IAEA SAFETY STANDARDS SERIES

Safety Assessment and Verification for Nuclear Power Plants

SAFETY GUIDE

No. NS-G-1.2

INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA

SAFETY ASSESSMENT AND VERIFICATION FOR NUCLEAR POWER PLANTS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN, REPUBLIC OF
BANGLADESH
BELARUS
BELGIUM
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BRAZIL
BULGARIA
BURKINA FASO
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHILE
CHINA
COLOMBIA
COSTA RICA
COTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
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
VIET NAM
YEMEN
YUGOSLAVIA
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".

Printed by the IAEA in Austria
November 2001
STI/PUB/1112

SAFETY STANDARDS SERIES No. NS-G-1.2

SAFETY ASSESSMENT AND VERIFICATION FOR NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2001

VIC Library Cataloguing in Publication Data

Safety assessment and verification for nuclear power plants : safety guide. —
Vienna : International Atomic Energy Agency, 2001.
p. ; 24 cm. — (Safety standards series, ISSN 1020–525X ; no. NS-G-1.2)
STI/PUB/1112
ISBN 92–0–101601–8
Includes bibliographical references.

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

VICL 01–00267

FOREWORD

by Mohamed ElBaradei
Director General

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following bodies oversee the development of safety standards: the Commission for Safety Standards (CSS); the Nuclear Safety Standards Committee (NUSSC); the Radiation Safety Standards Committee (RASSC); the Transport Safety Standards Committee (TRANSSC); and the Waste Safety Standards Committee (WASSC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA. Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

EDITORIAL NOTE

An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.

The English version of the text is the authoritative version.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. This publication supports the Safety Requirements on the Safety of Nuclear Power Plants: Design [1].

1.2. This Safety Guide was prepared on the basis of a systematic review of all the relevant publications including the Safety Fundamentals [2], Safety of Nuclear Power Plants: Design [1], current and ongoing revisions of other Safety Guides, INSAG reports [3, 4] and other publications that have addressed the safety of nuclear power plants. This Safety Guide also provides guidance for Contracting Parties to the Convention on Nuclear Safety in meeting their obligations under Article 14 on Assessment and Verification of Safety.

OBJECTIVE

1.3. The Safety Requirements publication entitled Safety of Nuclear Power Plants: Design [1] states that a comprehensive safety assessment and an independent verification of the safety assessment shall be carried out before the design is submitted to the regulatory body (see paras 3.10–3.13). This publication provides guidance on how this requirement should be met.

1.4. This Safety Guide provides recommendations to designers for carrying out a safety assessment during the initial design process and design modifications, as well as to the operating organization in carrying out independent verification of the safety assessment of new nuclear power plants with a new or already existing design. The recommendations for performing a safety assessment are suitable also as guidance for the safety review of an existing plant. The objective of reviewing existing plants against current standards and practices is to determine whether there are any deviations which would have an impact on plant safety. The methods and the recommendations of this Safety Guide can also be used by regulatory bodies for the conduct of the regulatory review and assessment. Although most recommendations of this Safety Guide are general and applicable to all types of nuclear reactors, some specific recommendations and examples apply mostly to water cooled reactors.

1.5. Terms such as ‘safety assessment’, ‘safety analysis’ and ‘independent verification’ are used differently in different countries. The way that these terms have been

used in this Safety Guide is explained in Section 2. The term ‘design’ as used here includes the specifications for the safe operation and management of the plant.

SCOPE

1.6. This Safety Guide identifies the key recommendations for carrying out the safety assessment and the independent verification. It provides detailed guidance in support of Ref. [1], particularly in the area of safety analysis. However, this does not include all the technical details which are available and reference is made to other IAEA publications on specific design issues and safety analysis methods.

1.7. Specific deterministic or probabilistic safety targets or radiological limits can vary in different countries and are the responsibility of the regulatory body. This Safety Guide provides some references to targets and limits established by international organizations. Operators, and sometimes designers, may also set their own safety targets which may be more stringent than those set by the regulator or may address different aspects of safety. In some countries operators are expected to do this as part of their ‘ownership’ of the entire safety case.

1.8. This Safety Guide does not include specific recommendations for the safety assessment of those plant systems for which dedicated Safety Guides exist.

STRUCTURE

1.9. Section 2 defines the terms ‘safety assessment’, ‘safety analysis’ and ‘independent verification’ and outlines their relationship. Section 3 gives the key recommendations for the safety assessment of the principal and plant design requirements. Section 4 gives the key recommendations for safety analysis. It describes the identification of postulated initiating events (PIEs), which are used throughout the safety assessment including the safety analysis, the deterministic transient analysis and severe accident analysis, and the probabilistic safety analysis. Section 5 gives the key recommendations for the independent verification of the safety of the plant.

2. SAFETY ASSESSMENT, SAFETY ANALYSIS AND INDEPENDENT VERIFICATION

SAFETY ASSESSMENT AND SAFETY ANALYSIS

2.1. In this context, safety assessment is the systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design of the plant. This would include also the requirements set by the operating organization and the regulators. Safety assessment includes, but is not limited to, the formal safety analysis (see Section 4). The design and the safety assessment are part of the same iterative process conducted by the plant designer which continues until a design solution which meets all the safety requirements, which may also include those developed during the course of the design, has been reached.

2.2. The scope of the safety assessment is to check that the design meets the requirements for management of safety, the principal technical requirements, the plant design and plant system design requirements given in Sections 3–6 of Safety of Nuclear Power Plants: Design [1], and that a comprehensive safety analysis has been carried out.

2.3. The requirements for management of safety (Section 3 in Ref. [1]) address the issues which relate to proven engineering practice, operating experience and safety research.

2.4. The principal technical requirements (Section 4 in Ref. [1]) include those which ensure that sufficient defence in depth has been provided and that the highest consideration is given to accident prevention and radiation protection.

2.5. The plant design requirements (Section 5 in Ref. [1]) relate to issues such as equipment qualification, ageing and the reliability of safety systems through the provision of redundancy, diversity and physical separation.

2.6. The plant system design requirements (Section 6 in Ref. [1]) address the issues which relate to the design of the reactor core, the reactor coolant system and the safety systems such as containment and emergency core cooling systems.

