantitative Level 1 PSA model for internal fire should be developed for further analysis.

Detailed analysis of fire

Analysis of fire scenarios

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

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

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

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

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

features). The recommendations in Section 5 should be applied for determining such fire propagation event trees.

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

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

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

7.53. 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 control room

7.54. The Level 1 PSA model for internal fire for the main control room should take into account the specific features associated with this location, such as the widespread effect of a fire in the main control room across all safety systems, the potential for spurious actuation of systems and the impact of fire in the main control room on operator actions. The latter should include:

(a) The effects of fire and smoke on the availability of instrumentation and related equipment;
(b) The capability of features for fire detection and suppression, including the potential adverse impact of flooding;
(c) The use of an alternative location for safe shutdown, taking into account aspects of accessibility and other possible limitations;
(d) The effects of the spreading of smoke and toxic gases.

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

Analysis of the fire in the electrical component room

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

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

Multicompartment fire analysis

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

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

Analysis of multiple hazards

7.59. The potential for occurrence of other consequential internal hazards (e.g. flooding caused by actuation of a fire extinguishing system discharging a large amount of water, explosion of hazardous material caused by fire, fire caused by explosion) should be identified and should be considered in the Level 1 PSA for internal fire.

7.60. If not addressed in the Level 1 PSA for external hazards (e.g. seismicity, lightning, external fire, airplane crash), particular consideration should be given in the qualitative analysis to internal fires induced by other hazards: fire

compartments where the combined impact of other hazards and fire could be important for safety, ignition sources induced by hazards, spurious actuation or degradation of fire suppression systems, difficulties in carrying out manual fire fighting actions, etc., (see the recommendations on Level 1 PSA for external hazards presented in Section 8).

7.61. The following effects of internal fire induced by other hazards on the performance shaping factors of operators should be taken into account as a minimum:

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

Quantification of risk of internal fire

7.62. 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.

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

7.64. The quantification of the Level 1 PSA model for internal fire, the uncertainty analysis and the sensitivity analysis should 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 be performed for the important assumptions. The relative importance of various contributors to the calculated results should be determined.

Documentation for Level 1 PSA for internal fire

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

(a) Description of the fire protection features specific to the plant, including passive and active mitigation features of the plant as well as partitioning of the plant into fire compartments.
(b) Description of the specific methods and data used for assessing the fire hazard.
(c) Specific changes made in the Level 1 PSA model for internal initiating events aimed to account for effects of internal fire.
(d) Characterization of fire compartments.
(e) Justification for the screening of particular fire compartments from the analysis.
(f) Results of the specific analyses for detailed fire scenarios, the main control room, the electrical component room, multicompartment fire, multiple hazards, etc.
(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) Report of the plant walkdown in support of fire analysis.

ANALYSIS OF INTERNAL FLOODING

General

7.66. 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 7.67–7.92. For a Level 1 PSA for internal flooding for low power and shutdown modes, the same aspects listed in para. 7.15 should be considered.

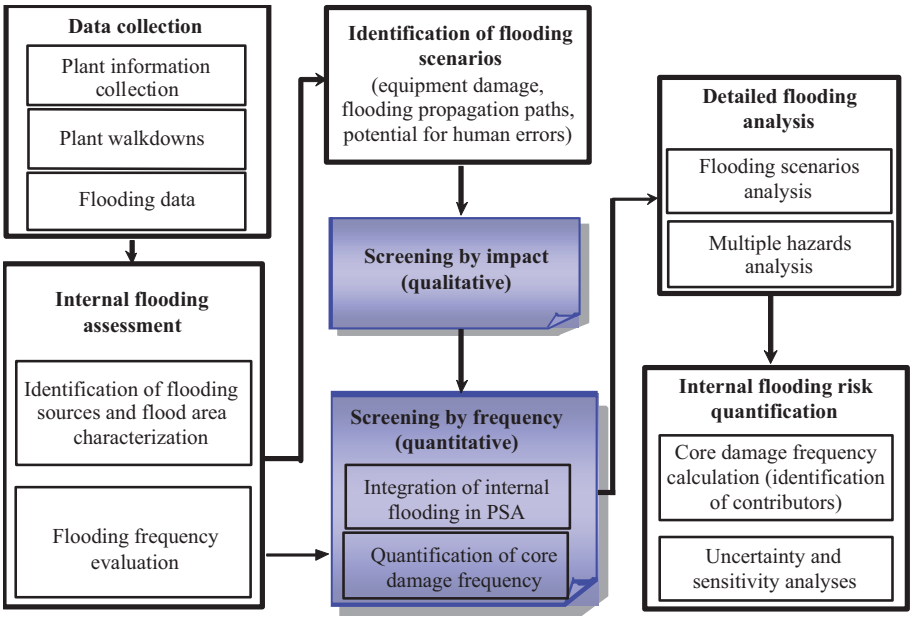

FIG. 4. Process of development of a Level 1 PSA for internal flooding.

Data collection and assessment of potential for internal flooding

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

7.68. Possible internal flooding events should be identified and characterized (see Ref. [10] for general considerations on flooding in the design of nuclear power plants). In carrying out this task, consideration should be given to:

(a) Possible sources of flooding: pipes, internal tanks, pools, valves, heat exchangers, connections to open-ended sources (e.g. sea, lake, river), multiunit shared systems or structures, etc.
(b) Possible flooding mechanisms: breaks, leaks, rupture, spurious or desired actuation of a spray system (e.g. the containment spray system or the fire extinguishing system) or human error during operation or during maintenance related activities (e.g. wrong positioning or inadvertent opening of a valve).

(c) Characteristics of the flood: capacity (depending on whether the source of flooding is a closed or open system), flow rate, temperature and pressure, presence or possible production of steam.
(d) Flooding related alarms, leak detection systems, capacity of draining systems and flooding related protection for components (such as equipment trip signals).
(e) Critical flooding heights of components relevant to PSA and room dimensions in the flooding areas.

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

7.70. 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 multiunit aspects and account should be taken of the potential for failure of flood barriers due to accumulated water.

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

7.72. The frequency of internal flooding events should be evaluated by following the recommendations in Section 5. As far as feasible, plant specific data should be used. When plant specific data are insufficient, it is possible to use generic data or expert judgement with appropriate justifications.

7.73. The main data for evaluation of the frequency of internal flooding events are estimates of pipe failure rates and rupture frequencies with associated uncertainties. Data should be selected for piping systems that represent significant sources of internal flooding. In addition, the frequency and severity of flooding events caused by human error should be evaluated, considering plant specific maintenance procedures and experience.

Identification of flooding scenarios

7.74. For each internal flooding event, structures, systems and components that could be affected by the flooding 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.

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

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

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

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

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

Screening by impact

7.80. Screening of flooding scenarios by their impact should be performed. Critical flooding scenarios can be selected by screening out plant compartments on the basis of negligible potential impact on plant safety. On the basis of the following qualitative criteria, a plant compartment may be screened out from the analysis if:

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

Screening by contribution to core damage frequency

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

7.81. Internal flooding events should be further screened for their contribution to the core damage frequency. Therefore, the Level 1 PSA for internal initiating events should be modified to account for flooding phenomena (both system models and operator actions).

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

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

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

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

7.84. Quantitative criteria for screening according to contribution to the core damage frequency should be defined for Level 1 PSA for internal flooding. Examples of such criteria could be:

(a) The cumulative contributions of all screened out flooding scenarios to core damage frequency should be under a specified threshold.

(b) The criterion for screening a single flooding scenario should be set to a value high enough to allow some screening but sufficiently low as to retain all risk significant flooding scenarios.

Detailed analysis of flooding

Analysis of flooding scenarios

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

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

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

7.87. Flooding scenarios should describe the time dependent course of a flood originating in a selected plant area and the subsequent component failures (see para. 7.74). A flooding scenario can be represented by event trees for flooding where all important features affecting flood development (design of flood barriers, flood detection and isolation of flooding sources) and probabilities of component failures are modelled. Generally, dedicated walkdowns should be performed in carrying out the Level 1 PSA for internal flooding in order to gather supporting information for verification of the detailed flooding analysis.

7.88. Additional human actions that may be necessary to mitigate flooding sequences should be identified and assessed with respect to their probability of succeeding or failing to detect and control the flooding. These include, for example, isolation and subsequent restoration of the electrical power supplies. The approach to human reliability analysis should take into account the possible

loss of instrumentation and control equipment and spurious indications that may be caused by the flooding.

Analysis of multiple hazards

7.89. Flooding and damage to structures, systems or components due to high energy pipe breaks should be treated in the Level 1 PSA for internal flooding if it has not been included as part of the Level 1 PSA model for internal initiating events.

7.90. Flooding caused by actuation of a fire extinguishing system discharging a large amount of water should be addressed in the context of the Level 1 PSA for internal fire (see para. 7.59).

Quantification of risk of internal flooding

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

Documentation for Level 1 PSA for internal flooding

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

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

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

OTHER INTERNAL HAZARDS

Analysis of heavy load drops

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

7.94. If the pathway along which a load is transported is located neither above the fuel nor above the regions containing critical equipment, screening out of individual initiators of heavy load drops may be possible.

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

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

7.97. The Level 1 PSA for heavy load drops should be consistent with the plant response model developed for the Level 1 PSA for internal initiating events for low power and shutdown modes (see para. 9.11).

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

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

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

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

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

Analysis of turbine missiles

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

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

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

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

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

7.108. Failure probabilities resulting from missile impact together with the probabilities of random failure of surviving safety related equipment 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.

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

Analysis of internal explosion

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

7.111. The design of the nuclear plant building basically considers the prevention and mitigation of explosions (see Ref. [9]). For that purpose, systematic analysis of explosions is used to characterize the potential sources of explosions (nature and quantity of the explosive materials, localization), the potential impacts of deflagrations or detonations on the plant (overpressure, impulse or drag loads, fire or heat) and prevention features. The Level 1 PSA for internal explosion should rely mainly on the information and data collected during these analyses to allow the qualitative screening out of explosion scenarios.

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

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

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

8. SPECIFICS OF LEVEL 1 PSA FOR EXTERNAL HAZARDS

INTRODUCTION

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

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

GENERAL ASPECTS OF BOUNDING ANALYSIS FOR EXTERNAL HAZARDS

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

8.3. In the bounding analysis, all potential impacts of each non-screened external hazard on the nuclear power plant should be considered.[25]

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

[25] Examples of impact categories (see Ref. [12]) are as follows:
(a) Loss of off-site power or station blackout;
(b) Degradation or loss of ultimate heat sink;
(c) Explosion or release of hazardous material;
(d) Degraded or isolated plant ventilation (owing to risk of toxic impact).

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

8.6. In the bounding analysis, combinations of external hazards should also be considered.

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

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

Seismic hazards

8.8. As seismic hazards appear to be important contributors to core damage frequency in many Level 1 PSAs, 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 bounding analysis for seismic hazards of a certain range. The secondary effects of seismic hazards (e.g. seismically induced fires and floods) should also be considered at this stage. Apart from this Safety Guide, detailed recommendations for seismic evaluation of existing nuclear installations, including considerations for PSA, are provided in Ref. [13].

High winds

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

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

The combination of high winds with other hazard phenomena should be considered, with account taken of possible dependencies (e.g. high winds and high water levels).

External floods

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

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

The combination of external floods with other hazard phenomena should be considered, with account taken of possible dependencies (e.g. high water level, consequential dam failures).

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

Other natural hazards

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

8.13. The combination of natural hazards with other hazard phenomena should be considered, with account taken of possible dependencies (e.g. severe weather conditions, high winds).

Human-induced hazards

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

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

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

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

PARAMETERIZATION OF EXTERNAL HAZARDS

General aspects

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

Seismic hazards

8.16. Seismic hazards are characterized by several parameters:

(a) The intensity, which is a descriptive index to measure the effects and damage.
(b) The ground motion, e.g. acceleration, velocity, displacement.
(c) The frequency content, which is generally represented by a response spectrum.
(d) The full time history of the seismic event, in terms of acceleration, velocity, displacements, etc.

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

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

8.17. The spectral acceleration or the averaged spectral acceleration over a selected band of frequencies should be used when available data support its estimation.[26]

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

8.19. Earthquake ground motion should not be screened out.

High winds

8.20. Different parameters should be considered depending on the wind type:

(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, etc.

External floods

8.21. The damage potential of external floods can be characterized by the discharge, velocity, water level, duration and contribution of wave action. Some or all of these parameters should be estimated for the characterization of external floods. For floods, the following parameters are commonly used:

(a) River: water level, water discharge/velocity and duration of flood.
(b) Sea/lake: water level, duration of flood and velocity.

[26] The spectral acceleration provides more comprehensive information than the peak ground acceleration.

(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.

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

Other natural hazards

8.23. 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.

8.24. 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

8.25. For each human-induced hazard, the parameters should be defined on the basis of their specific damage potential, for example:

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

8.26. Each human-induced hazard may result in a combination of various impact factors that have to be considered. For example, an aircraft crash may cause direct damage, explosion, fire and vibration. Similarly, a pipeline accident may result in a blast (impulsive load resulting from deflagration or detonation), fire and vibration. It may also produce missiles that can affect different parts of the plant. In the characterization of the 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, etc.

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

8.28. The combination of the human-induced hazard with other hazard phenomena should also be considered, with account taken of possible dependencies (e.g. chemical release, wind speed and direction).

DETAILED ANALYSIS OF EXTERNAL HAZARDS

8.29. A detailed analysis should be performed for all hazards that survive initial screening and for which the bounding analysis produces results from which, for particular application, it is difficult to draw conclusions and recommendations or to judge the significance of the contribution to risk from the hazard or an accident scenario.

8.30. When the bounding analysis cannot provide insightful results for the entire hazard, but only for hazards with a certain magnitude, the entire hazard should be divided into subcategories and detailed analysis should be performed for specific subcategories or for associated scenarios. The availability of the Level 1 PSA model for internal initiating events is a prerequisite for carrying out the detailed analysis of the external hazards.

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

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

FREQUENCY ASSESSMENT FOR EXTERNAL HAZARDS

General aspects

8.33. The purpose of the frequency assessment for external hazards is to acquire detailed site relevant information on the relationship between strength (as represented by some parameter for the hazard) and frequency of occurrence for each potentially relevant external hazard (the 'hazard curve'). Information sources for the plant and its environment should be used in the frequency assessment.

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

8.35. The hazards analysis (the estimation of the frequency of exceedance of a particular intensity) should be based on a probabilistic evaluation specific for the site that reflects recent available data, site specific information, and as-built and as-operated plant conditions if the corresponding data are available. Either historical data or phenomenological models or both should be used in the analysis. Up to date data on the occurrence of hazards and state of the art methodology should be always used when available. Typically, a family of hazard curves is developed to represent uncertainty in the characterization of the hazard.

8.36. Analysis of time trends should be performed to confirm the absence of trends towards increased frequency of the hazards. Recent, short term trends to decreasing hazard frequencies should not be accounted for unless they are well understood as being caused by processes having a non-random nature.[27]

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

8.37. When the hazard frequencies are developed on a regional or generic basis, correlation analysis should be performed with the aim of understanding the extent to which these data are applicable to the specific site and are up to date. The uncertainties associated with the use of regional and generic data should be reflected in the family of hazard curves, if provided (see para. 8.35).

8.38. 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. The procedure should ensure that a formal, highly structured and documented process is established with at least the following conditions being met:

(a) Qualified experts capable of evaluating the relative credibility of multiple alternative hypotheses in order to explain the available information are selected.
(b) Independence of the experts' opinions is maintained.
(c) The uses, rationale and background information for expert judgement are documented in a way that is traceable and reproducible.
(d) Uncertainties and variabilities in expert judgement are stated. The impacts or effects of these uncertainties and variabilities are assessed.
(e) The conclusions that are based on the results of the process have a sound basis.

Seismic hazards

8.39. The frequency of earthquakes at the site should be based on a site specific probabilistic analysis of the seismic hazards.

8.40. A comprehensive up to date database should be established that reflects the current state of the knowledge, including:

(a) Geological, seismological and geophysical data;
(b) Local site topography;
(c) Geotechnical and geophysical site properties.

As part of data collection, a catalogue of historically reported, geologically identified and/or instrumentally recorded earthquakes should be compiled.

8.41. All credible sources of potentially damaging earthquakes should be considered. Seismic sources should be characterized by location and geometry of the source, maximum magnitude of the earthquake and frequency of recurrence.

Aleatory and epistemic uncertainties should be included in the characteristics of the source.[28]

8.42. The process of using expert judgement to characterize seismic sources should be in compliance with the recommendations provided in para. 8.38.

8.43. The range of parameters used to characterize the seismic hazards should be sufficiently large and detailed to provide for the possibility of estimating accurately the seismic risk and should be consistent with the physical data and their interpretations.

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

8.45. In assessing the frequency of occurrence of a seismic hazard, it should be ensured that the size of the region considered and the scope of the investigations are adequate to characterize all credible seismic sources that may contribute to the estimated frequency of occurrence for a particular parameter.

High winds

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

8.47. For calculations of the frequencies and intensities of tornado winds, the state of the art methodology and up to date data on tornado occurrence, intensity, etc., should be applied. These calculations should include the following elements:

(a) Variation in tornado intensity with frequency of occurrence;
(b) Correlation of width of the damage area with its length;

[28] Aleatory uncertainties arise due to the random or stochastic nature of the events being modelled in the PSA. Epistemic uncertainties arise due to limitations in the state of knowledge.

(c) Correlation of the area of the tornado with its intensity;
(d) Variation in tornado intensity along the path length of the tornado;
(e) Variation in tornado intensity across the path width of the tornado;
(f) Variation in differential pressure of the tornado across the path width of the tornado.

8.48. For calculations of the frequencies and intensities of hurricanes, the state of the art methodology and up to date data on hurricane occurrence, intensity, etc., should be applied. These calculations should include the following elements:

(a) Distribution of central pressure.
(b) Radius of maximum winds.
(c) Decay of the storm over land.
(d) Wind field characteristics.
(e) Location of coast crossing, etc.

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

External floods

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

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

8.52. Calculation of the frequency and consequences of extreme ocean floods should be based on a probabilistic analysis that reflects recent, available, site specific information. These data should be supported by data for a longer period for other coastal areas, with proper account made for the topography of the area,

both within the adjusted coastal area and on the land. The combination of high waves and high winds should always be considered.

8.53. 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.

8.54. 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 properly accounted for.

Other natural hazards

8.55. 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.

8.56. 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.

8.57. 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

8.58. 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, as a minimum, the following data necessary to support realistic and valid estimations of the frequencies of hazards:

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

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

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

FRAGILITY ANALYSIS FOR STRUCTURES AND COMPONENTS

General aspects

8.59. The fragility[29] of structures and components should be evaluated using plant specific information when available and to the extent necessary for the purpose of the analysis (bounding analysis or detailed analysis) and accepted engineering methods. Findings from plant walkdowns should be considered in these analyses.

8.60. 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

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

materials, as failures involving such off-site structures may result in initiating events, such as loss of off-site power or a blast. Such failures may be highly correlated if the fragilities are low.

8.61. 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).

Seismic hazards

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

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

8.64. 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) and soil (e.g. liquefaction, slope instability, excessive differential settlement) that are found to be critical.

8.65. The fragility analyses should be supported by a plant walkdown. The walkdown should focus on the anchorage, lateral seismic support and potential interactions with structures, systems and components. Particular consideration should be given to the possibility that a non-seismically qualified structure, system or component could fall on to a seismically qualified item of equipment.

8.66. The potential for seismically induced fires and floods should also be included in the focus of the walkdown.

8.67. 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.

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

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

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

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

High winds

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

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

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

8.75. A family of fragility curves corresponding to a particular failure mode for each structure or component should be constructed and expressed in terms of median wind speed capacity and uncertainty characteristics (e.g. logarithmic standard deviations), representing randomness in capacity and uncertainty in median capacity of structures or components.

External floods

8.76. 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.[30]

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

8.78. The fragility analysis should include immersion, dynamic loads on structures and components from waves, and foundation failures (soil erosion).

Other natural hazards

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

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

Human-induced hazards

8.80. The general aspects and recommendations for the fragility analysis of seismic hazards, high winds and external floods should be followed for human-induced hazards as applicable.

INTEGRATION OF EXTERNAL HAZARDS IN THE LEVEL 1 PSA MODEL

General aspects

8.81. The Level 1 PSA model for internal initiating events is practically 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 in order 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, important structures, systems and components 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. 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.

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

Seismic hazards

8.83. 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.

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

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

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

8.86. 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 (structures, buildings, distribution systems, cable trays, relay chattering, etc.). The effects on reactor internals, in particular sticking of a control rod due to the impact of a seismic event on the reactor core, should be considered.

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

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

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

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

8.91. A thorough check and associated adjustment should be performed in relation to recovery actions and probabilities of human errors. Recovery actions that cannot be performed due to the impact of seismic events of certain magnitude should be removed from the Level 1 PSA model or 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. As a minimum, the following seismically induced effects on the operators' performance shaping factors should be taken into account:

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

8.92. Seismically induced fires and floods should be included in the Level 1 PSA model for seismic hazards, unless it is clearly justified that other seismic damage bounds additional effects from seismically induced fire and floods.

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

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

through the model for obtaining correct uncertainty characteristics of the core damage frequency.

High winds

8.95. 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.

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

External floods

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

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

Other natural hazards

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

Human-induced hazards

8.100. 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

8.101. Paragraphs 8.101–8.111 provide recommendations on meeting Requirement 20 on documentation for Level 1 PSA for external hazards [3]. The screening analysis, bounding analysis and detailed analysis for Level 1 PSA for external hazards should be documented in a manner that facilitates peer review, as well as future upgrades and applications of the Level 1 PSA:

(a) The screening of each specific external hazard should be documented in a manner that describes the processes that were used and provides details of the methods used, assumptions made and their bases.
(b) A description of the methods used for determining the hazard curves for each external hazard should be provided, including:
  (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 structures, systems and components subjected to the fragility analysis should be provided, together with:
  (i) The location of each structure, system or component;
  (ii) The key assumptions and methods used for the fragility analysis;
  (iii) The dominant failure modes for each structure, system or component;
  (iv) The sources of information for the analysis.
(d) Those structures, systems and components that are not subjected to fragility analysis should also be discussed and the basis for their screening out from the Level 1 PSA model should be provided.
(e) The specific adaptations made to the Level 1 PSA model for internal initiating events should be thoroughly documented, with an indication of the motivation for each adaptation.
(f) The final results of the bounding analysis and detailed analysis should be documented in terms of core damage frequencies, significant minimal cutsets and significant accident sequences for each scenario associated with external hazards. The general recommendations for documentation presented in paras 3.15–3.22 of this Safety Guide should be also followed.

8.102. 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.

Seismic hazards

8.103. A description of the specific methods used for the characterization of seismic sources and 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.

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

(a) List of structures, systems and components considered in the Level 1 PSA for seismic hazards;
(b) Fragility characterization and the technical bases for them for each structure, system and component;
(c) Quantified probabilities of damage for the range of seismic hazards modelled in the Level 1 PSA;
(d) Significant failure modes for structures, systems and components and the location of each structure, system and component;
(e) Specific adaptations made in the Level 1 PSA model for internal initiating events to account for 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.

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

8.106. 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 structure, system and component;
(f) Calculations of fragilities for each structure, system and component.

8.107. 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

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

(a) Description of the specific methods and data used for determining the hazard curves for high winds;
(b) Specific changes made in the Level 1 PSA model to account for effects relating to high winds;
(c) List of all structures, systems and components considered in the analysis along with the justification for the structures, systems and components that are screened out from the analysis;
(d) Methodology and data used to derive wind fragilities for all structures, systems and components modelled in the Level 1 PSA;
(e) Final results of the Level 1 PSA in terms of core damage as well as useful intermediate results.

External floods

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

(a) Description of the specific methods and data used for determining the hazard curves for external floods;
(b) Specific changes made in the Level 1 PSA model to account for effects relating to external floods;
(c) List of all structures, systems and components considered in the analysis along with justification for the structures, systems and components that are screened out from the analysis;

(d) Methodology and data used to derive flood fragilities for all structures, systems and components modelled in the Level 1 PSA;
(e) Final results of the Level 1 PSA in terms of core damage as well as selected useful results.

Other natural hazards

8.110. The general aspects and recommendations for documenting the analysis of seismic hazards, high winds and external floods should be followed as applicable.

Human-induced hazards

8.111. The general aspects and recommendations for documenting the analysis of seismic hazards, high winds and external floods should be followed as applicable.

9. LEVEL 1 PSA FOR LOW POWER AND SHUTDOWN MODES

GENERAL ASPECTS OF LEVEL 1 PSA FOR LOW POWER AND SHUTDOWN MODES

9.1. This section provides recommendations on meeting Requirements 6–13 of Ref. [3] for a Level 1 PSA for low power and shutdown modes. In principle, Level 1 PSA for low power and shutdown states for internal initiating events is based on the same methodology as Level 1 PSA for full power 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 low power and shutdown modes. Repetition of contents has been avoided and instead reference is made to earlier sections in this Safety Guide, unless approaches and conditions for low power and shutdown modes necessitate specific descriptions. However, it should be noted that the objective of the analysis is not necessarily the determination of a core damage frequency, since fuel damage frequency and inadvertent criticality may also be risk metrics of interest.

9.2. As for the full power state, internal and external hazards can be important for low power and shutdown states. The approaches discussed in Sections 6–8 of

this Safety Guide apply, but have to be modified according to the specifics of low power and 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 low power and shutdown states is much shorter compared with the duration of full power states. This ratio is in many cases of the order of 1:10 or less. Obviously, the probability of occurrence of an external hazard is then much smaller in the low power and shutdown states. On the other hand, the consequences can be very different for low power and shutdown states. For example, in the handling of heavy equipment, careful consideration may need to be given to seismic events or external explosions and external floods could also lead to different accident sequences in the plant.

9.3. During low power and shutdown states, the following main activities are typically performed in a light water reactor vessel type plant:

(a) Achieving the shutdown state from full power;
(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 full power.

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 operational states are provided.

SPECIFICATION OF OUTAGE TYPES AND PLANT OPERATIONAL STATES

9.4. In contrast to full power operation, in low power and shutdown modes the operational 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:

(1) Regular refuelling outages, during which major maintenance activities are also carried out;

(2) Planned outages, during which only specific maintenance activities are carried out;
(3) Unplanned but foreseeable outages that follow a disturbance during full power operation.

This is reflected in the plant's technical specifications, which are usually divided according to several operational modes, 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. The need for full analysis of the other two outage types should be decided with due consideration given to the objectives of the Level 1 PSA. It is essential that analysis of sequences following a disturbance be carried through until a safe and stable state is reached. Termination of the analysis at a fixed mission time may prevent meaningful results from being obtained. In many cases, as a first step, a typical outage is analysed. For reactors in operation, such an outage should be derived by starting from a recent outage and adding elements derived from the documentation of additional recent outages and from discussions with the personnel responsible for planning them. If necessary, certain elements of outages that are expected to contribute to risk should be evaluated separately. For example, in the cases of outages planned specifically for certain maintenance activities, a comparison of the risk associated with the planned outage with the risk associated with continued operation can be an important input to decision making.

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

9.7. In low power and shutdown periods, 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 states during low power and shutdown, a limited number of plant operational 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 operational 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 states:

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

9.9. For a Level 1 PSA for low power and shutdown states, the plant operational states should be specified on the basis of actual operational experience and according to present practices and procedures. Depending on the selection of the outage type performed in the previous step (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:

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

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

9.10. To ensure that the whole operating cycle is covered and in order to avoid missing contributors to risk from certain plant operational states, for example, intermediate plant power levels, or to avoid double counting, the points of interface between plant operational states (including full power state) should be clearly specified in terms of the duration, power level and system configuration of each plant operational state, the frequency (per calendar year) of entry into each plant operational state and the initiating events (e.g. the frequency of the same event can be estimated for both full power and low power analyses). Data on operational history should be used for this purpose.

INITIATING EVENTS ANALYSIS

9.11. In principle, the identification of initiating events follows the same approach as described in paras 5.11–5.39. Therefore, loss of coolant accidents and transients should be addressed, as well as initiating events that are identified in the analyses of internal and external hazards. As a starting point, a generic list can be compiled from the full power analysis. This list will need to be modified and extended according to the steps described in paras 9.12–9.22.

9.12. In para. 5.11, initiating events are defined as events that could directly lead to core damage or challenge normal operation and this requires successful mitigation using safety or non-safety systems to prevent core damage. As indicated in paras 9.4–9.8, the core can be in very different configurations in different low power and shutdown states, for example, core in-vessel versus unloaded to a fuel pool inside the containment. (Fuel stored in a spent fuel pool external to the reactor building is not covered in this Safety Guide.) 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 full power operation (see examples in Annex III). In addition, many initiating events may be human induced relating to maintenance activities or operational procedures. The major categories of initiating events that are of interest for a Level 1 PSA for low power and shutdown states are events that threaten critical safety functions such as heat removal, primary circuit inventory or integrity and reactivity control. This implies that not only core damage as for full power states might be an end state of the accident sequences in a Level 1 PSA for low power and shutdown states, but also states involving damage to fuel outside the reactor pressure vessel; such states are often termed fuel damage states and criticality events. It is necessary to decide which of these states need to be included in the analysis. This decision should be based on national targets for risk. The characteristics of such states are highly specific to the reactor type and therefore cannot be addressed here in

depth. In most cases, a Level 1 PSA for low power and shutdown states addresses the following events:

(a) Damage to fuel during handling;
(b) Damage to fuel due to dropping of heavy loads;
(c) Criticality due to changes in fuel configuration (either in the fuel pool or in-vessel);
(d) Loss of cooling to the fuel pool.

9.13. Care should be exercised to identify clearly the end states of interest. To complement the generic list obtained according to para. 9.11, systematic techniques should be used for the identification of end states. The following methods are available for this task (see paras 5.13–5.23):

(a) Systematic analytical methods, such as master logic diagrams, failure modes and effects analysis, and fault trees;
(b) Systematic examination of plant procedures for changing the configuration of the reactor coolant system and of procedures for equipment testing and maintenance.

The end points of the sequences could differ from core damage states.

9.14. Identification of potential human errors during the execution of such normal plant procedures is one of the key objectives of this process and it should incorporate plant walkdowns to familiarize PSA specialists with working practices in the plant.

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

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

Some publicly available sources of such information are:

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

9.16. Initiating events should be grouped as appropriate (see paras 5.32–5.39). Initiating event groups should include initiating events that can be analysed using the same event tree and fault tree model. In other words, the same accident sequences are applicable for all initiating events in the group. In general terms, the following criteria form the basis for grouping initiating events:

(a) All initiating events in the group have a similar effect on the availability and operation of safety systems and support systems.
(b) All initiating events in the group have similar success criteria for safety systems, support systems and other systems necessary for mitigating the event.
(c) All initiating events in the group place similar requirements on the operator.
(d) The expected response of operators is similar for all initiating events in the group.
(e) The assignment of plant damage states to sequence end points is the same for all initiating events in the group.

Obviously, the initiating event can occur in different plant operational states (see Annex III (1)), but as availability of systems and success criteria are in general different for the different plant operational states, grouping across plant operational states is not feasible in most cases.

9.17. In some cases, initiating event groups may include events that do not completely satisfy the criteria listed in para. 9.16. In such cases, the characteristics for the group should be defined on the basis of the most restrictive events within the group (see para. 5.35).

9.18. As in the case of PSA for full power states, quantification of the frequencies of initiating events should follow standard Level 1 PSA practices, as described in paras 5.128–5.132. However, the quantification of initiating event frequencies for low power and shutdown conditions should account for plant specific items such as equipment configuration and availability, technical specifications and outage management, including refuelling operations.

9.19. In a Level 1 PSA for shutdown states, the frequency of initiating events can be presented in terms of the expected hourly rate of occurrence in a specific plant

operational state. However, the frequencies should not be presented in such terms if the initiating event has arisen due to events relating to the occurrence of the plant operational state, rather than its duration (e.g. some initiating events may be related to testing or transition activities and the frequencies of such events would not scale in accordance with the duration of a plant operational state).

9.20. There are basically three approaches to quantifying the frequencies of initiating events occurring in a given plant operational state (see paras 5.128–5.132):

(1) Direct estimation from operational experience (the plant being analysed, other plants of similar design, or generic type of reactor);
(2) Estimation from frequencies determined in Level 1 PSA for full power states, with supplementary analysis;
(3) Use of a logic model, including all the foreseen inputs leading to the initiating event.

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.

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

ACCIDENT SEQUENCE ANALYSIS

Safety functions, safety systems and success criteria

9.22. 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 full power, the characteristics of the possible plant configurations may still give rise to events challenging safety functions. The analysis should take account of the following aspects:

(a) Owing to the disabling of automatic actuation of safety systems in the shutdown state, the availability of safety equipment may be reduced and the dependence on operator action increased.
(b) The integrity of the primary cooling system and the containment may be compromised.
(c) The performance of a front line system will depend in general on the particular initiating event, the characteristics of the plant operational state and the decay heat level.

9.23. Functional performance criteria should be used to specify success criteria for the various systems, which may differ from the success criteria specified for a Level 1 PSA for full power operating conditions.