2.7. Regarding safety analysis, para. 5.69 in Ref. [1] states 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 shall also be demonstrated that the plant as designed is capable of meeting any prescribed limits for radioactive releases and acceptable limits for potential radiation doses for each category of plant states, and that defence in depth has been effected." The scope and objectives of the deterministic and probabilistic safety analyses are outlined in paras 4.17–4.22 below.

INDEPENDENT VERIFICATION

2.8. Paragraph 3.13 in Ref. [1] states that "The operating organization shall ensure that an independent verification of the safety assessment is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body."

2.9. The independent verification should be carried out under the responsibility of the operating organization by a team of experts who are, as far as possible, independent of the designers and those performing the safety assessment. Personnel are considered independent if they have not participated in any part of the design and safety assessment. This independent verification is in addition to the quality assurance (QA) reviews carried out within the design organization.

2.10. Whereas the safety assessment is a comprehensive study carried out by the designers throughout the design process to address all relevant safety requirements, the independent verification would be carried out by or on behalf of the operating organization and may only relate to the design as delivered to the regulatory body for approval.

2.11. Owing to the complexity of the design and safety assessment issues that need to be addressed by the independent verification, this would typically be partly carried out in parallel with the design process rather than left to the end.

2.12. A separate independent review would be carried out by the regulators to check that the design meets their requirements.

RELATIONSHIP BETWEEN THE DESIGN, SAFETY ASSESSMENT AND INDEPENDENT VERIFICATION

2.13. Figure 1 shows the relationship between the safety assessment, independent verification, safety analysis and the other activities carried out during the design of a

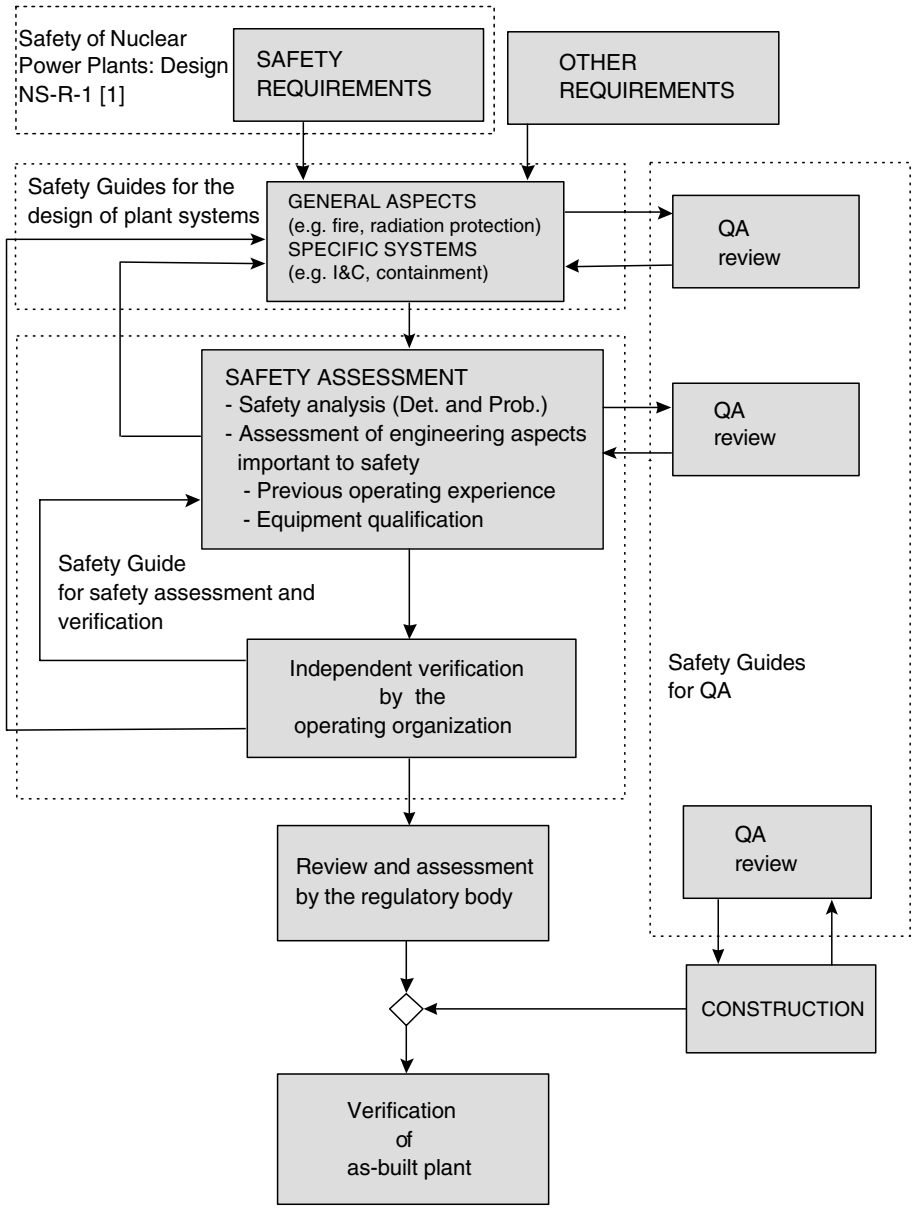

FIG. 1. Areas covered by the IAEA safety standards for the design of nuclear power plants [1] (Det.: deterministic; Prob.: probabilistic).

nuclear power plant. This figure also shows how the present Safety Guide relates to other IAEA publications relevant to the design process.

2.14. As the design is developed from a preliminary concept through to a complete design, the designer needs to take into account all the safety and other requirements defined by both the plant operator and the regulator. For developing nuclear programmes and the introduction of new designs, the design requirements may be revised or clarified during the design process. In the case of novel designs, detailed requirements may be developed while the design is in progress.

2.15. Throughout the design process, the safety assessment and independent verification are carried out by different groups or organizations. However, they are integral parts of an iterative design process and both have the main objective of ensuring that the plant meets the safety requirements. For this reason, both topics are addressed in the same Safety Guide. In some cases, the regulatory body is also involved during the design phase.

2.16. At various stages during the course of the design process (for example, before the start of construction or operation at power) the status of the design will be frozen and a safety analysis report will be produced that will describe the design and safety assessment that has been carried out up to that point. This provides input for the review and assessment of the regulatory body.

2.17. The independent verification is more effective if it is carried out in parallel with the design and safety assessment since early discussion and clarification of safety issues speeds up and facilitates their resolution. Any recommendations made to improve the design or safety assessment are most easily accommodated while the design work is still in progress. On the other hand, too close a relation will call into question the independence of the verification and a balance should be struck between effectiveness and independence.

2.18. Major design decisions to be taken in the course of the design may require special independent design reviews by the operating organization which are limited to the scope of the decision to be taken, and which may consider compliance with the safety requirements applicable to the matter to be decided.

2.19. The design work should be performed according to a QA programme which includes independent reviews of all design documents. The general QA process is addressed in Safety Guide SG-Q-10 [5].

3. ENGINEERING ASPECTS IMPORTANT TO SAFETY

GENERAL

3.1. This section includes recommendations and important considerations for assessing the compliance of the design with the requirements of Sections 3–5 of Ref. [1]. These requirements cover general engineering aspects important to safety and apply to all systems of the nuclear plant. While the assessment of the correct implementation of the requirements for such aspects may not be explicitly addressed in the safety analysis, it constitutes a relevant part of the safety assessment. For some of these aspects, no well-defined acceptance criteria are available and therefore the assessment of the compliance with the safety requirements is largely based on good engineering judgement.

PROVEN ENGINEERING PRACTICES AND OPERATIONAL EXPERIENCE

3.2. For reactors of an evolutionary type, wherever possible, the design should use structures, systems and components (SSCs) with previous successful applications in operating plants, or at least take due account of relevant operational experience which has been gained at other plants.

3.3. Available operating experience should be taken into account in the safety assessment with the aim of ensuring that all relevant lessons in the area of safety have been adequately considered in the design. Operating experience should be a fundamental source of information to improve the defence in depth of the plant.

3.4. The operational experience feedback on design and safety assessment should make full use of the large amount of operating information which is, in most part, openly available to interested organizations and individuals. The data on operating experience should be drawn from: (i) the national data bank; (ii) the incident reporting systems of the World Association of Nuclear Operators (WANO) and the IAEA–OECD Nuclear Energy Agency (OECD NEA); and (iii) the reports of IAEA ASSET (Assessment of Safety Significant Events Team) missions.

3.5. Extrapolative analysis from a real event sequence to what might ultimately have happened in a plant if there had been additional malfunctions (compared with the malfunctions which happened in the real situation) has been demonstrated to be a useful design tool.

3.6. The results of general safety research programmes may also provide useful support to designers and reviewers in their evaluation tasks. The results of safety research are generally available in open meetings, the literature and computer databases. The IAEA generic safety issues databases and IAEA technical documents (IAEA-TECDOCs) are examples of international results in the area of safety research.

INNOVATIVE DESIGN FEATURES

3.7. Based on lessons learned from operating experience, safety analysis and safety research, it is necessary to allow for consideration of the need for and value of design improvements beyond established practice. Where an innovative or non-proven design or design feature is introduced, compliance with the safety requirements should be demonstrated by an appropriate supporting demonstration programme and the features should be adequately tested before being put into service.

3.8. For example, passive safety systems are independent from external support systems such as electric power and have the potential for being simpler and more reliable than active systems. However, the actual performance and reliability of passive systems should be convincingly proven by appropriate and thorough development, testing and analysis programmes.

3.9. Another example of application of modern technology is the use of computer based safety and control systems. Computerized systems have potential advantages compared to classical hard wired systems, including greater functionality, better capability for testing and higher reliability of the hardware. These advantages, however, may have been gained in some embodiments at the expense of simplicity and transparency, and hence extensive assessment and testing should be performed to prove the performance and the overall reliability of the computerized systems, including the software, under conditions as close as possible to the real operating conditions. Further guidance in this area can be found in Ref. [6].

IMPLEMENTATION OF DEFENCE IN DEPTH

3.10. The objective of the defence in depth strategy as indicated in para. 2.10 of Ref. [1] is twofold: first, to prevent accidents and second, if prevention fails, to detect and limit their potential consequences and to prevent any evolution to more serious conditions.

TABLE I. OBJECTIVE OF EACH LEVEL OF PROTECTION AND ESSENTIAL MEANS OF ACHIEVING THEM

Level	Objective	Essential means
Level 1	Prevention of abnormal operation and of failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and emergency procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

3.11. Defence in depth is generally structured in five levels. Should one level fail, it would be compensated for or corrected by the subsequent level. The levels of defence are implemented so as to be independent of the effectiveness of higher and lower levels of defence. The objective of each level of protection and the essential means of achieving them are shown in Table I. Measures on the first three levels of defence should be considered within the design basis in order to ensure maintenance of the structural integrity of the core and to limit potential radiation hazards to members of the public. By contrast, measures on the fourth level of defence should be considered beyond the design basis in order to keep the likelihood and the radioactive releases of severe plant conditions as low as reasonably achievable (ALARA), taking economic and social factors into account.

3.12. The highest priority should be given to the prevention of: undue challenges to the integrity of physical barriers; failure or bypass of a barrier when challenged; failure of a barrier as a consequence of failure of another barrier; and significant releases of radioactive materials.

3.13. The design should be assessed to verify that specific measures are implemented to ensure the effectiveness of defence levels 1 to 4.

3.14. The assessment of the implementation of defence in depth should be achieved through the demonstration of compliance with a large number of requirements supported by the complete safety analysis. This assessment should confirm that possible initiating events are adequately dealt with on the respective defence in depth level by ensuring that the fundamental safety functions are performed and that the release of radioactive materials is controlled.

3.15. The assessment process should pay special attention to internal and external hazards which could have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of redundant equipment of safety systems.

3.16. The design should have provisions to detect the failure or bypass of each level of defence as far as applicable. The requested levels of defence should be specified for each operational mode (for example, an open containment may be allowed in certain shutdown modes, and the specified levels of defence should be available at all times when in that mode).

RADIATION PROTECTION

3.17. Detailed recommendations on design aspects of radiation protection are given in a specific IAEA Safety Guide[1]. The designer should consider these recommendations for the plant design. The subject of the assessment is the demonstration of the compliance with the Radiation Protection Objective as it is stated in the Safety Fundamentals. Some significant aspects of the radiation protection design are discussed below.