Analysis to support the specification of success criteria

9.24. The fault tree models constructed for the Level 1 PSA for full power operating conditions should be revised as appropriate. Even if the logic and the response of the system remain basically the same as at full power, possible changes in the conditional availabilities of components or systems should be taken into account.

9.25. 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 modes (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 full power, and models designed for thermohydraulic calculations for full power states will be applicable (e.g. RELAP, TRAC, MAAP, MELCOR). In other cases, the applicability has to be demonstrated. For other plant operational states, a comparison of the primary system characteristics and the model capabilities should be carried out to assess the applicability of a particular code. For example, for light water reactors, the thermohydraulic analyses to support the specification of success criteria should, as a minimum, take into account the following factors:

(a) The status of the primary circuit pressure boundary;
(b) Vessel head removed or de-tensioned;
(c) Safety valve removed or primary system vent open;
(d) Loops isolated or nozzle dams installed;
(e) Water level in steam generators;

(f) Primary circuit parameters (temperature, pressure, presence of non-condensable gas, shutdown margin);
(g) Water level in the primary system;
(h) Residual heat level;
(i) Isolation status of the containment.

Modelling of accident sequences

9.26. Event trees (see paras 5.57–5.61) or equivalent presentations should be used to model the response of the plant and plant operators to initiating events. It is considered good practice to draw detailed event sequence diagrams, including human interactions, before modelling the accident sequences.

9.27. 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 points and plant damage states

9.28. As for full power conditions, 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 require such a grouping of plant damage states for the Level 1 PSA. Appropriate mission times should be specified for the safety systems (see para. 5.49), taking into account the specific features and timing of the processes taking place.

9.29. The process of selecting the plant damage states for a Level 1 PSA for low power and shutdown states should take account of the plant damage states specified for the Level 1 PSA for full power operating conditions. However, for a Level 1 PSA for low power and shutdown states, additional plant damage states different from those for a Level 1 PSA for full power operating conditions should be identified. For example, additional plant damage states may be necessary for conditions unique to certain shutdown plant operational 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 of the plant operational state (time since shutdown from full power operations);
(b) Containment state — especially for plant operational states where the containment is open;
(c) Conditions that determine the time to restore containment isolation and the potentially reduced effectiveness (leaktightness) of the containment during such time;
(d) The integrity of the primary system pressure boundary with vessel head removed, nozzle dams installed, safety valves removed, primary system vent open;
(e) The inventory of water in the primary circuit.

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

SYSTEMS ANALYSIS

9.31. As for Level 1 PSA for full power conditions, the objective of systems analysis for Level 1 PSA for low power and shutdown modes 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 the full power condition (see paras 5.69–5.91) may be utilized and adapted as far as possible and useful. 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 operational states, for example, the system may be configured differently to accommodate maintenance.
(b) A particular system that was on standby during full power operation is operating during shutdown.
(c) Actuation of a system is performed manually during shutdown, whereas in full power operation actuation was automatic.
(d) The required mission time for systems may be significantly different.
(e) Success criteria change for different plant operational states.
(f) The number of trains initially available is different for each plant operational state.

(g) Time ‘windows’ and plant conditions are significantly different, which could influence the probability of success of recovery actions.
(h) A particular system was not modelled as this was not necessary for full power conditions.
(i) Interconnection of particular systems is necessary to establish a configuration for a safety function that is used just in low power and shutdown states, for example, using the spent fuel cooling system for core cooling; account should be taken of the procedure for this connection.
(j) A particular system was not modelled as this would only be necessary for the Level 2 PSA for full power operating conditions.

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

ANALYSIS OF DEPENDENT FAILURES

9.32. As described in paras 5.86–5.91 for full power states, the objective of this task is to identify dependencies that may influence the logic and quantification of the accident sequences and system models. The main types of dependency in this regard are functional dependence on supply systems and support systems; hardware sharing between systems or process coupling; physical dependence, including dependencies caused directly or indirectly by initiating events; dependencies on human interactions and common cause failures. These dependencies should be included in the analysis.

9.33. As a point of departure from the conditions given at full power, the different support and front line systems as well as their interdependencies should be reviewed and checked regarding their applicability for the specific plant operational states. The analysis team should be aware that testing and maintenance activities may create new sources of dependencies, such as coincident repairs or maintenance of redundant components. Examples are presented in Annex III.

9.34. Revisions to the dependency models for full power operating conditions should be implemented as necessary, especially if the success criteria are different for low power and shutdown operation or conditions are different for support systems, e.g. requirements for ventilation systems and power supply systems. Alignment of systems and component outages should also be reviewed.

9.35. The analyst should be aware of the various common cause failure mechanisms and the potential impact of maintenance and other activities specific to shutdown conditions on their occurrence.

HUMAN RELIABILITY ANALYSIS

9.36. In paras 5.96–5.113, the key aspects of human reliability analysis are explained; these aspects hold largely for low power and shutdown conditions as well. The analysis of human interactions during shutdown is complex. Therefore, human reliability analysis should be performed in a structured and logical manner. As with other analysis tasks, the process of human reliability analysis should be thoroughly documented in a traceable way. Human reliability analysis should aim to generate failure probabilities which are both consistent with one another and consistent with the analysis carried out in other portions of the Level 1 PSA.

9.37. In accordance with para. 5.107, typical aspects of low power and shutdown conditions, such as extensive use of external maintenance staff from external organizations, frequent overtime work and increased requirements for control room work need adequate consideration in the analysis. Account should also be taken of difficulties in work supervision and pressures due to tight schedules.

9.38. For human reliability analysis, close interaction with plant operating personnel and maintenance personnel should be practised in order to ensure that plant design and operational features during low power and shutdown conditions are properly reflected in the analysis. If this is not possible, for example, for a plant in the design stage or construction stage, the analyst should attempt to gain knowledge based on practical experience gained from similar operating plants.

Type A interactions — pre-initiator human actions

9.39. Type A interactions (see para. 5.102) consist of actions associated with testing, maintenance, repair and calibration that, if not carried out correctly, could lead to equipment unavailability. The process of identification and quantification of type A interactions is similar to that for Level 1 PSA for full power conditions, but should account for particular low power and shutdown features, especially:

(a) Functional testing performed close to the end of the outage might be subject to difficult time constraints and therefore could have a high potential for human errors.

(b) Reduced availability of automatic realignment functions (e.g. no automatic closure signal for a valve that can be left open after a test).

Type B interactions — human actions that may cause an initiating event

9.40. 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 operating experience concerning frequencies of initiating events (e.g. drain down due to adverse valve alignment) specific to low power and shutdown conditions. 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) as discussed in para. 9.45). This assessment may result in identification of human failures that lead to unavailability of components, either immediately or as latent faults in the case of a demand modelled in the fault tree of an initiator. For the analysis, the following sources of information can be used:

(a) Written procedures for startup and shutdown of operation;
(b) Operating experience;
(c) Documents on outage planning, including technical specifications and testing and maintenance procedures.

Screening may be necessary for the analysis of type B interactions 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 5.107–5.111.

Type C interactions — post-initiator human actions

9.41. Type C human interactions (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 low power and shutdown conditions. Thus, thorough consideration should be given to a realistic assessment of the failure probabilities of such interactions.

9.42. The methodology selected should account for specific aspects relevant for modelling and quantifying type C actions in the frame of a Level 1 PSA for low power and shutdown conditions in a systematic manner. Certain aspects may differ from the full power case, for instance:

(a) More frequent actuation of alarms and standing alarms;
(b) Quality of procedural guidance;
(c) Status of operator training;
(d) Duration of time windows for response;
(e) Quality of interfaces that facilitate human actions in low power and shutdown states.

9.43. Care should be exercised that values generated by the use of time reliability correlations specific to full power operation are not uncritically accepted, since the time windows in shutdown states may be well outside the applicable ranges of such correlations.

9.44. 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.

9.45. As in a Level 1 PSA for full power operating conditions, dependencies between human interactions in the same accident sequence should be taken into account (see paras 5.112 and 5.113). However, in the PSA model for low power and shutdown states, it is of particular importance to address the dependencies between type B and type C interactions. If an initiating event such as a loss of decay heat removal is caused by a human error, the circumstances that led to the operator making the error will likely complicate the recovery of the decay heat removal function and may lead to increased failure probability compared with the case where loss of function was a result of mechanical failure.

DATA ASSESSMENT

9.46. The data necessary for quantification of the Level 1 PSA for low power and shutdown conditions includes the following:

(a) Initiating event frequencies;
(b) Data relating to human error probabilities;
(c) Duration of plant operational states;
(d) Allowed outage times;
(e) Component reliability data;
(f) Maintenance unavailabilities, including overlapping maintenance based on operational history;
(g) Assessment of common cause failures;
(h) Other data needs.

The basic needs and approaches for data acquisition that have been described in Section 5 apply to low power and shutdown states as well. Recommendations on data assessment — especially for analysis of dependent failures, human reliability and initiating event frequencies — have already been provided in this section, along with associated methodical outlines.

9.47. Data for the quantification of component reliability parameters that are specific for shutdown conditions are less widely available than for full power conditions. Thus, a widely used approach has been to adapt data from full power operation. This should not be done without transparent justification as regards the applicability of such data.

9.48. A major part of testing during planned outages serves to verify the function of the components that were previously undergoing maintenance, i.e. such tests are functional tests before equipment is put back into operation. Determination of unavailability should be related to the average test duration and to the duration of the plant operational state during which the component is tested.

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

9.50. The possibility of repair should be considered because it can significantly increase availability of safety systems in plant operational states for low power and shutdown conditions. Neglecting repair may, in many cases, lead to an overestimation of risk, especially in post-initiator scenarios, crediting in the analysis the probability of recognizing the possibility of a specific repair option which 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.

9.51. Dependency of repair times on the plant operational state should be taken into account. Such dependencies may be due to the accessibility of systems and equipment, the availability of staff to undertake repair, the availability of spare parts and, for some accident sequences, the level of radiation in the surroundings of the component to be repaired.

9.52. The analysis team for the Level 1 PSA for low power and shutdown states should be aware that components that are on standby during power operation might be in operation during an outage. If the operating policy for shutdown is to cycle the use of redundant components or trains, then an appropriate reliability model should be selected.

9.53. Mission times are used in models that calculate the probability that operating equipment used to maintain or attain a stable state following an initiator fails to continue to operate. Mission times can have a significant impact on calculated probabilities of system failure. Assumptions regarding mission times should be consistent with the modelling of accident sequences.

9.54. If foreseeable changes in outage procedures are to be incorporated in the analysis, this might have implications on data acquisition. The changes might be such that the available information on operating experience either cannot provide the necessary data or can only provide the necessary data after adaptation by analysis or engineering judgement.

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

QUANTIFICATION OF ACCIDENT SEQUENCES

9.56. For Level 1 PSA for low power and shutdown states, quantification of accident sequences should basically be performed using the same techniques as for a Level 1 PSA for full power conditions. It should be noted, however, that in a Level 1 PSA for shutdown conditions in which long mission times or recovery times are often applicable, use of Markovian techniques instead of standard fault tree and event tree evaluation methods may have the potential to yield more realistic results. Use of such techniques might, however, be cumbersome for rather complex systems. Markovian techniques are currently in the development stage for PSA for nuclear power plants.

9.57. When reviewing the results of the quantification, as in the case of a Level 1 PSA for full power operating conditions, a careful review of the minimal cutsets obtained should be carried out. In a Level 1 PSA for low power and shutdown states, the system models may have to be modified to represent the conditions of the different plant operational states. If system models are modified, cross-checking should be performed for the minimal cutsets obtained for similar

accident sequences or systems in different plant operational states to ensure that any differences in these indeed reflect different plant operational states or sequence characteristics and do not stem from modelling errors.

IMPORTANCE ANALYSIS, SENSITIVITY STUDIES AND UNCERTAINTY ANALYSIS

9.58. For the uncertainty analysis, the same techniques should be used as for a Level 1 PSA for full power conditions (see paras 5.159 and 5.160).

9.59. Importance analysis and sensitivity studies should be performed using the same techniques as for a Level 1 PSA for full power conditions (see paras 5.154–5.158 and para. 10.19).

9.60. Sensitivity studies are an important part of the analysis in Level 1 PSA for low power and shutdown states; they are aimed at analysing the potential impact of many factors specific to PSA for low power and shutdown states. For example, the specific conditions that were selected to characterize a plant operational state may represent a wider range of conditions that can actually occur during the plant operational state. Compared with PSA for full power conditions, there may be different combinations of systems that are unavailable; some combinations may result from more conservative analysis and some from less conservative analysis. The plant operational state may have a longer or shorter duration. Times available for human action can vary considerably depending on the time of the plant operational 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 operational state result in a dominant contribution to risk.

DOCUMENTATION AND PRESENTATION OF RESULTS

9.61. Paragraphs 9.61–9.71 provide recommendations on meeting Requirement 20 on documentation for Level 1 PSA for low power and shutdown modes [3]. The structure of the Level 1 PSA report should comprise procedures for a Level 1 PSA for full power operating conditions and, in addition, sections for describing those aspects which are particular to Level 1 PSA for low power and shutdown conditions should be added, such as a section describing in detail the process used for identification of outage types, plant operational states and initiating events.

9.62. The results obtained in each major step of the study, as discussed in the preceding sections, should be integrated and displayed, together with the important engineering insights gained from the analysis. Assessments of the overall results and findings and a discussion of the uncertainty should be included in the documentation.

9.63. Frequently, written maintenance or operational procedures are improved or introduced in response to preliminary analysis findings. This should be outlined in the documentation as well.

9.64. 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) Core damage frequency — important contributions integrated over all plant operational states:
  (i) Contribution of the dominant sequences;
  (ii) Contribution of the plant operational 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 operational 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.

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

9.66. 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 operational states as a function of outage time or time after the beginning of power reduction. In Annex III, an example is provided.

9.67. The following detailed information from the Level 1 PSA for low power and 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 operational state.

The level of significance of minimal cutsets should be determined according to the objectives of the PSA.

9.68. 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.

9.69. In addition to core damage frequency, other end states, for example, involving criticality or damage to the fuel pool and their frequencies should be assessed and the results documented (see paras 9.12, 9.13 and 9.19).

9.70. 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.

9.71. The drawing up of documentation should support regulatory review requirements.

10. USE AND APPLICATIONS OF PSA

SCOPE OF PSA FOR APPLICATIONS

10.1. The Safety Requirements publication on Safety Assessment for Facilities and Activities (see Ref. [3]) states that the safety assessment is required to include a full scope PSA for evaluating and assessing challenges to safety in various operational states, 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 modes of operation of the plant including startup, operation at power, low power and all modes that occur during plant shutdown and refuelling) will ensure that the insights from the PSA relating to the risk significance of accident sequences, structures, systems and components, human errors, common cause failures, etc., are derived from a comprehensive, integrated model of the plant. This section provides recommendations on meeting Requirement 23 of Ref. [3] on the use of Level 1 PSA. Level 1 PSA should be used to support applications. It is recognized that, in many cases, the results and insights from Level 2 PSA should be included in the consideration.[31]

10.2. In many cases, the scope of the PSA that is necessary to support a specific application may vary from the full scope described above. In any case, when the risk insights are to be derived from a PSA that has a smaller scope than is in fact necessary for the application, this should be recognized in applying the insights from the PSA.

10.3. The PSA to be used for any application should be maintained as a 'living PSA' that is regularly updated to reflect the current design and operation of the plant and current analysis of its transients and has been fully documented so that the analysis can be traced back to details of the design and supporting analysis.

10.4. In deriving risk insights from the PSA, the analyst should take care to understand the relative significance of the contributions from the various types of accident initiator (internal initiating events, internal fires, internal floods, earthquakes, etc.) to the PSA results. In particular, the analyst should recognize that, even if the PSA models for the various types of accident initiator are combined into one large PSA model, the analyses of the various types will be performed in different ways and this results in differing levels of detail and degrees of conservatism. 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 damage frequency is judged to be low enough according to the screening criterion adopted. This is done to avoid unnecessary expenditure of resources on detailed fire modelling or cable tracing. Such differing levels of detail may lead to misleading

[31] Note that, in this section, the focus is on the Level 1 PSA. It should be noted, however, that for many applications, it is expected that insights from a Level 2 PSA or even a Level 3 PSA will also be necessary.

insights. This is of particular concern for applications of PSA that rely on the evaluation of importance measures and for risk monitor type applications.

10.5. If a PSA is intended for use as a representative PSA for more than one similar unit at a site, the impact of any differences between a specific unit and the representative model should be identified and the impact on the results of the PSA should be assessed.

RISK INFORMED APPROACH

10.6. In any of the PSA applications described below, the insights from PSA should be used as part of the process of risk informed decision making that takes account of:

(a) Any mandatory requirements that relate to the PSA application being addressed (which would typically include any legal requirements or regulations that need to be complied with);
(b) The insights from deterministic safety analysis (such as whether the provision of the defence in depth requirement is met, whether there are adequate safety margins and whether lower level requirements such as the provision of sufficient levels of redundancy and diversity in the safety systems that perform safety functions are met and that the equipment in the plant has been qualified to a sufficient level so that it can withstand the harsh environments that would follow initiating events);
(c) Any other applicable insights or information (which could include a cost–benefit analysis and details on the remaining lifetime of the plant, inspection findings, operating experience, doses to workers that would arise in making necessary changes to the plant hardware, etc.).

10.7. The aim of applying a risk informed approach is to ensure that a balanced approach is taken for any decisions that are made in any of the PSA applications that take account of all the relevant factors. The PSA applications addressed in the remainder of this section do not cover all possible PSA applications.[32]

[32] Examples of publications providing additional information on application of PSA are IAEA-TECDOC-1200 on Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants [14] and IAEA-TECDOC-1511 on Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants [15].

Use of PSA throughout the lifetime of the plant

10.8. The PSA should be used to provide one of the inputs into the evaluation of the design throughout the lifetime of the plant. The PSA should be:

(a) Used at the concept stage to provide insights into whether the proposed design of the safety systems, the support systems and the layout of the plant are adequate;
(b) Updated throughout the detailed design and construction stages to take account of the new information relating to design and safety analysis as it becomes available;
(c) 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 life extension of the plant, and to provide insights into whether proposed design modifications and operational changes are adequate.

10.9. The same PSA should be used throughout the lifetime of the plant, with the scope, level of detail and accuracy of the PSA increasing as the design develops, as more analysis is carried out to support the modelling assumptions in the PSA and as data become available from plant operating experience. The results of the PSA should be used to identify weaknesses in the design and operation and to assess and rank options for improving the design or operation.

10.10. The results of the PSA should be used to provide insights into the design and operation of safety systems and safety related systems in preventing core damage. Such use of the PSA results should include a comparison with the overall risk criteria and targets where they have been specified.

Identification of plant vulnerabilities

10.11. To obtain maximum benefit, the PSA used for design evaluation should be a full scope PSA as specified above (para. 10.1). 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 and external hazards included in the PSA and the range of plant operating modes addressed in the PSA.

10.12. The detailed quantitative information (such as frequencies of initiating event groups and cutset frequencies, importance values for basic events) and the qualitative information derived from the PSA should be used to provide more detailed insights for design evaluation, i.e. to identify specific vulnerabilities relating to core damage.

Comparison with risk criteria and targets

10.13. The overall results of the Level 1 PSA (usually the core damage frequency) should be compared with risk 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 risk criteria and/or targets 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 safety systems and emergency procedures have been incorporated in the plant design and operation to prevent core damage. The same consideration is applicable in principle to the results of Level 2 PSA and Level 3 PSA.

10.14. Comparison of the results of the Level 1 PSA with risk criteria and/or targets should be made for the concept design in order to check that it is adequate and at various points of the design stage, construction stage and operations stage to check that the design is adequate.

10.15. In making the comparison, account should be taken of the results of the sensitivity studies and the uncertainty analysis that have been carried out. This will indicate the degree of confidence in meeting the criterion and/or target and the likelihood that it has been exceeded.

Use of cutsets

10.16. The list of cutsets from the Level 1 PSA model should be used to identify where there are relative weaknesses in the design and operation of the plant. This review should be carried out for the cutsets that make significant contributions to core damage frequency (see paras 5.146 and 5.149) to identify the initiating event groups and the safety functions that make the greatest contributions to the core damage frequency. This should also be done for cutsets containing basic events whose importance values are high.

10.17. The contributions to the core damage frequency and the cutsets for individual groups of initiating events should be used to determine whether the design of the plant is balanced in that no particular group of initiating events and

no particular accident sequence makes an unduly large contribution to the core damage frequency. The same consideration is applicable in principle to the results of the Level 2 PSA and Level 3 PSA.

10.18. The lists of cutsets should be used to determine whether there are any single order cutsets that will indicate that the single failure requirement is not complied with for any of the safety systems.

Use of importance values

10.19. Importance measures for basic events, groups of basic events, safety systems, initiating event groups, etc., should be calculated and used to interpret the results of the PSA. Importance values used in Level 1 PSA typically include:

(a) The Fussell–Vesely importance;[33]
(b) The risk achievement worth (also termed risk increase ratio) and the risk reduction worth (also termed risk reduction ratio);
(c) The Birnbaum importance.

10.20. The importance values should be used to identify the components and systems that significantly contribute to risk and should be considered carefully at the design level or during the operation of the plant. The importance values should be used to identify areas of the design or operation of the plant where improvements need to be considered.

10.21. A high Fussell–Vesely importance value or Birnbaum importance value for an independent failure event may indicate insufficient redundancy of the system in some plant operating modes and hence a need for improvement. In this case, either system redundancy should be increased or limiting conditions for operation of the system should be made more rigorous for the particular plant operating mode, if possible. A high risk achievement worth for an independent failure event may indicate that the level of reliability of the equipment should be carefully maintained to avoid an increase in risk. In general, the two aspects provided by the Fussell–Vesely importance value or risk reduction worth and the risk achievement worth should be used together.

[33] For explanation of the various importance measures, see footnotes 13 to 16.

10.22. A high Fussell–Vesely importance value for a common cause failure may indicate insufficient diversity of safety systems in respect of a particular safety function. In this case, a considerable change in the design basis might be required.

10.23. The results of the Level 1 PSA should be used to provide an approach for determining whether:

(a) The safety systems have adequate levels of diversity and redundancy;
(b) There are sufficient levels of equipment qualification for structures, systems and components that experience harsh conditions in accident conditions;
(c) There is sufficient separation and segregation of areas for hazards such as fire and flooding;
(d) 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.

The results of the Level 1 PSA should also be used to determine whether the design is balanced or additional measures need to be incorporated to reduce risk.

10.24. In identifying the plant vulnerabilities, account should be taken of the uncertainties inherent in the results of the Level 1 PSA and the insights provided by the sensitivity studies.

Comparison of design options

10.25. When modifications are being considered for a nuclear power plant, there are usually a number of options available. The Level 1 PSA should be used to provide an input into the comparison of options. The way that this is done depends on the complexity of the modification being considered, but could range from carrying out a revision of the Level 1 PSA model to incorporate a proposed new safety system to carrying out post-processing of the cutsets to take account of simpler changes. The Level 1 PSA provides one of the inputs for an integrated and risk informed decision making process to determine which of the options to choose.

Limitations of the Level 1 PSA for design evaluation

10.26. If the scope of the Level 1 PSA is less than the full scope described in this Safety Guide — for example, if the PSA does not include all initiating events and hazards that could contribute to the core damage frequency — this should be taken into account in the use of the Level 1 PSA.

10.27. In addition, it should be noted that there are some areas where the models and data are not very well developed. For example, at the design stage, there may be significant uncertainties in data, models and plant operating practices, especially for novel concepts and equipment, or in modelling the effects of ageing and/or modelling safety culture. This should be recognized in using the results of the Level 1 PSA.

RISK INFORMED TECHNICAL SPECIFICATIONS

10.28. The technical specifications for the plant specify the limits and conditions for plant operation, maintenance and testing. They provide an envelope for plant operation that is safe and consistent with the assumptions made in the safety analysis. The requirements of the technical specifications are traditionally based on deterministic requirements and engineering judgement.

10.29. The limiting conditions for operation give, for example, the requirements for equipment operability, the allowed outage times and the actions required (e.g. the testing requirements for redundant equipment). The allowed outage time for a particular system or component is the period of time within which any maintenance or repair activity should be completed. If the allowed outage time is exceeded, the technical specifications specify the actions that the plant operators should take. For example, if an allowed outage time is exceeded during operation at power, the requirement may be for the operators to reduce power or to shut down the plant. In addition, the requirements for equipment operability usually include limits on the combinations of equipment that can be removed for maintenance at the same time (usually referred to as configuration control). Insights from PSA can be used as an input to justify limiting conditions for operation and allowed outage times.

10.30. The surveillance test intervals give the requirements for testing of safety related systems and specify the frequency of testing and sometimes the testing strategy that must be followed. If a surveillance test interval is exceeded, then the technical specifications will require that the affected equipment be considered to be inoperable. This application of PSA relates to the use of a risk informed approach using insights from the PSA to optimize allowed outage times, surveillance test intervals and test strategies.

10.31. A risk informed approach should be used to provide a basis for the technical specifications. The aim should be to provide a consistent basis that is related to the risk significance of the affected plant features.

10.32. The insights provided by the Level 1 PSA should include the information necessary for comparison with the decision criteria or guidelines used to support the risk informing of the technical specifications. Such information may include, for example, the conditional core damage frequency 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 damage frequency.

10.33. Where it is proposed to move a particular maintenance activity from power operation to shutdown mode (or vice versa), the PSA should be used to determine the corresponding change in risk for both full power and shutdown modes.

10.34. In providing input from the Level 1 PSA for the optimization of the surveillance test intervals, justification should be provided for the correlation used between the surveillance test interval and the component failure probability.

10.35. Where changes are proposed to the testing strategy (e.g. the introduction of staggered testing), the Level 1 PSA should be used to determine the change in the core damage frequency that this would lead to. Consideration should be given to indirect effects such as changes to common cause failure probabilities and changes in the potential for human errors of commission.[34]

RISK MONITORS

10.36. A risk monitor is a real time analysis tool that generates risk information based on the actual plant configuration in terms of a number of factors that typically include: the plant operational state (power operation or one of the shutdown modes), the components that have been removed from service and the choice of operating trains and standby trains for normally operating systems. 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.

[34] While errors of commission may not be explicitly included in the PSA model, a discussion of how a change might affect the potential for errors of commission can provide useful additional information that can support the decision on the acceptability of the change.

10.37. Risk monitors have also been useful in addressing the maintenance rule of the United States Nuclear Regulatory Commission, which requires operating organizations to assess and manage the risk associated with maintenance activities. There are a large number of risk monitors being used routinely at nuclear power plants in support of operational decisions. Hence, this can be seen as a very mature application of PSA.

PSA model for a risk monitor

10.38. Although a risk monitor is a specific application of the living PSA, it needs to be recognized that the PSA model required for the risk monitor is different from the living PSA and changes usually need to be made to it, as specified in the following paragraphs.

10.39. The Level 1 PSA model should be amended so that it calculates the 'point in time risk' for each of the plant configurations entered rather than the average risk generally calculated by the PSA. This requires that all the modelling assumptions and data that relate to the calculation of the average risk (e.g. frequencies of initiating events, unavailabilities of components due to maintenance) are identified and replaced by the equivalent assumptions and data for estimating the point in time risk.

10.40. The PSA model should be amended to remove any simplifications made to reduce the amount of analysis needed for the PSA, as they could lead to the risk monitor giving incorrect results for some of the plant configurations that could arise. Removal of simplifications in the PSA model typically includes:

(a) Replacing initiating events that are modelled in the PSA as an event with a lumped frequency, by individual initiating events (e.g. replacing a loss of coolant accident modelled as an event in one of the coolant loops by individual events in each of the coolant loops);
(b) Modelling system alignments and the choice of operating trains and standby trains of normally operating systems explicitly;
(c) Removing basic events that have been included in the PSA to model maintenance or by setting their probability to zero.

10.41. The PSA model should be enhanced so that it provides a calculation of the risk that relates more closely to the actual plant configuration. Enhancement of the PSA model typically includes:

(a) Specifying a process for determining the appropriate common cause failure probability when components are removed from service for maintenance;
(b) Using a human reliability model that takes account of the human errors that could occur during the actual plant configuration;
(c) Introducing dynamic events to model changes in initiating event frequencies and basic event probabilities that arise due to changes in the plant environment.

10.42. The PSA model developed should also be compatible with the software used for the risk monitor. The changes necessary may include changing the event tree and fault tree models developed in the PSA into a logically equivalent large fault tree model (usually referred to as a 'top logic model') or changing the way that NOT logic and logical switches are used in the model.

10.43. A number of databases will be necessary to support the operation of the risk monitor. For example, there needs to be a database that provides a link between the normal terminology for plant components that is familiar to the plant operators and the basic events modelled in the PSA that relate to the failure or unavailability of these plant components. All the databases necessary to support the risk monitor application should be verified.

10.44. The logic structure of the PSA model and the related databases developed for the risk monitor may be significantly different from those of the original PSA and hence should be validated. The validation process should aim at providing a high level of confidence that the quantitative results given by the risk monitor are accurate and the same as, or equivalent to, those given by the original PSA for all likely plant configurations.

10.45. There is a large body of experience in converting a living PSA for use in a risk monitor application so that it calculates the point in time risk, removing simplifications that are not suitable for the risk monitor, making enhancements to increase the precision of the PSA model and validating the resulting PSA model [16].

Risk monitor software

10.46. Software for risk monitors is significantly different from that used for developing and solving a PSA. The essential difference is that the risk monitor is designed to be used by all nuclear power plant personnel, rather than just PSA specialists, and that the user does not need to have specialist knowledge of PSA techniques. The user is limited to making changes to the plant configuration, for

example, specifying the plant operational state and identifying the components that have been removed from service for maintenance. This is done using the normal plant identifiers for the equipment selected. Hence, the users do not need to interact directly with the PSA model and generally no special training is required in PSA techniques.

10.47. A number of high quality software codes have been developed that support a wide range of functions, including both quantitative and qualitative measures of risk. Computers permit a common approach to be taken, whereby the risk monitor includes a full PSA model that is used to calculate the point in time risk for the core damage frequency for each actual or proposed plant configuration, since this allows greater flexibility in the modelling and provides greater precision in the calculation of the level of risk for all plant configurations. An alternative approach that has been used is the creation of a catalogue of pre-solved assessments for an extensive number of configurations.

10.48. 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. The software should be capable of providing results in real time. For risk monitors that are based on real time solution of the PSA model, the computational speed associated with the software should be reasonably high.

Presentation of information from risk monitors

10.49. The risk monitor provides both quantitative risk information (calculations of the point in time core damage frequency, allowed configuration time and the cumulative incremental conditional core damage probability) and qualitative risk information (the status of safety functions and systems). The qualitative information is related to deterministic requirements and gives insights that are additional to those provided by the quantitative results. These insights are particularly useful for risk management of shutdown modes.

10.50. The risk monitor should be able to be used by a wide range of plant personnel in a number of roles. Therefore, the risk monitor should present information in a way that can be understood by the wide range of 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.

Use of risk monitors

10.51. If the risk monitor is used by control room staff and others, it should be kept up to date so that the information on the current plant configuration and environmental factors is accurate. It is good practice for updating to be done as soon as possible so that the risk monitor can be used in real time and will indicate the current plant risk.

10.52. The risk monitor can be used for the planning of future maintenance outages, long term profiling of risk, analysis of the cumulative incremental conditional core damage probability and the evaluation of unexpected events such as equipment failures.

10.53. The quantitative and qualitative risk information produced by the risk monitor should be used as part of an integrated, risk informed decision making process that also takes account of the mandatory requirements (such as the plant's technical specifications) and the deterministic requirements (such as maintaining defence in depth).

Limitations of risk monitors

10.54. There may be limitations in the scope or level of detail of the living PSA and consequent limitations in the risk information provided by the risk monitor. For example, the Level 1 PSA model may not include all internal and external hazards, may not address all plant operational states and may not model all the operating trains and standby trains, plant interconnections, etc. Users of the risk monitor should be made aware of any such limitations, which should be taken into account in using the information to support operational decisions.

RISK INFORMED IN-SERVICE INSPECTION

10.55. The overall aim of the programme for in-service inspection of the pipework at a nuclear power plant is to identify areas of degradation that can be repaired before a failure occurs. The programme of inspections that is carried out has typically been based on a traditional deterministic approach and engineering judgement.

10.56. The aim of the risk informed approach is to use the insights provided by the PSA to revise the programme of inspections (in terms of the frequency of inspection, methods used, sample size, etc.) and focus it on those segments of pipework that have the highest risk significance and reduce the inspections carried

out on segments of pipework with a low risk significance. The expectation is that this will lead to a reduction in the overall number of pipework inspections that are carried out, a reduction in costs and a reduction in the associated dose burden to the operating staff, without increasing the risk from the plant.

10.57. Several approaches to carrying out risk informed in-service inspection have been developed.[35]

Use of PSA in risk informed in-service inspection

10.58. Insights from the Level 1 PSA should be used as one of the inputs in determining the following:

(a) The pipework segments to be assessed by the risk informed in-service inspection project;
(b) The risk significance of the segments of pipework to be assessed;
(c) The target failure probabilities for the pipework segments that are to be inspected;
(d) The change in the risk resulting from changes to the in-service inspection programme.