3.18. Two design objectives should be considered for normal operation and anticipated operational occurrences: (1) keep the radiation doses below prescribed limits, and (2) keep the radiation doses as low as reasonably achievable. The compliance with the first objective should be demonstrated by comparing the calculated equivalent dose with the prescribed limit specified in the national legislation. The relevant design calculations should be assessed by the designer to ensure the correctness of the input data and the validity of the methodology used (see Section 4).

---

[1] Safety Series No. 50-SG-D9, Design Aspects of Radiation Protection for Nuclear Power Plants (1985).

3.19. The second design objective (meeting the ALARA principle) implies that all doses should be kept as low as reasonably achievable, taking economic and social factors into account. The process of optimization of radiation protection should involve some degree of balancing detriments (costs) and benefits (safety gains). In this optimization process, orientation values for radiation exposures and related design measures could be derived from similar existing plants with good operating records. The safety assessment should take into account the operational experience and consider additional design provisions or improvements to further reduce the radiation exposure to workers and members of the public. Such measures could be either direct (improved shielding) or indirect (reduction of equipment maintenance time).

3.20. The exposures should be kept low through practices such as minimization of cladding defects, use of corrosion resistant materials, reduction of formation of long lived corrosion and activation isotopes, very low primary circuit coolant leakage, minimization of maintenance in high radiation areas and use of remote handling tools and robots.

3.21. Provisions such as sufficient space for inspection and maintenance, adequacy of shielding for radiation protection, and correct installation of plant equipment should be systematically assessed during the design.

3.22. The plant designer and safety assessor should also take into account the operational doses during the final decommissioning. Choice of materials and space for access to dismantle equipment and tools are among the subjects deserving attention, as is the use of 'sacrificial layers' in structures subject to high radiation doses, e.g. concrete shields around the pressure vessel to minimize the amount of highly active waste and to facilitate its removal.

3.23. The design of spaces and equipment such as spent fuel storage and handling facilities, and radioactive waste storage should account for provisions to minimize the release that could result from their failure.

3.24. The designer should show that sufficient design measures have been effected to allow adequate monitoring for radiation protection in accordance with Ref. [1].

3.25. The adequacy of design provisions for protection against accident conditions should be assessed by comparing the releases and the doses calculated in the safety analysis with the limits specified or accepted by the regulatory body. The mitigation of the radiological consequences of beyond design basis accidents may require special actions on the site and around the plant (accident management and emergency

response planning). In the safety assessment the designer should ensure that the relevant parameters for accident management and emergency planning have been adequately incorporated into the plant design.

SAFETY CLASSIFICATION OF STRUCTURES, SYSTEMS AND COMPONENTS

3.26. The importance to safety of all SSCs should be established and a safety classification system as defined in Ref. [1] should be set up in order to identify for each safety class:

- The appropriate codes and standards, and hence the appropriate provisions to be applied in design, manufacturing, construction and inspection of a component;
- System related characteristics like degree of redundancy, need for emergency power supply and for qualification to environmental conditions;
- The availability or unavailability status of systems for PIEs to be considered in deterministic safety analysis;
- QA provisions.

3.27. In general, the following classifications should be established and should be verified for adequacy and consistency:

- Classification of systems on the basis of the importance of the affected safety function;
- Classification for pressure components, on the basis of the severity of the consequences of their failure, mechanical complexity and pressure rating;
- Classification for resistance to earthquakes, on the basis of the need for the structure or component considered to retain its integrity and to perform its function during and after an earthquake, taking into account aftershocks and consequent incremental damage;
- Classification of electrical, instrumentation and control systems on the basis of their safety or safety support functions, which may be different from the classification of other plant systems owing to the existence of field specific, widely used classification schemes;
- Classification for QA provisions.

3.28. The assignment of SSCs to safety classes should be based on national approaches and should appropriately credit deterministic and probabilistic considerations as well as engineering judgement.

3.29. For the purposes of the deterministic safety analysis, those safety functions that are used to determine compliance with acceptance criteria should be performed using classified SSCs only.

3.30. Probabilistic safety analysis (PSA) can be used in the design phase to confirm the appropriate classification of structures, systems and components.

3.31. The failure of a system and/or component in one safety class should not cause the failure of other systems and/or components of a higher safety class. The adequacy of the isolation and separation of different and potentially interacting systems assigned to different safety classes should be assessed.

PROTECTION AGAINST EXTERNAL EVENTS

3.32. External events are extensively addressed in several specific IAEA Safety Series publications[2] that also provide guidance for the safety assessment. Some key issues are, however, summarized in the following.

3.33. The set of events which should be addressed in the safety assessment depends on the site chosen for the plant but would typically include:

Natural external events such as:

— Extreme weather conditions;
— Earthquakes;
— External flooding;

[2] Safety Series Nos 50-SG-D5, External Man-induced Events in Relation to Nuclear Power Plant Design (1996); 50-SG-D15, Seismic Design and Qualification for Nuclear Power Plants (1992); 50-C-S (Rev. 1), Code on the Safety of Nuclear Power Plants: Siting (1988); 50-SG-S1 (Rev. 1), Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting (1991); 50-SG-S5, External Man-induced Events in Relation to Nuclear Power Plant Siting (1981); 50-SG-S7, Nuclear Power Plant Siting: Hydrogeologic Aspects (1984); 50-SG-S10A, Design Basis Flood for Nuclear Power Plants on River Sites (1983); 50-SG-S10B, Design Basis Flood for Nuclear Power Plants on Coastal Sites (1983); 50-SG-S11A, Extreme Meteorological Events in Nuclear Power Plant Siting, Excluding Tropical Cyclones (1981); 50-SG-S11B, Design Basis Tropical Cyclone for Nuclear Power Plants (1984).

Human made events such as:

— Aircraft crashes;
— Hazards arising from transportation and industrial activities (fire, explosion, missiles, release of toxic gases).

3.34. The design basis should be adequate for the selected site and based on historical and physical data, and expressed by a set of values selected on the general probability distribution of each event according to specified thresholds[3].

3.35. When such a probabilistic evaluation is not possible because of lack of confidence in the quality of data, deterministic approaches are applied, relying upon enveloping criteria and engineering judgement.

3.36. The SSCs which are required to perform the fundamental safety functions should be designed to withstand the loads induced by the design basis events and able to perform their functions during and after such events. This should be achieved through adequate structural design, redundancy and separation.