10.59. For each pipework segment included in the study, the consequences of failure of the segment should be determined in one of the following ways:

(a) As an initiating event, with account taken of any secondary failure(s) that could occur (e.g. as a result of a release of water or steam, pipe whip);
(b) As a failure in a standby system that could lead to a train of the system (or the whole system) being unavailable to perform its safety function;
(c) As a failure of a train of a system (or the whole system) when it operates on demand due to the loads imposed on the pipework segment.

10.60. Pipework failures that lead directly to initiating events would normally already be included in a full scope Level 1 PSA. It should be checked that this is indeed the case. However, pipework failures that lead to the unavailability of safety systems or failure of safety systems on demand are not generally included in the PSA model since the contribution to the failure probability of safety

[35] Examples include methods developed by, and known as, the Electric Power Research Institute methodology and the Westinghouse Owners Group methodology, which have both been used extensively.

systems from failure of the pipework is negligible in comparison to that from failure of active components.

10.61. For pipework failures leading to initiating events, the PSA should be used to determine the conditional core damage probability. For pipework failures leading to the failure of standby systems or the failure of systems on demand, the PSA should be used to calculate the conditional core damage frequency.

10.62. The rigorous way of determining the risk significance of all segments of pipework included in the risk informed in-service inspection project would be to revise the PSA model to include these pipework segments explicitly and thereby determine the associated core damage frequency and conditional core damage probability directly. This approach has been used in some of the risk informed in-service inspection projects that have been carried out in various Member States.

10.63. An alternative approach that is often adopted is to use a surrogate approach where the failures of the segments of pipework not included explicitly in the PSA are correlated with basic events (or groups of basic events) already included in the PSA and for which the consequences of failure are the same. In doing this, consideration needs to be given to ensuring that any secondary effects of pipework failure are taken into account in the PSA model.

10.64. When the revised in-service inspection programme has been determined, the PSA should be used to determine the risk insights necessary for comparison with the decision criteria or guidelines used to assess the acceptability of the change in the in-service inspection programme. This can be done by estimating the specific changes in initiating event frequencies or component failure probabilities that would result from a change in the in-service inspection programme and by re-quantifying the PSA with these revised values, or by carrying out sensitivity studies. In this process, the associated limitations on the PSA in terms of modelling details, scope, etc., should be recognized and taken into account.

RISK INFORMED IN-SERVICE TESTING

10.65. The current approach to in-service testing requires that it be carried out by following a code or standard, which may or may not be incorporated into a prescribed regulation[36], that uses a deterministic approach to deciding on the programme of in-service testing that needs to be carried out for components in the plant.

[36] An example is Section OM of Ref. [17].

10.66. The aim of the application of a risk informed approach to in-service testing is to use the risk information provided by the PSA to help optimize the in-service testing programme so that it focuses on the components that have the highest risk significance. From the point of view of the plant operators, a risk informed approach to in-service testing has the potential to reduce overall maintenance costs while still maintaining a very high level of safety.

10.67. 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. The risk information from the PSA should be derived using both the Fussell–Vesely importance and the Birnbaum importance (or the risk achievement worth), since both these importance measures provide insights into the risk significance of components.

10.68. The risk information should be used to identify components with a relatively high safety significance for which rigorous in-service testing is required 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.

10.69. When the in-service test intervals have been revised, the Level 1 PSA should be used to calculate the core damage frequency for the new test intervals in order to determine whether this is acceptable.

GRADED QUALITY ASSURANCE[37]

10.70. The aim of the quality assurance programme applied to the structures, systems and components in a nuclear power plant is to provide a high level of confidence that they will perform their safety functions reliably within the range of conditions that they would encounter during normal operation and following accidents. The normal approach is to apply deterministic methods and

[37] In the United States of America, risk informed quality assurance has been superseded by risk informing the 'special treatment' requirements which include quality assurance, but which also include items such as environmental qualification. The reason for this is that even if changing the quality assurance requirements were demonstrated as being feasible, the other special treatment requirements would not allow the change to be implemented. Therefore, the special treatment requirements have to be treated as a whole. This application is addressed through a voluntary regulation, 10 CFR 50.69 [18].

engineering judgement to identify the structures, systems and components that are safety related and to apply a high level of quality assurance to them. The historical approach is to apply the same high level of quality assurance to all safety related structures, systems and components in the plant.

10.71. However, the results of many PSAs carried out to date have shown that some of the structures, systems and components that have been classified as safety related have a relatively low risk significance and some of the structures, systems and components classified as not being safety related have a relatively high risk significance.

10.72. The aim of the application of a graded approach to quality assurance is to consider whether changes can be made to the traditional quality assurance requirements for some of the structures, systems and components to bring the requirements more in line with the risk significance of the structures, systems and components. From the point of view of the plant operators, this may reduce the resources necessary to carry out the quality assurance programme, and from the point of view of the regulatory body, it will remove unnecessary burdens from the plant operators.

10.73. The Level 1 PSA should be used to determine the risk significance of structures, systems and components. The risk significance should be derived using both the Fussell–Vesely importance and the Birnbaum importance (or the risk achievement worth) since both these importance measures provide insights into the risk significance of structures, systems and components. In addition, the derivation of the risk significance should be mainly done at the level of safety functions and safety systems rather than at the level of individual structures, systems or components (since the quality assurance requirements would be expected to be the same for sets of components that perform the same safety function or are part of the same safety system). However, the importance of individual components may also need to be considered.

10.74. The safety classification (derived from the deterministic analysis and engineering judgement) and the risk significance (derived from the PSA) should be used together in deciding whether changes should be made to the current quality assurance arrangements for an existing plant or the proposed quality assurance arrangements based on the traditional approach for a new plant.

10.75. Consideration should be given on whether the quality assurance arrangements could be reduced for structures, systems and components that have been classified as safety related but which have a relatively low risk significance

and whether they need to be increased for the structures, systems and components that have been classified as not being safety related but which have a relatively high risk significance. The existing quality assurance arrangements would continue to be applied for the other structures, systems and components.

PSA BASED SAFETY PERFORMANCE INDICATORS

10.76. Safety performance indicators that are based on PSA can be used to provide retrospective or current indications of plant safety performance. Such indicators typically include the risk profile for past plant operation, the current risk and the cumulative core damage probability from maintenance outages, etc. Many such indicators can be derived directly using a risk monitor. Other safety performance indicators can also be derived from event analysis that is based on PSA.

10.77. A set of safety performance indicators that use information directly from the Level 1 PSA should be developed for the plant and should be monitored.

PSA BASED EVENT ANALYSIS

10.78. Operating events can be analysed using the PSA model. This is now an increasingly common practice in many States and forms a routine part of operational feedback to complement the traditional deterministic analysis that is carried out to determine root causes, etc. The purpose of event analysis is typically to determine the risk significance of possible events and the contributors to the risk, so that the events can be responded to according to their risk significance.

10.79. PSA based event analysis should be carried out for events at the plant (referred to as ‘direct events’) and events at other plants (‘transposed events’). PSA based event analysis should include the analysis of initiating events (where an initiating event actually occurred and where failures occurred, but where an initiating event was prevented by prompt operator intervention) and of conditional events (where the likelihood of an initiating event was increased or the availability of the safety systems required to respond to initiating events was reduced).

10.80. PSA based event analysis should be carried out for events with high potential safety significance. This necessitates that screening criteria be developed that can be applied to screen out events with low safety significance and to rank events according to their significance.

10.81. The condition of the plant, failures that have occurred and the operator actions that were carried out during the event should be determined and accurately mapped on to the PSA model. The PSA model should be re-quantified to generate the results necessary for comparison with the criteria discussed in para. 10.80. The results necessary for comparison are typically the conditional core damage probability for initiating events and the instantaneous core damage frequency for conditional events. The analysis of the event should be supplemented by sensitivity studies to provide the answer to "what if?" questions. For example, "what would the conditional core damage probability have been if the operator 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.

10.82. PSA based event analysis should be carried out to complement deterministic analysis by allowing multiple failure to be addressed using an integrated model and by providing a quantitative indication of the risk significance of operational 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.

10.83. Care should be taken in using the results of the PSA based event analysis for the identification of trends in the performance of a nuclear power plant or a set of nuclear power plants over a period of time. The results of such an application of PSA based event analysis could be misleading unless the analysis uses the same models, methods and assumptions throughout.

RISK INFORMED REGULATIONS

10.84. The insights provided by the PSA can be used by regulatory bodies in making decisions on the way in which they carry out their activities. This is additional to the use of the PSA by the regulatory body in making decisions about nuclear power plant safety issues and the PSA applications as described earlier in this section.

10.85. Insights from the PSA should be used as part of an integrated, risk informed decision making process. The aim should be to prioritize and to optimize regulatory activities so that they focus on areas that have the highest risk significance. This should also aim to reduce the regulatory burden on plant operators by removing unnecessary regulations and requirements.

Risk informed development and updating of regulations

10.86. In developing and updating regulations and regulatory guides, the regulatory body should employ a risk informed approach that takes account of the risk information and insights provided by the Level 1 PSA.

10.87. The aim should be to use insights from the Level 1 PSA:

(a) To identify areas not covered by existing regulations that are risk significant so that further regulations can be drawn up;
(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 deleted.

Risk informed prioritization and optimization of regulatory activities

10.88. The activities carried out by a regulatory body include: issuing, amending, suspending or revoking authorizations or licences; carrying out regulatory inspections and oversight; ensuring that corrective actions are taken and taking enforcement actions when necessary.

10.89. The risk information provided by the Level 1 PSA should be used to prioritize and to optimize the activities of the regulatory body. For example, the risk information provided by the Level 1 PSA can be used to determine the priorities for carrying out the set of regulatory inspections proposed for the next period of time. The aim should be to ensure that inspections are focused on areas of the plant design and operation that have high risk significance and are reduced or not carried out in areas that have low risk significance.

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. NS-R-1, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).

[4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on Nuclear Safety, Legal Series No. 16, IAEA, Vienna (1994).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Safety Series No. 106, IAEA, Vienna (1992).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).

[11] 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).

[12] NUCLEAR REGULATORY COMMISSION, Evaluation of External Hazards to Nuclear Power Plants in the United States, NUREG/CR-5042, Supplement 2, USNRC, Washington, DC (1989).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Safety for Existing Nuclear Installations, IAEA Safety Standards Series No. NS-G-2.13, IAEA, Vienna (2009).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, IAEA-TECDOC-1200, IAEA, Vienna (2001).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants, IAEA-TECDOC-1511, IAEA, Vienna (2006).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, Risk Monitors: The State of the Art in their Development and Use at Nuclear Power Plants, WGGRisk, NEA/CSNI/R(2004)20, OECD, Paris (2004).
[17] AMERICAN SOCIETY OF MECHANICAL ENGINEERS, Boiler and Pressure Vessel Code, 2007 edn, ASME, New York (2007).
[18] NUCLEAR REGULATORY COMMISSION, Risk-Informed Categorization and Treatment of Structures and Components for Nuclear Power Reactors, 10 CFR 50.69, US Govt Printing Office, Washington, DC (2004).

Annex I

EXAMPLE OF A GENERIC LIST OF INTERNAL AND EXTERNAL HAZARDS

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
Air based natural hazards			
A1	Strong wind	The hazard is defined in terms of damage to the plant due to strong winds. It includes both direct damage from wind pressure and indirect damage due to wind-borne missiles.	The hazard does not include tornado (A2) due to the unique characteristics of this hazard. The hazard does not include the differentiating effects of snowstorm (included in A7), saltstorm (A12) or sandstorm (A13). However, the wind effects of these hazards are included. Effects of storm surges are covered by the hazard high water level (W3).
A2	Tornado	The hazard is defined in terms of damage to the plant due to tornadoes. The hazard is separated from other strong winds owing to its special characteristics with respect to duration, wind speed and frequency of occurrence.	
A3	High air temperature	The hazard is defined in terms of impact on the plant of high air temperature.	Plant impact due to high water temperatures is treated separately (W4).
A4	Low air temperature	The hazard is defined in terms of impact on the plant of low air temperature.	Plant impact due to low water temperature (W4) or ice impact (W7, W8, W9) is treated separately.
A5	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.	

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
A6	Extreme rain	The hazard is defined in terms of damage to the plant due to extreme rain.	It includes both damage due to rain load on structures and damage due to rain induced flooding.
A7	Extreme snow (including snowstorm)	The hazard is defined in terms of damage to the plant due to extreme snow, including snowstorms.	Wind effects due to snowstorms are covered by the hazard strong wind (A1). Flooding effects due to melting of snow are judged to be bounded by flooding effects due to extreme rain (A6).
A8	Extreme hail	The hazard is defined in terms of damage to the plant due to extreme hail. It includes damage due to hail load on structures.	Flooding effects due to melting of hail are bounded by flooding effects due to extreme rain (A6). Any possible effects on the ultimate heat sink are judged to be bounded by ice hazards (W7, W8, W9).
A9	Mist	The hazard is defined in terms of impact on the plant of mist.	
A10	White frost	The hazard is defined in terms of impact on the plant of white frost.	
A11	Drought	The hazard is defined as an extended drought period that lowers the water level of lakes, rivers and open water basins.	Possible plant impacts due to high air temperature (A3) or high water temperature (W4) are covered by the analysis of these hazards. There is considered to be no effect on water level (heat sink).
A12	Saltstorm	The hazard is defined as a storm involving salt covering of plant structures.	Wind effects from saltstorms are covered by the hazard strong wind (A1).
A13	Sandstorm	The hazard is defined in terms of impact on the plant of storm-borne sand.	Wind effects from sandstorms are covered by the hazard strong wind (A1).

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
A14	Lightning	The hazard is defined in terms of damage to the plant due to lightning. The impact may be direct, causing structural damage or hazards relating to loss of off-site power, or indirect through an electromagnetic feeder fire started by lightning.	Fire started by lightning is bounded by external fire (G7) and by the internal fire analysis.
A15	Meteorite	The hazard is defined in terms of damage to the plant due to meteorite impact.	
Ground based natural hazards			
G1	Land rise	The hazard is defined in terms of impact on the plant of land rise.	
G2	Soil frost	The hazard is defined in terms of impact on the plant of soil frost.	
G3	Animals	The hazard is defined in terms of impact on the plant of animals.	Impact on intake water from fish, mussels, etc., is covered by W10.
G4	Volcanic phenomena	The hazard is defined in terms of impact on the plant of volcanic eruptions.	
G5	Avalanche	The hazard is defined in terms of impact on the plant of avalanches.	
G6	Above water landslide	The hazard is defined in terms of impact on the plant of above water landslide.	

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
G7	External fire	The hazard is defined in terms of impact on the plant of fire originating from outside the plant, inside or outside the site area.	Internal fires spreading from another plant on the site are treated separately (M15). Fires resulting as secondary effects of other external hazards are treated as part of these hazards (M2, M11, M20). Internal fires are analysed as part of the PSA for internal hazards.
G8	Seismic hazards	The hazard is defined in terms of impact on the plant of an earthquake.	
G9	Karsts	The hazard is defined in terms of impact due to fissures, sinkholes, underground streams and caverns caused by erosion.	
Water based natural hazards			
W1	Strong water current (underwater erosion)	The hazard is defined in terms of damage to plant structures due to strong water current.	The effects of underwater landslide are treated separately (W6).
W2	Low water level	The hazard is defined in terms of impact on the plant of low water level.	Level decrease due to land rise is covered by G1.
W3	High water level	The hazard is defined in terms of impact on the plant of high water level. High water levels may be due to storm surges, waves or seiches. High water levels are also affected by tidal variations.	
W4	High water temperature	The hazard is defined in terms of impact on the plant of high water temperature.	Plant impact due to high air temperature is treated separately (A3).

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
W5	Low water temperature	The hazard is defined in terms of impact on the plant of low water temperature.	Plant impact due to low air temperature (A4) or ice impact (W7, W8, W9) is treated separately.
W6	Underwater landslide	The hazard is defined in terms of impact on the plant of underwater landslide.	An underwater landslide may be due to above water causes, such as prolonged and intense precipitation. Plant impact due to underwater erosion is treated as part of the strong current hazard (W1).
W7	Surface ice	The hazard is defined in terms of impact on the plant of thick surface ice.	The hazard does not include effects due to frazil ice (W8) and ice barriers (W9).
W8	Frazil ice	The hazard is defined in terms of impact on the plant of frazil ice in the cooling water intake.	
W9	Ice barriers	The hazard is defined in terms of impact on the plant of ice barriers.	
W10	Organic material in water	The hazard is defined in terms of impact on the plant of organic material in intake water. The material may be algae, seaweed, fish, mussels, jellyfish, etc.	
W11	Corrosion (from salt water)	The hazard is defined in terms of impact on the plant of corrosion.	
W12	Solid or fluid (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.	

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
W13	Chemical release to water	The hazard is defined in terms of impact on the plant of chemical releases to water. The focus is on reduction of water quality. The releases may be due to a ship accident, but may also originate on land.	The hazard does not include effects due to release of solid or fluid (non-gaseous) impurities (W12).
W14	Tsunami	The hazard is defined in terms of damage to the plant due to high water level and pressure from the wave.	
Off-site accidents			
M1	Direct impact from ship collision	The hazard is defined in terms of the direct impact of a ship.	The hazard does not cover consequences of releases in connection with a ship accident (explosion, pollution, intake clogging or release of toxic gases), as these hazards are handled separately (M2, M3, W12, W13).
M2	Explosion after transportation accident	The hazard is defined in terms of damage to the plant resulting from explosion after ground transportation accidents outside the site or due to sea, lake or river transportation accidents. The damage may be due to pressure impact or impact from missiles.	The hazard does not include damage due to aircraft crash (M20) or originating from pipeline accident (M5). Toxic effects from a chemical release are covered by M3.
M3	Chemical release after transportation accident	The hazard is defined in terms of toxic impact on the plant resulting from chemical release after ground transportation accidents outside the site or due to sea, lake or river transportation accidents.	Explosion effects from transportation accidents are covered by M2.

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
M4	Explosion outside plant	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) of solid substances or gas clouds outside the site. The damage may be due to pressure impact or impact of missiles.	The hazard does not include explosions in connection with transportation accidents outside the site (M2) or originating from pipelines (M5). Toxic effects from a chemical release are covered by M6.
M5	Explosion after pipeline accident	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) after a pipeline accident. The damage may be due to pressure impact or impact of missiles.	Toxic effects from a chemical release are covered by M7. Explosion effects from a release outside or within the site are covered by M4 and M11. Toxic effects after transportation or pipeline accidents are analysed in M3 and M7.
M6	Chemical release outside site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release outside the site. These releases may originate from process accidents outside the plant or from leakages of substances stored outside the plant.	
M7	Chemical release after pipeline accident	The hazard is defined in terms of toxic impact on the plant resulting from chemical release after a pipeline accident.	Explosion effects from pipeline accidents are covered by M5.
M8	Missiles from military activity	The hazard is defined in terms of impact on the plant of missiles from military activity.	Impact on power supply and heat sink assumed to be bounded by other hazards.
M9	Excavation work	The hazard is defined in terms of impact on the plant of excavation work, inside or outside the site area.	

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
On-site accidents			
M10	Direct impact of heavy transportation within the site	The hazard is defined in terms of damage to the plant resulting from direct impact of heavy transportation within the site, but outside the plant buildings. This also includes transportation of the containment external maintenance platform.	Heavy transportation within plant buildings is analysed as part of the PSA for internal hazards.
M11	Explosion within the site	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) of solid substances or gas clouds within the site, but outside the plant buildings. The damage may be due to pressure impact or impact of missiles.	The explosions within plant buildings are analysed as part of the PSA for internal hazards.
M12	Explosion after pipeline accident within the site	The hazard is defined in terms of damage to the plant resulting from explosions (deflagration or detonation) after a pipeline rupture on the site. The damage may be due to pressure impact or impact from missiles.	
M13	Chemical release within the site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release within the site.	These releases may originate from process accidents inside the plant or from leakages of substances stored within the site, but outside the plant buildings. The chemical releases from substances stored inside buildings are analysed as part of the PSA for internal hazards.

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
M14	Chemical release after pipeline accident within the site	The hazard is defined in terms of toxic impact on the plant resulting from chemical release after a pipeline accident at the site.	
M15	Internal fire spreading from other units on the site	The hazard is defined in terms of impact on the plant of fires originating in another unit on the site.	External fires are treated separately (G7). Fires resulting as secondary effects from other external hazards are treated as part of these hazards (M2, M11, M20).
M16	Missiles from other units on the site	The hazard is defined in terms of damage to the plant resulting from missiles generated at another unit on the site.	
M17	Internal flood and harsh environment spreading from other units on the site	This hazard is defined in terms of damage to the plant resulting from water spreading effects from other units.	
M18	Excavation work within the site area	The hazard is defined in terms of impact on the plant of excavation work within the site area.	
Aircraft crash			
M19	Satellite crash	The hazard is defined in terms of damage to the plant resulting from satellite impact.	
M20	Aircraft crash	The hazard is defined in terms of damage to plant structures resulting from an aircraft crash within the site area. The aircraft may be commercial, private or military.	

Code	Hazard	Hazard definition and hazard impact	Interfaces and comments
Other human-induced hazards			
M21	Magnetic disturbance	The hazard is defined in terms of impact on the plant of human-induced magnetic or electrical fields. The main examples of such fields are those attributable to radar, radio and mobile phones.	
M22	Failure of a dam upstream of the plant	The hazard is defined in terms of damage to plant structures, systems and components resulting from high level water and water waves.	

Note: The list of hazards is based on one given in the footnote reference[1]. Internal hazards originating inside plant buildings are not included in the table.

[1] KNOCHENHAUER, M., LOUKO, P., Guidance for External Events Analysis, Rep. SKI-R-02/27-SE, SKI, Stockholm, February 2003.

Annex II

EXAMPLES OF FIRE PROPAGATION EVENT TREES AND SEISMIC EVENT TREES

ILLUSTRATION OF THE USE OF THE EVENT TREE TECHNIQUE FOR THE ANALYSIS OF FIRE MITIGATION AND PROPAGATION

II–1. The example of a fire propagation event tree presented in Fig. II–1 comprises the relevant features starting with fire initiation. Early and late detection of fire are distinguished as these cases are associated with different probabilities to control and extinguish the fire. For fire propagation, it is relevant whether and to what degree the room is closed. Further modelling addresses available fire suppression equipment, taking into account possible damage to safety relevant items caused by the means of suppression. Figure II–1 provides an illustration of how the event tree technique can be used to analyse fire mitigation and propagation.

ILLUSTRATION OF THE USE OF THE EVENT TREE TECHNIQUE FOR IDENTIFICATION OF SEISMICALLY INDUCED INITIATING EVENTS

II–2. Figure II–2 provides an illustration of how the event tree technique can be used to model different consequences of seismically induced initiating events. In this example, it is assumed that the seismic initiating event always leads to a loss of off-site power.

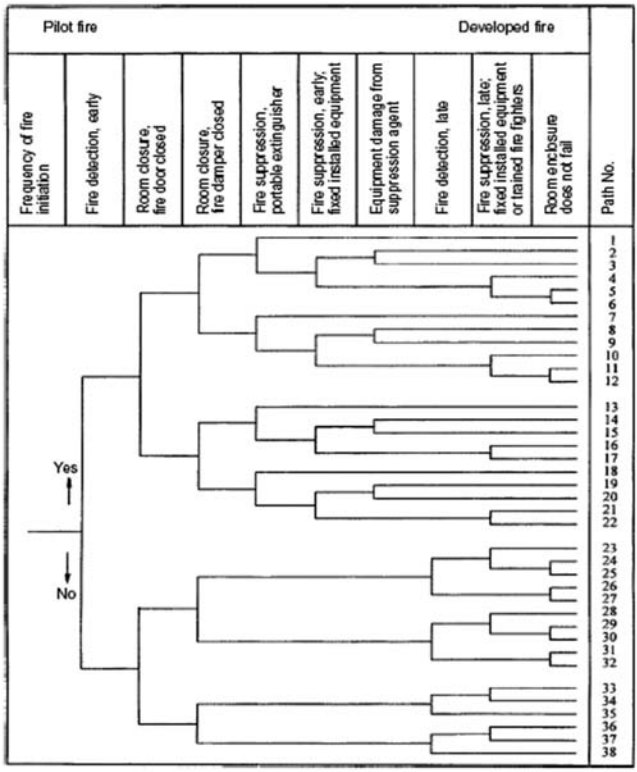

FIG. II–1. Example of a fire propagation event tree.

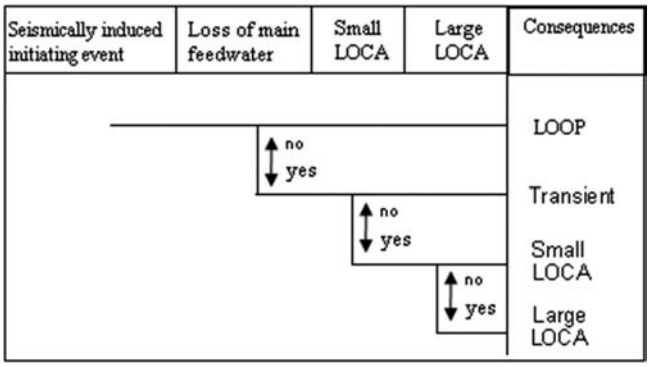

FIG. II–2. Example of an event tree for the modelling of a seismically induced initiating event. LOCA: loss of coolant accident.

Annex III

SUPPORTING INFORMATION ON PSA FOR LOW POWER AND SHUTDOWN MODES

EXAMPLES OF PLANT OPERATIONAL STATES AND ASSOCIATED INITIATING EVENTS

III–1. In the framework of a PSA for the German boiling water reactor type SWR 69, a probabilistic evaluation of low power and shutdown states was performed [III–1]. An example of a pressurized water reactor plant is provided in Ref. [III–2].

III–2. On the basis of Ref. [III–1], information is presented to illustrate how the plant operational state can be specified and how initiating events can be associated with the plant operational state. For the description of the changing of system related and physical states, the outage was divided into plant operational states (see Fig. III–1 and Table III–1). The plant operational states were chosen in such a way that the system availability and the physical states are as constant as possible. Normally, during the outage (states 3-1 to 3-7), one of the two electrical redundancies for emergency power supply, two of the four trains of the residual heat removal system and one of the two trains of the emergency standby system are available. In state 3-4, where most of the maintenance work is performed, the leakage return system in the reactor building sump needs to be available.

III–3. A detailed evaluation of operating experience in Germany was performed to find events that can lead to initiating events or that can influence the control of accidents during low power and shutdown modes. In addition to evaluating German operating experience, the results of international low power and shutdown PSAs were evaluated [III–3, III–4].

III–4. German documents providing guidance on PSA were also used as a basis for identification of initiating events [III–5 to III–7].

III–5. The identification of the initiating events and the assignment to the plant operational state in which they can occur lead to the matrix shown in Table III–2. The cells marked with an 'X' in Table III–2 indicate that the initiating event can occur in this plant operational state. As pointed out in para. 9.11, the end states to be included have to be decided on the basis of national risk criteria.

III–6. As an example, corresponding information for a pressurized water reactor type plant is provided in Ref. [III–2] and summarized in Tables III–3 and III–4. Table III–3 shows the plant operational states to be distinguished. In Table III–4, the initiating events to be considered in the different plant operational states are displayed. This list is based on an analysis of national and international operating experience.

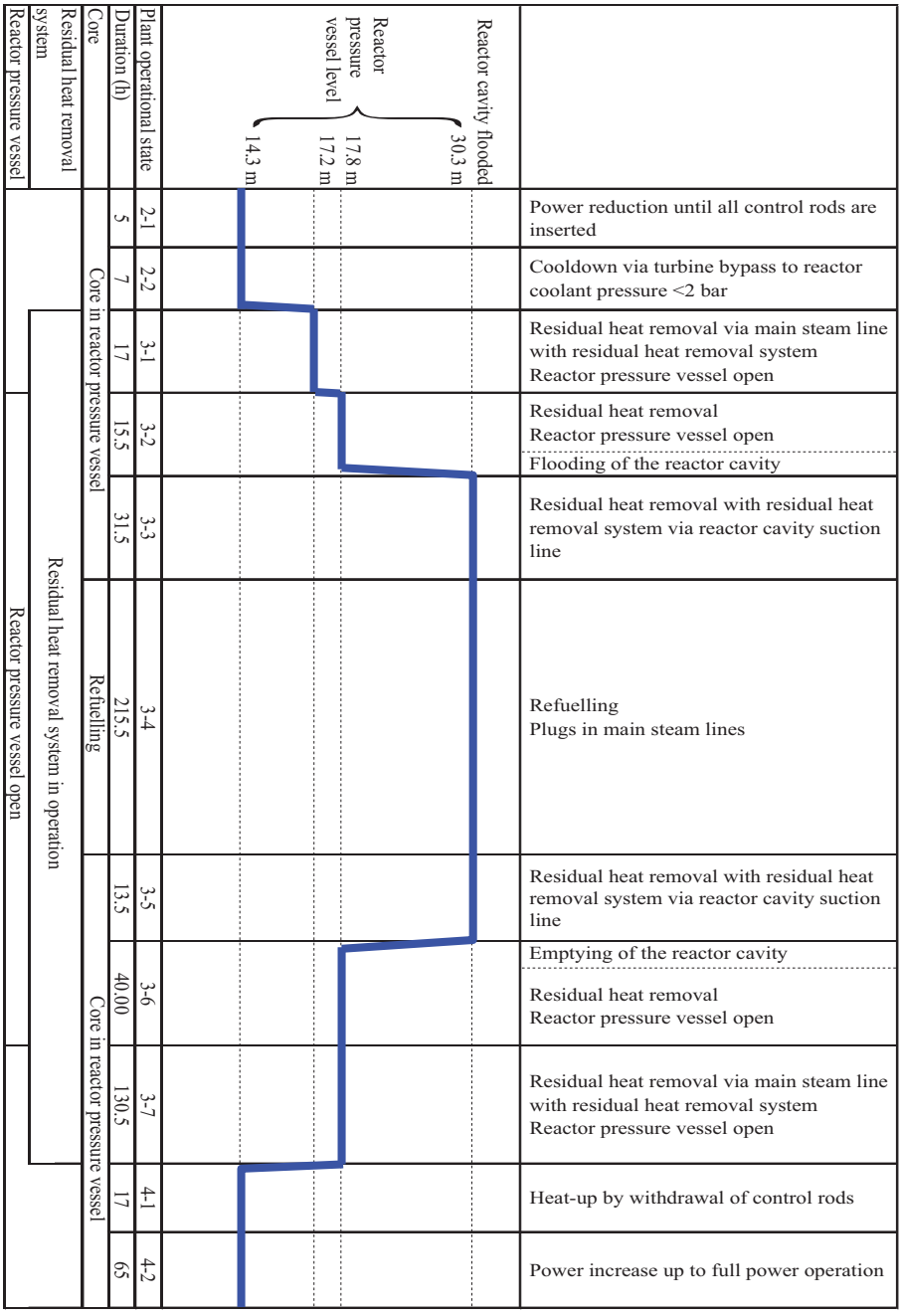

FIG. III–1. Reactor coolant level during outage.

TABLE III–1. PLANT OPERATIONAL STATES DURING OUTAGE IN THE REFERENCE PLANT

	Plant operational state	Characterization of plant operational 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 operational state										
		Shutdown		Outage							Restart	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
Transients												
T1	Loss of main heat sink	X	X									X
T2	Loss of preferred power	X	X	X	X	X	X	X	X	X	X	X
T3	Loss of main feedwater	X	X									X
T4	Loss of main feedwater and main heat sink	X	X									X
T5	Failure to close a safety valve	X	X								X	X
T6	Leak at suppression pool		X		X							
T7	Overfeeding of reactor pressure vessel with main feedwater system	X	X									X
T8	Overfeeding of reactor pressure vessel with residual heat removal system		X									
T9	Loss of residual heat removal			X	X	X	X	X	X	X		
T10	Loss of spent fuel pool cooling	X	X	X	X	X	X	X	X	X	X	X
TA	Anticipated transient without scram	X									X	X
Loss of coolant accidents												
S1	Leak at the reactor pressure vessel inside containment											
S1.1	Due to pipe rupture:											
S1.1.1	Above the core (A-nozzle)					X	X	X				
S1.1.2	Underneath the core (L-nozzle)					X	X	X				

TABLE III–2. INITIATING EVENTS DURING OUTAGE IN THE REFERENCE PLANT *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event respectively)* (cont.)

Initiating event		Plant operational state										
		Shutdown		Outage							Restart	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
S1.2	Due to human error during:											
S1.2.1	Inspection of valves in main steam line						X					
S1.2.2	Inspection of valves in core spray and in primary make-up systems						X					
S1.2.3	Pulling the shaft of a recirculation pump						X					
S1.2.4	Inspection of control rod drives						X					
S1.2.5	Change of in-core neutron flux detectors						X					
S2	Leak at the residual heat removal system			X	X	X	X	X	X	X		
S3	Leak at the reactor cavity seal liner				X	X	X	X	X			
S4	Leak into a connected system											
S4.1	Failure to control the level in reactor pressure vessel			X	X				X	X		
S4.2	Opening of a safety valve during residual heat removal			X	X	X		X	X	X		
S4.3	Leak in residual heat removal heat exchanger			X	X	X	X	X	X	X		
S5	Leak at the spent fuel pool			X	X	X	X	X	X	X		
Fire and internal flooding												
B1	Fire inside containment	X	X	X	X	X	X	X	X	X	X	X
B2	Fire outside containment	X	X	X	X	X	X	X	X	X	X	X
IF	Internal flooding			X	X	X	X	X	X	X		

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)* (cont.)