3.37. The radiological risk associated with external events should not exceed the range of radiological risk associated with the accident of internal origin. It should be verified that external events that are slightly more severe than those included in the design basis do not lead to a disproportionate increase in consequences.

3.38. Extreme weather conditions: a design basis event should be defined for each of the extreme weather conditions. This would include the following:

— Extreme wind loading,
— Extreme atmospheric temperatures,
— Extremes of rainfall and snowfall,
— Extreme cooling water temperatures and icing,
— Extreme amounts of sea vegetation.

3.39. The design basis should take into account the combinations of extreme weather conditions that could reasonably be assumed to occur at the same time.

---

[3] In some Member States the design is expected to provide protection against those natural events with a frequency greater than 10^{-4} per year. See also Safety Series No. 50-SG-S1 (Rev. 1), Earthquakes and Associated Topics in Relation to Nuclear Power Plant Siting (1991).

3.40. It should be demonstrated by tests, experiments or engineering analyses that structures in the nuclear power plant will withstand the loading imposed by the external events without inducing any failure of items necessary to bring the plant back to and maintain it in a state where all fundamental safety functions can be guaranteed in the long term.

3.41. It should be demonstrated by tests, experiments or engineering analyses that safety systems can perform their safety functions in the range of conditions (e.g. atmospheric temperatures, sea water temperatures and levels) specified in the design basis.

3.42. Results of geological surveys of the region surrounding the site, historical information on the occurrence of earthquakes in the region, and palaeoseismic data should be used to derive the SL-2 earthquake for the site, as indicated in IAEA Safety Series No. 50-SG-S1 (Rev. 1).[4] The SL-2 earthquake should be used to establish the design basis earthquake (DBE) for the nuclear power plant.

3.43. The systems, structures and components with the function of shutting down the plant and maintaining it in a long term safe stable state should be designed to withstand the design basis earthquake without a loss of function.

3.44. The seismic qualification should include structural analysis, shaker table testing and comparison with operating experience, as appropriate.

3.45. External flooding: the region surrounding the site should be evaluated to determine the potential for an external flood to occur which could endanger the nuclear power plant. This should include the potential for flooding due to high precipitation, high tides, overflowing of rivers, failure of dams and their possible combination.

3.46. Protection should be provided to prevent an external flood leading to the failure of safety system equipment.[5]

---

[4] Safety Series No. 50-SG-S1 (Rev. 1), Earthquakes and Associated Topics in Relation to Nuclear Power Siting (1991). This Safety Guide also defines a second earthquake level (SL-1) which corresponds to an earthquake often denoted as operational basis earthquake (OBE) which can reasonably be expected to occur at the plant site during its operating life. It may also correspond to the inspection level earthquake after which the plant safety is reassessed to continue operation.

[5] For further information on external flooding refer to Safety Series Nos 50-SG-S10A, Design Basis Flood for Nuclear Power Plants on River Sites (1983); 50-SG-S10B, Design Basis Flood for Nuclear Power Plants on Coastal Sites (1983).

3.47. The estimated probability of aircraft crashes on the plant should be derived from relevant crash statistics taking into account the distance from airports, the flight paths and the number of movements for all types of aircraft near the specific site. The crash statistics should be kept up to date throughout the plant's life.

3.48. If the estimated probability of aircraft crashes is greater than the acceptable value, the protection should include strengthening the structures that have systems and components which are important to safety and the separation and segregation of redundant trains of equipment in such a manner that they would not all be damaged by the impact of an aircraft or a subsequent fuel fire. Protection against aircraft crashes should be focused on items necessary to bring the plant back to a safe condition and maintain it in a state in which all safety functions can be guaranteed.[6]

3.49. For hazards arising from transportation and industrial activities, transport of hazardous material close to the site[7] and industrial activities which cause fire, explosion, missiles and release of toxic gases and affect the safety of the nuclear power plant should be identified and the design basis events specified.

PROTECTION AGAINST INTERNAL HAZARDS

3.50. Internal hazards are extensively addressed in specific IAEA Safety Series publications[8] that also provide guidance for the safety assessment. Some key issues are summarized in this section.

3.51. The design should take into consideration specific loads and environmental conditions (temperature, pressure, humidity, radiation) imposed on structures or components by internal events such as:

---

[6] For further information on the consideration of aircraft crashes, refer to Safety Series No. 50-SG-S5, External Man-induced Events in Relation to Nuclear Power Plant Siting (1981); this will be superseded by a Safety Guide on External Human Induced Events in Site Evaluation for Nuclear Power Plants (to be published).

[7] For further information on the consideration of hazards arising from industrial activity, refer to Safety Series No. 50-SG-S5(to be superseded; see footnote 6).

[8] Safety Standards Series No. NS-R-1, Safety of Nuclear Power Plants: Design (2000); Safety Series No. 50-SG-D2, Fire Protection in Nuclear Power Plants (1992); 50-SG-D4, Protection Against Internally Generated Missiles and their Secondary Effects in Nuclear Power Plants (1980).

— Pipe whipping;
— Impingement forces;
— Internal flooding and spraying due to leaks or breaks of pipes, pumps, valves;
— Internal missiles;
— Load drop;
— Internal explosion;
— Fire.

3.52. It should be demonstrated that the effects of pipe failures such as jet impingement forces, pipe whip, reaction forces, pressure wave forces, pressure buildup, humidity, temperature and radiation on components, building structures, electrical and instrumentation and control (I&C) equipment are sufficiently taken into account. Specifically, it should be shown that:

— Reaction forces have been taken into account in the design of safety classified equipment, supports for this equipment, and associated building structures;
— Components important to safety and their internals have been designed against credible pressure wave forces and flow forces;
— Pressure buildup has been considered for buildings important to safety such as the containment;
— Electrical and I&C equipment important to safety has been designed to withstand temperature, humidity and radiation extremes in the event of postulated leaks and breaks.

3.53. Regarding internal flooding, a flooding analysis for the relevant buildings of the plant should be performed and the following potential initiators of flooding should be considered: leaks and breaks in pressure retaining components, flooding by water from neighbouring buildings, spurious actuation of the fire fighting system, overfilling of tanks, and failures of isolating devices.

3.54. SSCs important to safety should be located at an elevation higher than the expected maximum flood level or should be sufficiently protected.