Initiating event		Plant operational 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
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 OPERATIONAL STATES OF A TWO WEEK OUTAGE IN THE REFERENCE PRESSURIZED WATER REACTOR PLANT

No.	Changes in physical condition / *System features*
(1)A0	Power reduction to condition subcritical hot / *Reactor protection signals and availability of safety systems same as during power operation*
(1)A1	Shutdown via steam generators down to primary system pressure of 3.1 MPa and primary system temperature of 120°C / *All reactor protection systems still available*
(1)B1	Primary system cooldown to depressurized cold / *Startup of the residual heat removal system at 120 °C, accumulators and high pressure pumps are disconnected*
(1)B2	Level lowering to mid-loop, mid-loop operation / *Core within reactor pressure vessel, primary system pressure tight closed*

TABLE III–3. PLANT OPERATIONAL STATES OF A TWO WEEK OUTAGE IN THE REFERENCE PRESSURIZED WATER REACTOR PLANT (cont.)

No.	Changes in physical condition / *System features*
(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 same as during power operation*

Note: (1) denotes plant operational state during shutdown, (2) denotes plant operational state during restart.

TABLE III–4. INITIATING EVENTS DURING LOW POWER AND SHUTDOWN MODES FOR PRESSURIZED WATER REACTOR *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event, respectively)*

	Plant operational state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Transients	Reactor pressure vessel closed				Reactor pressure vessel open					Reactor pressure vessel closed			
Loss of preferred power – external	x	x	x	x	x	x	x	x	x	x	x	x	x
Loss of preferred power – internal						x	x	x					
Loss of main feedwater without loss of main heat supply	x	x										x	x
Loss of main heat sink without loss of main feedwater	x	x										x	x
Loss of main feedwater and main heat sink	x	x										x	x
Main steam line leak outside containment	x	x										x	x
Main steam line leak inside containment	x	x										x	x
Feedwater line leak in turbine building	x	x										x	x
Feedwater line leak inside containment, non-isolable	x	x										x	x
Loss of residual heat removal due to:													
— Faulty level lowering				x					x				
— Operational failure of residual heat removal trains			x	x	x	x		x	x	x			
Unintended activation of emergency core cooling system signals				x									

TABLE III–4. INITIATING EVENTS DURING LOW POWER AND SHUTDOWN MODES FOR PRESSURIZED WATER REACTOR *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event, respectively)* (cont.)

	Plant operational state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Loss of coolant accidents	Reactor pressure vessel closed				Reactor pressure vessel open					Reactor pressure vessel closed			
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
Inadvertant open P-bdV[a] due to maintenance fault		x	x	x						x	x	x	
Inadvertant open P-bdV on loss of off-site power	x	x	x								x	x	x
Inadvertant open P-bdV after turbine trip	x	x	x								x	x	x
Steam generator tube leak	x	x	x								x	x	x
Leak in residual heat removal system inside containment			x	x	x	x	x	x	x	x			
Leak in residual heat removal system in annulus			x	x	x	x	x	x	x	x			
Leak in volume control system	x	x	x	x	x	x	x	x	x	x	x	x	x
Leak in reactor cavity/setdown pool						x		x					
Leak into an affiliated system			x	x	x	x	x	x	x	x			

TABLE III–4. INITIATING EVENTS DURING LOW POWER AND SHUTDOWN MODES FOR PRESSURIZED WATER REACTOR *(with indication of the loss of critical safety functions or the mechanism triggering the initiating event, respectively)* (cont.)

	Plant operational state												
Initiating event	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
Unexpected deboration	Reactor pressure vessel closed				Reactor pressure vessel open					Reactor pressure vessel closed			
Leaks from system containing unborated water:													
— Steam generator tube leak			x	x	x	x	x	x	x	x	x		
— Leak in residual heat removal heat exchanger			x	x	x	x	x	x	x	x	x		
— Leak in bearing seal			x	x	x	x	x	x	x	x	x		
— Inadvertent primary system injection			x	x	x	x	x	x	x	x	x		
Inadvertent unborated water in residual heat removal system			x	x	x	x	x	x	x	x	x		
Boron dilution during decontamination work									x				
Boron dilution during level raising										x			
Borating fault on shutdown		x											
Inadvertent boron dilution on shutdown following loss of all main coolant pumps												x	

[a] P-bdV denotes pressurizer blow down valve.

EXAMPLES FOR SPECIFIC SYSTEM MODELLING REQUIREMENTS

III–7. Reference [III–8] has been the primary and almost exclusive source for the examples presented in paras III–8 to III–10.

III–8. Particular systems may require specific modelling for low power and shutdown conditions. For example, fuel pool cooling systems might not be included in the analysis for full power operating conditions, but could be

important during shutdown conditions. Certain modes of operation of the residual heat removal system may also be used only during outages and these therefore need to be considered. The system models have to reflect the operating modes and specific system alignments. Success criteria, for example, *k* out of *n* trains of a particular system required, may be less stringent for low power or shutdown conditions because of the lower decay heat level. Detailed thermohydraulic calculations need to be performed to determine these criteria. The automatic start features of a system may be bypassed during low power or shutdown conditions in order to prevent an inadvertent start. For example, safety injection systems may be blocked with regard to automatic start mode to prevent actuation during shutdown. Thus, the control logic in the fault trees for these systems needs to be changed to reflect the fact that the systems will have to be manually initiated if required. Models for the related human interactions also need to be developed.

III–9. Manual recovery actions credited in the analysis for full power operating conditions may not be possible during the outage due to ongoing activities as part of the outage. For example, cross-connecting of low pressure systems may be an appropriate action during full power operation. However, during an outage, the cross-connection may be locked closed, or a system train may be entirely disabled. Therefore, if actions of this type are included in the fault trees for full power operation, they need to be modified for the low power and shutdown evaluation. In summary, each fault tree from the PSA for full power operating conditions adapted to the PSA for shutdown modes needs to be reviewed for each plant operational state to determine whether there are any features of that plant operational state that might have an impact on the logic of the fault tree structure.

III–10. The changing availabilities of the various systems during outage complicate the task of system modelling. Some systems or parts of systems may not be available during certain plant operational states. Also, the probability of component failure represented by a basic event may change. Most PSA software packages are based on a ‘fast cutset algorithm’, which generates and stores equations for minimal cutsets. An analysis of minimal cutsets can be carried out on several levels: a particular fault tree gate, an individual event tree sequence, or a particular consequence (every event tree sequence can be assigned one or more consequences, e.g. a plant damage state). An analysis case can specify a ‘boundary condition set’, which includes a list of value specifications or changes that need to be applied to the model. The boundary condition set can include true/false settings for logical switches, setting of probabilities for basic events and fault tree gates, setting of true/false states for

basic events and fault tree gates and setting of values for parameters. This is very useful for performing analyses of the same basic model with different variations depending on the plant operational 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 modes, 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 ACTIONS RELEVANT TO PSA FOR LOW POWER AND SHUTDOWN MODES

III–11. As a detailed analysis of all measures that could be taken by personnel during low power and 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 operational state selected for the PSA for low power and shutdown modes. 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 full power.

III–13. For the elements of this list, empirical evaluations, including, for example, plant walkdowns, of the working environment and the tasks are performed to identify potential human errors and consequences. The significance of each potential error is then judged. In determining possible consequences, it is distinguished between unavailabilities of components or system parts on the one hand and initiating events on the other.

III–14. In the first case, it is assessed how the failure can be detected, for which time interval unavailabilities or latent faults would result and for which initiating events these unavailabilities or latent faults would become evident. Finally, possible counter measures and consequences are described.

III–15. In the second case, the initiating event is classified (e.g. loss of coolant accident). Again, possible counter measures and consequences are described.

III–16. One important objective of such a screening analysis is to prepare, in a transparent and systematic way, a table comprising the entire screening results. Operating experience relevant to the potential errors or consequences is included.

III–17. If detailed analysis is deemed necessary, it can be performed using the approaches to human reliability analysis described in Section 5.

III–18. As an intermediate case, for groups of initiating events of similar nature (e.g. loss of coolant accidents with leak positions above the core), a rough estimate of the integral failure probability could be sufficient.

EXAMPLE OF AN OUTAGE RISK PROFILE AS AN OUTCOME OF A PSA FOR LOW POWER AND SHUTDOWN MODES FOR A BOILING WATER REACTOR PLANT

III–19. In Ref. [III–9], results of a PSA for low power and shutdown modes are presented for a boiling water reactor plant. Six plant operating states ("POS" in Figs III–2 and III–3) have been specified:

(1) Plant operational 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 operational state 2: Startup and hot shutdown with pressure from 35 kg/cm^2 to 10 kg/cm^2.
(3) Plant operational state 3: Hot shutdown with pressure lower than 10 kg/cm^2 and temperature higher than 93ºC.
(4) Plant operational state 4: Cold shutdown with temperature lower than 93ºC until the vessel head is removed.
(5) Plant operational state 5: Refuelling with the vessel head removed and the water level raised to the steam lines.
(6) Plant operational state 6: Refuelling with the vessel head removed and the water level raised to the spent fuel pool and the refuelling transfer tube open.

III–20. In Fig. III–2, for plant operational states 1–4, the thermal power and the pressure in the primary circuit are displayed as a function of time. In Fig. III–3, for plant operational states 1–4, the risk profile is shown. Clearly, the risk in plant operational state 4 is the highest, compared with the risk in the other plant operational states. This example emphasizes the insights provided by a risk profile, thereby helping to allocate efforts for safety improvements.

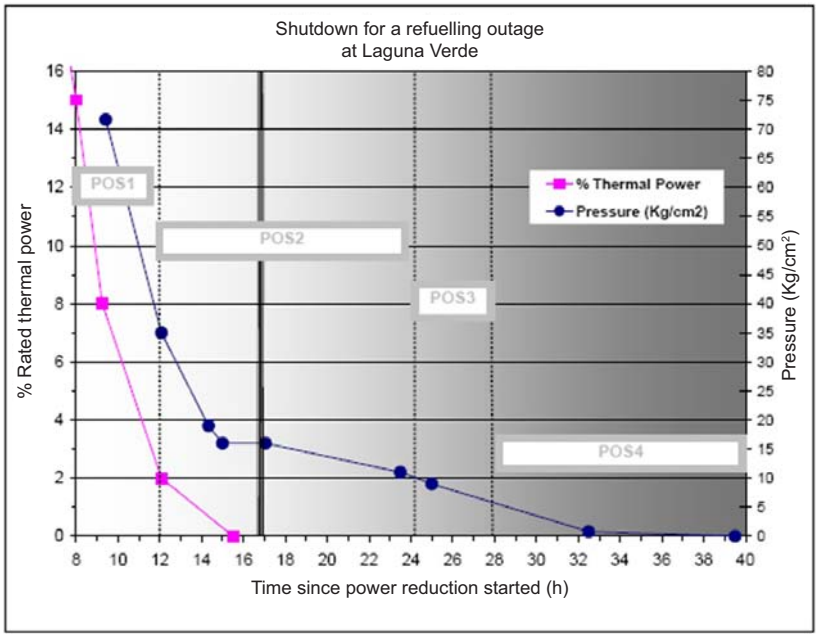

FIG. III–2. Plant operational states in PSA for low power and shutdown modes at Laguna Verde nuclear power plant. POS: plant operational state.

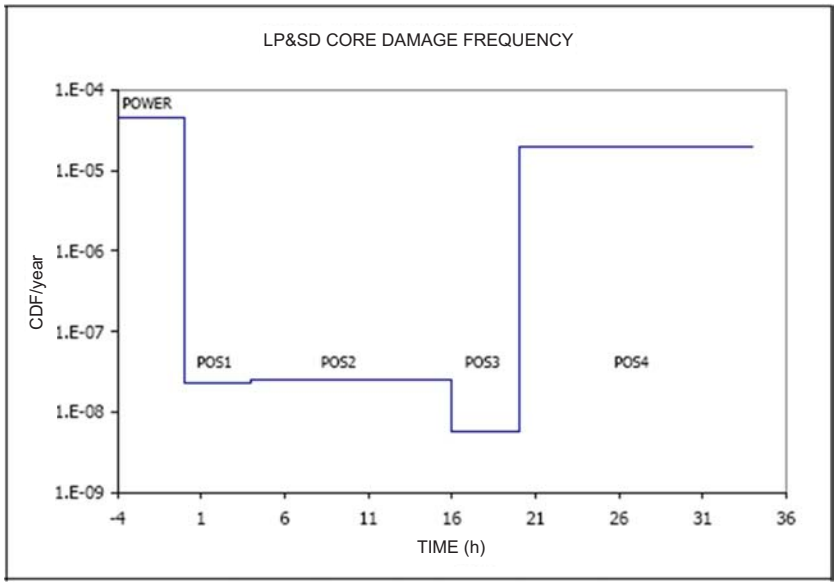

FIG. III–3. Comparison of core damage frequency per year for PSA for full power states and low power and shutdown modes. POS: plant operational state.

REFERENCES TO ANNEX III

[III–1] BABST, S., et al., "Insights and results of the shutdown PSA for a German SWR 69 type reactor", Probabilistic Safety Assessment and Management (Proc. 8th Int. Conf. New Orleans, 2006), ASME, New York (2006).

[III–2] MÜLLER-ECKER, D., MAYER, G., GASSMANN, D., "Probabilistic safety analysis for a modern 1300-MW_E pressurized water reactor under low-power and shut-down conditions", Probabilistic Safety Assessment and Management (Proc. 6th Int. Conf. San Juan, Puerto Rico, 2002), Elsevier Science, Oxford (2002).

[III–3] COOPERATIVE PROBABILISTIC RISK ASSESSMENT PROGRAM (COOPRA), Cooperative Probabilistic Risk Analysis, Low Power Shutdown Working Group, Status Report, October 2001, Idaho National Engineering and Environmental Laboratory, Idaho Falls (2001).

[III–4] COOPERATIVE PROBABILISTIC RISK ASSESSMENT PROGRAM (COOPRA), Cooperative Probabilistic Risk Analysis, Low Power Shutdown Working Group, Initiating Events — Summary, July 2004, Idaho National Engineering and Environmental Laboratory, Idaho Falls (2004).

[III–5] BUNDESMINISTERIUM FÜR UMWELT, NATURSCHUTZ UND REAKTORSICHERHEIT, Bekanntmachung des Leitfadens zur Durchführung der "Sicherheitsüberprüfung gemäß §19a des Atomgesetzes — Leitfaden Probabilistische Sicherheitsanalyse" für Kernkraftwerke in der Bundesrepublik Deutschland vom 30. August 2005, Bundesanzeiger **207a** (3 November 2005).

[III–6] FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-37/05, Bundesamt für Strahlenschutz, Salzgitter (2005).

[III–7] FACHARBEITSKREIS PROBABILISTISCHE SICHERHEITSANALYSE FÜR KERNKRAFTWERKE, Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, BfS-SCHR-38/05, Bundesamt für Strahlenschutz, Salzgitter (2005).

[III–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessments of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA-TECDOC-1144, IAEA, Vienna (2000).

[III–9] ESQUIVEL TORRES, J.L., LÓPEZ MORONES, R., "Probabilistic safety assessment for low-power and shutdown states for LVNPP", Probabilistic Safety Assessment and Management (Proc. 8th Int. Conf. New Orleans, 2006), ASME, New York (2006).