3.55. Internal missiles can be generated by failure of rotating components such as turbines or by failure of pressurized components. Preferential flight paths of possible turbine missiles should be considered and reflected in the orientation of the turbine with respect to safety classified buildings, unless it can be demonstrated that potential missiles are not likely to result in significant damage to SSCs important to safety. Similarly, the location of high energy components in safety classified buildings should be restricted to the extent possible.

3.56. The failure of lifting gears should be considered in the design when the associated load drop can result in radiation exposure inside or outside the plant, or when it can cause damage of a system important to safety.

CONFORMITY WITH APPLICABLE CODES, STANDARDS AND GUIDES

3.57. To ensure the safety of the nuclear power plant, design of SSCs should take into account their safety related significance. Design of SSCs important to safety should be performed according to design requirements corresponding to the importance of the safety functions to be performed. The class assigned to the SSCs provides a basis for determining codes and standards which will be applied to the design of the SSCs.

3.58. In general, a list of codes and standards for design are given by the operating organization in the form of utility requirements or directly by the regulatory body. However, they should be reviewed and analysed to evaluate their applicability, adequacy and sufficiency for the design of SSCs important to safety according to current knowledge and technology. If some codes and standards are insufficient to ensure the SSC quality corresponding to the importance of the safety function to be performed, these should be supplemented or modified as necessary in order to ensure commensurate SSC quality.

LOAD AND LOAD COMBINATION

3.59. Relevant safety classified structures and components should be designed to withstand all relevant loading resulting from operational states and design basis accidents including those resulting from internal and external hazards.

3.60. A significant part of the safety assessment is therefore:

— To identify for each safety classified structure or component the relevant loading and loading combinations;
— To identify for each loading and loading combination the expected frequency of occurrence;
— To evaluate the stresses and strains in the safety classified structures and components for the identified loading and loading combinations;
— To evaluate the individual and cumulative damage in the structure or component taking account of all relevant deteriorations (e.g. creep, fatigue, ageing) and their potential interactions.

3.61. The set of loading and loading combinations should be complete and consistent with the assumptions of the safety analysis. The expected frequency of occurrence, together with the total number of anticipated transients during plant life, should be assessed based on historical records, operating experience, utility requirements or site characteristics, as appropriate.

3.62. In addition to all pertinent physical quantities, the evaluation of stresses and strains should consider the environmental conditions resulting from each loading, each loading combination and appropriate boundary conditions. The acceptance criteria should adequately reflect the prevention of consequential failure of structures or components needed to mitigate the consequences of the hazards which are correlated to the assumed loading.

SELECTION OF MATERIALS

3.63. Materials should meet the standards and requirements for their design and fabrication. The design lifetime of the materials should be determined considering the effects of operational conditions (e.g. radiological and chemical environment, single and periodic loads). In addition, effects of design basis accidents on their characteristics and performance should be considered.

3.64. For materials whose adequacy is based on testing, all test results should be documented.

3.65. Materials in contact with radioactive effluents should have anticorrosion properties against relevant corrosion mechanisms and resistance to chemical reactions under operational conditions. Contact of carbon steel with radioactive products should be avoided as much as possible. Polymer materials should be radiation resistant if used for systems containing radioactive effluents.

3.66. Stainless steel or nickel alloys, materials of steam generator tubes, major pipes and cladding in contact with reactor coolant should have adequate anticorrosion properties. Low melting point elements such as lead, antimony, cadmium, indium, mercury, zinc, bismuth, tin and their alloys should not enter into contact with the components of the reactor primary coolant system or the secondary system fabricated with stainless steel or nickel alloy. Bearing alloys containing low melting point elements should be prevented from contaminating the feedwater system. In order to reduce operational doses, the content of cobalt in materials in contact with reactor coolant should be limited as much as possible, and justification should be provided

when cobalt alloy is exceptionally used. The release to the reactor coolant of nickel from materials in contact with the coolant should be evaluated.

3.67. Control of halogen elements in materials (e.g. pipe insulation) in contact with stainless steel components should be ensured by design in order to avoid inter-granular stress corrosion cracking (IGSCC).

3.68. For ferritic materials of the reactor coolant pressure boundary, the resistance against rapidly propagating fracture and fatigue resistance under high temperature and pressure should be proved. All weldments of stainless steel should have resistance against grain boundary corrosion, and delta ferrite content should be controlled to minimize microcrack formation during austenitic stainless steel welding.

3.69. Particular attention should be given to compatibility of the materials used with regard to the water chemistry in order to prevent corrosion phenomena. For all equipment exposed to damp steam or to fluids which can cause severe erosion, corrosion and erosion resistant materials should be used. Low alloy steel containing chromium (Cr >0.5%) may be used.

3.70. Insulation materials should be chosen in such a way as to minimize adverse effects from their use (e.g. doses to personnel during outages, sump clogging in accidents). The sump clogging behaviour of the debris generated from the insulation materials during accidents by jet forces should be tested for the insulation materials selected.

3.71. The choice of materials used in a radiation environment should take into consideration the effect of radiation on material properties. For example, optical fibres may be damaged when exposed to neutron fields. This would have an adverse effect on the safety function of all systems served by such cables (usually computer based control and protection systems).

3.72. Because of radiation activation, the choice of materials used in a radiation environment could have a significant effect on decommissioning during service. These aspects should be evaluated at the design stage.

SINGLE FAILURE ASSESSMENT AND REDUNDANCY/INDEPENDENCE

3.73. The application of the single failure criterion, as expressed in Ref. [1] and further explained in IAEA Safety Series No. 50-P-1, Application of the Single Failure

Criterion [7], ensures that the safety functions required after a PIE[9] considered within the design basis are performed and the limits specified in the design basis for that event are not exceeded, assuming a single failure in any one component of the safety group[10].

3.74. In the application of the single failure criterion, any failure which could occur as a consequence of the PIE should be identified and included in the starting point for the single failure analysis.

3.75. The safety group which carries out the required set of safety functions should be identified for each of the PIEs identified for the plant. The single failure analysis should identify all the failure modes of the components in the safety group, including all the needed support systems. In addition, all the failures which could occur as a consequence of the single failure should be identified and included in the analysis along with the single failure. This should include failures of a component which would occur due to failure of a support system such as electrical power or cooling water. However, at no time during the single failure analysis should more than one random failure be assumed to occur.