CONTRIBUTORS TO DRAFTING AND REVIEW

Alzbutas, R.	Lithuanian Energy Institute, Lithuania
Bagdonas, A.	Ignalina Nuclear Power Plant, Lithuania
Berg, P.	Bundesamt für Strahlenschutz, Germany
Bryant, R.	Rolls-Royce, United Kingdom
Burgazzi, L.	ENEA, Italy
Bykov, M.	OKB “Gidropress”, Russian Federation
El-Shanawany, M.	International Atomic Energy Agency
Elter, J.	Paks Nuclear Power Plant, Hungary
Fujimoto, H.	Japan Nuclear Energy Safety Organization, Japan
Goertz, R.	Bundesamt für Strahlenschutz, Germany
Hari, V.	Nuclear Power Corporation of India, India
Hessel, P.	Canadian Nuclear Safety Commission, Canada
Hlavac, P.	Relko Ltd, Slovakia
Husarcek, J.	Urad Jadroveho Dozoru SR, Slovakia
Hustak, S.	Nuclear Research Institute Rez, Czech Republic
Kajimoto, M.	Japan Nuclear Energy Safety Organization, Japan
Kirchsteiger, C.	European Commission
Kivirinta, T.	Fortum Power and Heat Oy, Finland
Kompella, D.	Swiss Federal Nuclear Safety Inspectorate, Switzerland
Kouzmina, I.	International Atomic Energy Agency
Kovacs, Z.	Relko Ltd, Slovakia

Loeffler, H.	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
Lopez, A.	Comisión Nacional de Seguridad Nuclear y Salvaguardias, Mexico
Lyubarskiy, A.	Scientific and Engineering Center for Nuclear and Radiation Safety, Russian Federation
Mancheva, K.	Risk Engineering Ltd, Bulgaria
Niemelä, I.	Radiation and Nuclear Safety Authority, Finland
Palmaerts, S.	Tractebel Engineering, Belgium
Papazov, V.	Kozloduy Nuclear Power Plant, Bulgaria
Parry, G.	Nuclear Regulatory Commission, United States of America
Rogers, P.	Rolls-Royce, United Kingdom
Röwekamp, M.	Gesellschaft für Anlagen- und Reaktorsicherheit, Germany
Shepherd, C.	Corporate Risk Associates, United Kingdom
Sorel, V.	Electricité de France DIN-SEPTEN, France
Taglioni, A.	ENEA, Italy
Tokmachev, G.	Atomenergoprojekt, Russian Federation
Tronea, M.	National Commission for Nuclear Activities Control, Romania
Tudor, C.	Cernavoda Nuclear Power Plant, Romania
Varde, P.	Bhabha Atomic Research Centre, India
Yang, J.	Korea Atomic Energy Research Institute, Republic of Korea

Yang, Zhichao	China Nuclear Power Technology Research Institute, China
Yli-Kauhaluoma, M.	Loviisa Nuclear Power Plant, Finland
Yllera, J.	International Atomic Energy Agency
Youngchuay, U.	Thailand Institute of Nuclear Technology, Thailand
Zeng, Yi	Canadian Nuclear Safety Commission, Canada
Zhao, Bo	Beijing Institute of Nuclear Engineering, China

BODIES FOR THE ENDORSEMENT OF IAEA SAFETY STANDARDS

An asterisk denotes a corresponding member. Corresponding members receive drafts for comment and other documentation but they do not generally participate in meetings. Two asterisks denote an alternate.

Commission on Safety Standards

Argentina: González, A.J.; *Australia*: Loy, J.; *Belgium*: Samain, J.-P.; *Brazil*: Vinhas, L.A.; *Canada*: Jammal, R.; *China*: Liu Hua; *Egypt*: Barakat, M.; *Finland*: Laaksonen, J.; *France*: Lacoste, A.-C. (Chairperson); *Germany*: Majer, D.; *India*: Sharma, S.K.; *Israel*: Levanon, I.; *Japan*: Fukushima, A.; *Korea, Republic of*: Choul-Ho Yun; *Lithuania*: Maksimovas, G.; *Pakistan*: Rahman, M.S.; *Russian Federation*: Adamchik, S.; *South Africa*: Magugumela, M.T.; *Spain*: Barceló Vernet, J.; *Sweden*: Larsson, C.M.; *Ukraine*: Mykolaichuk, O.; *United Kingdom*: Weightman, M.; *United States of America*: Virgilio, M.; *Vietnam*: Le-chi Dung; *IAEA*: Delattre, D. (Coordinator); *Advisory Group on Nuclear Security*: Hashmi, J.A.; *European Commission*: Faross, P.; *International Nuclear Safety Group*: Meserve, R.; *International Commission on Radiological Protection*: Holm, L.-E.; *OECD Nuclear Energy Agency*: Yoshimura, U.; *Safety Standards Committee Chairpersons*: Brach, E.W. (TRANSSC); Magnusson, S. (RASSC); Pather, T. (WASSC); Vaughan, G.J. (NUSSC).

Nuclear Safety Standards Committee

Algeria: Merrouche, D.; *Argentina*: Waldman, R.; *Australia*: Le Cann, G.; *Austria*: Sholly, S.; *Belgium*: De Boeck, B.; *Brazil*: Gromann, A.; **Bulgaria*: Gledachev, Y.; *Canada*: Rzentkowski, G.; *China*: Jingxi Li; *Croatia*: Valčić, I.; **Cyprus*: Demetriades, P.; *Czech Republic*: Šváb, M.; *Egypt*: Ibrahim, M.; *Finland*: Järvinen, M.-L.; *France*: Feron, F.; *Germany*: Wassilew, C.; *Ghana*: Emi-Reynolds, G.; **Greece*: Camarinopoulos, L.; *Hungary*: Adorján, F.; *India*: Vaze, K.; *Indonesia*: Antariksawan, A.; *Iran, Islamic Republic of*: Asgharizadeh, F.; *Israel*: Hirshfeld, H.; *Italy*: Bava, G.; *Japan*: Kanda, T.; *Korea, Republic of*: Hyun-Koon Kim; *Libyan Arab Jamahiriya*: Abuzid, O.; *Lithuania*: Demčenko, M.; *Malaysia*: Azlina Mohammed Jais; *Mexico*: Carrera, A.; *Morocco*: Soufi, I.; *Netherlands*: van der Wiel, L.; *Pakistan*: Habib, M.A.; *Poland*: Jurkowski, M.; *Romania*: Biro, L.; *Russian Federation*: Baranaev, Y.; *Slovakia*: Uhrik, P.; *Slovenia*: Vojnovič, D.; *South Africa*: Leotwane, W.; *Spain*: Zarzuela, J.; *Sweden*: Hallman, A.; *Switzerland*: Flury, P.; *Tunisia*: Baccouche, S.;

Turkey: Bezdegumeli, U.; *Ukraine*: Shumkova, N.; *United Kingdom*: Vaughan, G.J. (Chairperson); *United States of America*: Mayfield, M.; *Uruguay*: Nader, A.; *European Commission*: Vigne, S.; *FORATOM*: Fourest, B.; *IAEA*: Feige, G. (Coordinator); *International Electrotechnical Commission*: Bouard, J.-P.; *International Organization for Standardization*: Sevestre, B.; *OECD Nuclear Energy Agency*: Reig, J.; **World Nuclear Association*: Borysova, I.

Radiation Safety Standards Committee

**Algeria*: Chelbani, S.; *Argentina*: Massera, G.; *Australia*: Melbourne, A.; **Austria*: Karg, V.; *Belgium*: van Bladel, L.; *Brazil*: Rodriguez Rochedo, E.R.; **Bulgaria*: Katzarska, L.; *Canada*: Clement, C.; *China*: Huating Yang; *Croatia*: Kralik, I.; **Cuba*: Betancourt Hernandez, L.; **Cyprus*: Demetriades, P.; *Czech Republic*: Petrova, K.; *Denmark*: Øhlenschlæger, M.; *Egypt*: Hassib, G.M.; *Estonia*: Lust, M.; *Finland*: Markkanen, M.; *France*: Godet, J.-L.; *Germany*: Helming, M.; *Ghana*: Amoako, J.; **Greece*: Kamenopoulou, V.; *Hungary*: Koblinger, L.; *Iceland*: Magnusson, S. (Chairperson); *India*: Sharma, D.N.; *Indonesia*: Widodo, S.; *Iran, Islamic Republic of*: Kardan, M.R.; *Ireland*: Colgan, T.; *Israel*: Koch, J.; *Italy*: Bologna, L.; *Japan*: Kiryu, Y.; *Korea, Republic of*: Byung-Soo Lee; **Latvia*: Salmins, A.; *Libyan Arab Jamahiriya*: Busitta, M.; *Lithuania*: Mastauskas, A.; *Malaysia*: Hamrah, M.A.; *Mexico*: Delgado Guardado, J.; *Morocco*: Tazi, S.; *Netherlands*: Zuur, C.; *Norway*: Saxebol, G.; *Pakistan*: Ali, M.; *Paraguay*: Romero de Gonzalez, V.; *Philippines*: Valdezco, E.; *Poland*: Merta, A.; *Portugal*: Dias de Oliveira, A.M.; *Romania*: Rodna, A.; *Russian Federation*: Savkin, M.; *Slovakia*: Jurina, V.; *Slovenia*: Sutej, T.; *South Africa*: Olivier, J.H.I.; *Spain*: Amor Calvo, I.; *Sweden*: Almen, A.; *Switzerland*: Piller, G.; **Thailand*: Suntarapai, P.; *Tunisia*: Chékir, Z.; *Turkey*: Okyar, H.B.; *Ukraine*: Pavlenko, T.; *United Kingdom*: Robinson, I.; *United States of America*: Lewis, R.; **Uruguay*: Nader, A.; *European Commission*: Janssens, A.; *Food and Agriculture Organization of the United Nations*: Byron, D.; *IAEA*: Boal, T. (Coordinator); *International Commission on Radiological Protection*: Valentin, J.; *International Electrotechnical Commission*: Thompson, I.; *International Labour Office*: Niu, S.; *International Organization for Standardization*: Rannou, A.; *International Source Suppliers and Producers Association*: Fasten, W.; *OECD Nuclear Energy Agency*: Lazo, T.E.; *Pan American Health Organization*: Jiménez, P.; *United Nations Scientific Committee on the Effects of Atomic Radiation*: Crick, M.; *World Health Organization*: Carr, Z.; *World Nuclear Association*: Saint-Pierre, S.

Transport Safety Standards Committee

Argentina: López Vietri, J.; **Capadona, N.M.; *Australia*: Sarkar, S.; *Austria*: Kirchnawy, F.; *Belgium*: Cottens, E.; *Brazil*: Xavier, A.M.; *Bulgaria*: Bakalova, A.; *Canada*: Régimbald, A.; *China*: Xiaoqing Li; *Croatia*: Belamarić, N.; **Cuba*: Quevedo Garcia, J.R.; **Cyprus*: Demetriades, P.; *Czech Republic*: Ducháček, V.; *Denmark*: Breddam, K.; *Egypt*: El-Shinawy, R.M.K.; *Finland*: Lahkola, A.; *France*: Landier, D.; *Germany*: Rein, H.; *Nitsche, F.; **Alter, U.; *Ghana*: Emi-Reynolds, G.; **Greece*: Vogiatzi, S.; *Hungary*: Sáfár, J.; *India*: Agarwal, S.P.; *Indonesia*: Wisnubroto, D.; *Iran, Islamic Republic of*: Eshraghi, A.; *Emamjomeh, A.; *Ireland*: Duffy, J.; *Israel*: Koch, J.; *Italy*: Trivelloni, S.; **Orsini, A.; *Japan*: Hanaki, I.; *Korea, Republic of*: Dae-Hyung Cho; *Libyan Arab Jamahiriya*: Kekli, A.T.; *Lithuania*: Statkus, V.; *Malaysia*: Sobari, M.P.M.; **Husain, Z.A.; *Mexico*: Bautista Arteaga, D.M.; **Delgado Guardado, J.L.; **Morocco*: Allach, A.; *Netherlands*: Ter Morshuizen, M.; **New Zealand*: Ardouin, C.; *Norway*: Hornkjøl, S.; *Pakistan*: Rashid, M.; **Paraguay*: More Torres, L.E.; *Poland*: Dziubiak, T.; *Portugal*: Buxo da Trindade, R.; *Russian Federation*: Buchelnikov, A.E.; *South Africa*: Hinrichsen, P.; *Spain*: Zamora Martin, F.; *Sweden*: Häggblom, E.; **Svahn, B.; *Switzerland*: Krietsch, T.; *Thailand*: Jerachanchai, S.; *Turkey*: Ertürk, K.; *Ukraine*: Lopatin, S.; *United Kingdom*: Sallit, G.; *United States of America*: Boyle, R.W.; Brach, E.W. (Chairperson); *Uruguay*: Nader, A.; *Cabral, W.; *European Commission*: Binet, J.; *IAEA*: Stewart, J.T. (Coordinator); *International Air Transport Association*: Brennan, D.; *International Civil Aviation Organization*: Rooney, K.; *International Federation of Air Line Pilots' Associations*: Tisdall, A.; **Gessl, M.; *International Maritime Organization*: Rahim, I.; *International Organization for Standardization*: Malesys, P.; *International Source Supplies and Producers Association*: Miller, J.J.; **Roughan, K.; *United Nations Economic Commission for Europe*: Kervella, O.; *Universal Postal Union*: Bowers, D.G.; *World Nuclear Association*: Gorlin, S.; *World Nuclear Transport Institute*: Green, L.

Waste Safety Standards Committee

Algeria: Abdenacer, G.; *Argentina*: Biaggio, A.; *Australia*: Williams, G.; **Austria*: Fischer, H.; *Belgium*: Blommaert, W.; *Brazil*: Tostes, M.; **Bulgaria*: Simeonov, G.; *Canada*: Howard, D.; *China*: Zhimin Qu; *Croatia*: Trifunovic, D.; *Cuba*: Fernandez, A.; *Cyprus*: Demetriades, P.; *Czech Republic*: Lietava, P.; *Denmark*: Nielsen, C.; *Egypt*: Mohamed, Y.; *Estonia*: Lust, M.; *Finland*: Hutri, K.; *France*: Rieu, J.; *Germany*: Götz, C.; *Ghana*: Faanu, A.; *Greece*: Tzika, F.; *Hungary*: Czoch, I.; *India*: Rana, D.; *Indonesia*: Wisnubroto, D.; *Iran, Islamic*

Republic of: Assadi, M.; *Zarghami, R.; *Iraq*: Abbas, H.; *Israel*: Dody, A.; *Italy*: Dionisi, M.; *Japan*: Matsuo, H.; *Korea, Republic of*: Won-Jae Park; **Latvia*: Salmins, A.; *Libyan Arab Jamahiriya*: Elfawares, A.; *Lithuania*: Paulikas, V.; *Malaysia*: Sudin, M.; *Mexico*: Aguirre Gómez, J.; **Morocco*: Barkouch, R.; *Netherlands*: van der Shaaf, M.; *Pakistan*: Mannan, A.; **Paraguay*: Idoyaga Navarro, M.; *Poland*: Wlodarski, J.; *Portugal*: Flausino de Paiva, M.; *Slovakia*: Homola, J.; *Slovenia*: Mele, I.; *South Africa*: Pather, T. (Chairperson); *Spain*: Sanz Aludan, M.; *Sweden*: Frise, L.; *Switzerland*: Wanner, H.; **Thailand*: Supaokit, P.; *Tunisia*: Bousselmi, M.; *Turkey*: Özdemir, T.; *Ukraine*: Makarovska, O.; *United Kingdom*: Chandler, S.; *United States of America*: Camper, L.; **Uruguay*: Nader, A.; *European Commission*: Necheva, C.; *European Nuclear Installations Safety Standards*: Lorenz, B.; **European Nuclear Installations Safety Standards*: Zaiss, W.; *IAEA*: Siraky, G. (Coordinator); *International Organization for Standardization*: Hutson, G.; *International Source Suppliers and Producers Association*: Fasten, W.; *OECD Nuclear Energy Agency*: Riotte, H.; *World Nuclear Association*: Saint-Pierre, S.

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

DEVELOPMENT AND APPLICATION OF LEVEL 2 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-4
STI/PUB/1443 (2010)
ISBN 978–92–0–102210–3 Price: €22.00

DETERMINISTIC SAFETY ANALYSIS FOR NUCLEAR POWER PLANTS
IAEA Safety Standards Series No. SSG-2
STI/PUB/1428 (62 pp.; 2009)
ISBN 978–92–0–113309–0 Price: €23.00

SEVERE ACCIDENT MANAGEMENT PROGRAMMES FOR NUCLEAR POWER PLANTS
SAFETY GUIDE
IAEA Safety Standards Series No. NS-G-2.15
STI/PUB/1376 (66 pp.; 2009)
ISBN 978–92–0–112908–6 Price: €25.00

SAFETY ASSESSMENT FOR FACILITIES AND ACTIVITIES
IAEA Safety Standards Series No. GSR Part 4
STI/PUB/1375 (40 pp.; 2009)
ISBN 978–92–0–112808–9 Price: €48.00

EVALUATION OF SEISMIC SAFETY FOR EXISTING NUCLEAR INSTALLATIONS
IAEA Safety Standards Series No. NS-G-2.13
STI/PUB/1379 (84 pp.; 2009)
ISBN 978–92–0–100409–3 Price: €20.00

AGEING MANAGEMENT FOR NUCLEAR POWER PLANTS
Safety Guide
IAEA Safety Standards Series No. NS-G-2.12
STI/PUB/1373 (48 pp.; 2009)
ISBN 978–92–0–112408–1 Price: €20.00

Safety through international standards

The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.

This fundamental safety objective of protecting people — individually and collectively — and the environment has to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks.

— Fundamental Safety Principles: Safety Fundamentals,
IAEA Safety Standards Series No. SF-1 (2006)

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–114509–3
ISSN 1020–525X