3.76. The single failure criterion should be applied during the worst possible configuration of the safety group. In particular, where the operation of the plant allows equipment to be taken out of service for a considerable length of time for maintenance, testing, inspection or repair at a time when the safety group would need to be available, the single failure should be assumed to occur at a time when the maximum outage of equipment allowed by the operating rules or technical specifications of the plant had occurred. Nonetheless, as stated in Ref. [1] para. 5.38, non-compliance with the single failure criterion may be justified for outages which are of a specified limited duration. A justification should be given for all such cases, in conjunction with the derivation of the allowed outage times (see para. 5.42 of Ref. [1]).

3.77. The failures which should be considered in the single failure analysis would typically include those of active components (such as failure of valves to open or

---

[9] For the definition and a more detailed explanation of PIEs, refer to the Annex in IAEA Safety Standards Series No. NS-R-1, Safety of Nuclear Power Plants: Design.

[10] 'Safety group' is defined as: "The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded."

close on demand and failure of pumps to start and run) and those of passive components (such as failure of safety system piping) which have a wide range of probabilities of occurrence. In the single failure analysis, the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality level may not need to be assumed, provided it remains unaffected by the PIE. However, justification should be provided for each component failure mode which is omitted from the single failure analysis. For a passive component, this should take into account the total period of time after the occurrence of the PIE for which the component is expected to operate. In practice, single failures of passive components are often considered only in the long term (e.g. 24 hours) after the occurrence of a PIE owing to the quality standards applied.

3.78. The single failure analysis may not need to address PIEs with a very low frequency of occurrence or take account of consequences of the PIE that would be very unlikely to occur.

3.79. The Safety Requirements publication on Safety of Nuclear Power Plants: Design [1] specifies that the following safety functions should be performed by associated plant systems on the assumption of a single failure:

— Fast reactor shutdown,
— Residual heat removal from the core,
— Emergency core cooling,
— Containment isolation,
— Containment heat removal,
— Containment atmosphere control and cleanup.

3.80. In practice, higher levels of redundancy than those derived from the single failure criterion may be provided to achieve sufficiently high reliability or for operational reasons; for example (i) to allow equipment to be removed from service for maintenance or for repairs to be carried out at a time when the safety group needs to be available; (ii) to allow for surveillance testing; or (iii) to reduce problems in the layout of the plant. This means that a PIE itself is not an accident. It is only the event that initiates a sequence that leads to an operational occurrence, a design basis accident or a severe accident, depending on the additional failures that occur. Typical examples are: equipment failures (including pipe breaks), human errors, human induced events and natural events. Connections between trains should be designed in such a way that a single failure cannot lead to the loss of more than one train. Redundant trains should be separated by barriers or distance in order to ensure that an internal hazard cannot lead to the loss of more than one train.

DIVERSITY

3.81. The reliability of a safety system which incorporates redundancy by use of similar components will be limited by common cause failure, which can lead to the simultaneous failure of a number of redundant components. To prevent such a limitation, reliability can be increased by the incorporation of diversity (see Appendix II of Ref. [1]).

3.82. The level of diversity provided can be different depending on the design solution implemented. It is high if the diverse systems carry out the same safety function in ways that are physically different and use different types of equipment. For example, a reactor shutdown where the diverse systems involve dropping solid neutron absorber into the reactor core and injecting a solution of neutron absorber into the primary coolant. However, it is lower if the diverse systems carry out the safety function in the same way using components of a different type. For example, an emergency feedwater system where the pumps and valves in the diverse parts of the system are of a different type or are provided by a different manufacturer.

3.83. Where very high reliability is required, a diversified means of carrying out the safety function should be incorporated. The level of diversity should be commensurate with the required reliability of the means to perform the safety function.

3.84. Where diversity is provided within safety systems, compliance with the required system reliability should be demonstrated. For this purpose, potential common vulnerabilities like common cause failures should be adequately addressed. For example, these can be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human induced event, or an unintended cascading effect from any other operation or failure within the plant.

3.85. It should be recognized that the provision of diversity increases the complexity and costs of the plant and introduces difficulties and costs in its operation and maintenance. This should be addressed in the design process and a balance should be struck between the gains in the reliability of the safety systems and the additional complexity achieved.

IN-SERVICE TESTING, MAINTENANCE, REPAIR,
INSPECTIONS AND MONITORING OF ITEMS IMPORTANT TO SAFETY

3.86. Those SSCs important to safety should, except as provided for below, be designed to be tested, maintained, repaired and inspected or monitored periodically

in terms of their integrity and functional capability during the life of the nuclear power plant. The period may vary from days to years, depending on the nature of the item. Clearly, the more frequently maintenance is performed while the plant is on load, the less will be the need for maintenance during plant outage. The design should be such that these activities can be performed to standards commensurate with the importance of the safety functions to be performed, without undue exposure to radiation of the site personnel.

3.87. If the SSCs important to safety cannot be designed to be tested, inspected or monitored to the extent desirable, adequate safety precautions should be taken to compensate for potential undiscovered failures.

3.88. Designers should prepare specific design guides intended to guarantee accessibility for inspection and testing. In this connection, key issues which should be assessed include: availability of sufficient space around components; reduction of radiation fields around components by reduction of the deposition of radioactive material inside the primary pressure boundary or shielding; reduction of primary water leaks; provision of permanent or removable access gangways and of hang-points on structures for the movement of components; and installation of components in a convenient position to facilitate inspection and testing.

3.89. Where accessibility is impracticable, permanent rails and adequate space can be provided by design which allow inspection equipment to be properly positioned and operated by remote actuation devices. Safety assessment should ascertain that such possibilities have been considered.

3.90. Although the implementation of provisions such as those outlined above tend to resolve, in most cases, the conflict between the need for keeping operational doses small and the need for periodic tests and inspections, in some complex situations an accurate study of the correct trade-off between the two needs should be done, using the safety analysis at the design level.

EQUIPMENT QUALIFICATION

3.91. Equipment qualification applies mainly to safety systems which are required to perform safety functions in accident conditions.

3.92. The conditions under which equipment is expected to perform a safety function may differ from those to which it is normally exposed and its performance may be affected by ageing or service conditions as plant operation goes on. The

environmental conditions under which equipment is expected to function should be identified as part of the design process. Among these should be the conditions expected in a wide range of accidents, including extremes of temperature, pressure, radiation, vibration and humidity, and jet impingement.

3.93. The required functional capability should be maintained throughout the plant's life. Attention should be given during design to the common cause failure effects of ageing. Ageing should be taken account of in the design by the appropriate definition of environmental conditions, process conditions, duty cycles, maintenance schedules, service life, type testing schedules, replacement parts and replacement intervals.

3.94. A qualification procedure should confirm that the equipment is capable of performing, throughout its operational life, its safety functions while being subjected to the environmental conditions (dynamic effects, temperature, pressure, jet impingement, radiation, humidity) existing at the time of need. These environmental conditions should include the variations expected during normal operation, anticipated operational occurrences and accident conditions. Where the equipment is subject to external natural events and is expected to perform a safety function during or following such an event, the qualification programme should replicate the conditions imposed on the equipment by the natural phenomena.

3.95. In addition, any unusual environmental conditions that can be reasonably anticipated and could arise from specific operating conditions, such as during periodic containment leak rate testing, should be included in the qualification programme. To the extent possible, equipment that is expected to operate during severe accidents should, by tests, experiments or engineering analysis, be shown with reasonable confidence to be capable of achieving the design intent under severe accident conditions.

3.96. It is preferable that qualification be achieved by the testing of prototypical equipment (type testing). This is not always fully practicable for the vibration of large components or the ageing of equipment. In such cases extrapolation of equipment performance under similar conditions, analyses or tests plus analyses should be relied upon.

AGEING AND WEAR-OUT MECHANISMS

3.97. The safety assessment should take into account the fact that plant systems and components are affected in varying measure by ageing effects. Some effects of this kind are well known and provisions can be taken to cope with them. Others, by

experience, are not foreseeable and suitable testing, inspection and surveillance programmes should be employed in order to detect their possible occurrence. A complete programme of actions during the plant lifetime should be drawn up and technical prerequisites for its implementation established at the design stage. Periodic safety reviews are a good way of determining whether ageing and wear-out mechanisms have been correctly taken into account, and to detect unpredicted issues.

3.98. The vessel should be designed taking into consideration the embrittlement due to the action of the fast neutron flux from the core for the full life of the plant. Protection resides in good design for preventing excessive embrittlement, for facilitating embrittlement detection and possible remedial actions. Pressurized water reactors (PWRs) are more affected than boiling water reactors (BWRs) by this problem owing to dimensional and/or neutronic effects. Weld areas are more easily affected by embrittlement, as impurities introduced in the welding process may render the weld zone particularly sensitive to neutron irradiation. The heat affected zone (HAZ) around a weld is frequently the region where microcracks and residual stresses accumulate, making the region even more sensitive to the effects of embrittlement.

3.99. The presence of welds at the level of the active fuel region should be avoided to the extent practicable.

3.100. Appropriate consideration should be given to limiting and monitoring vessel embrittlement. For this purpose, neutron fluence (neutron flux integrated over the plant lifetime) should be kept below a level that ensures that adequate mechanical properties are maintained, with uncertainties taken into account. The presence of adequate surveillance programmes using vessel weld samples and neutron fluence measurement devices exposed to neutron flux in representative conditions should be ensured. Another major ageing process affects steam generator tubing of PWRs. Tube degradation occurs for a variety of reasons and should be monitored in order to permit preventive and remedial actions such as water chemistry changes and tube repairs or plugging prior to leakage or failure. The design should facilitate steam generator surveillance, repair and replacement through adequate clearances, rails and attachment points.

3.101. Other possible ageing effects indicated by past operating experience are listed below. The design of the plant should eliminate the problems during the design stage or include means for timely detection of their inception and for implementing the appropriate corrective actions:

— Channel hydriding and embrittlement in pressure channel reactors, which may lead to channel replacement;

— Corrosion of vessel internals, vibration and failure, the possibility of which should be detectable by suitable surveillance means;
— Cracking of core nozzles and reactor internals;
— Thermal and pressure transients in nozzles and piping;
— Thermal mixing in pipe joint areas;
— Thermal stratification in piping and other piping erosion in components, which should be detectable by periodic inspections, facilitated by suitable design provisions;
— Ageing of organic cable insulation or ventilation sealing materials, which should be taken into account in the design to permit detection and possible replacement.

HUMAN–MACHINE INTERFACE AND THE APPLICATION OF HUMAN FACTOR ENGINEERING

3.102. Detailed recommendations on the application of human factors principles in design are given in specific IAEA Safety Guides[11]. Some key issues are summarized in the present section.

3.103. The plant design should facilitate the job of the operators and promote optimum human performance during operational states and accidents. This should be done by paying careful attention to the design of the plant, the provision of operating procedures and the training of all operating staff.

3.104. Systematic consideration of human factors and the human–machine interface should be included in the design process at an early stage of design development and should continue throughout the entire process.

3.105. Safety actions which are assigned to the operating staff should be identified. This would include safety actions carried out by operators with responsibilities for monitoring and controlling the plant and for responding to faults and maintenance, testing and calibration activities.

3.106. Task analysis should be performed for the safety actions, to assess the demands that will be placed on the operators in terms of decision making and

[11] Safety Series Nos 50-SG-D3, Protection System and Related Features in Nuclear Power Plants (1986); 50-SG-D8, Safety-related Instrumentation and Control Systems for Nuclear Power Plants (1984); and Safety Standards Series No. NS-G-2.2, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants (2000).

carrying out the actions. The results of the task analysis should determine the design specifications of the human–machine interface, the information and controls that need to be provided, the preparation of the operating procedures, and the training programmes.

3.107. The information and controls provided should be sufficient to allow the operators to:

— Carry out normal operations such as changing the power level of the reactor;
— Assess readily the general state of the plant in normal operation, anticipated operational occurrences and accident conditions;
— Monitor the state of the reactor and the status of all plant equipment;
— Identify changes in the state of the plant which are important to safety;
— Confirm that the designed automatic safety actions are being carried out;
— Identify any actions prescribed and carry them out.

3.108. The operator should be provided with sufficient information on the parameters associated with individual plant systems and equipment to confirm that the required safety actions have been achieved and to provide feedback that the actions have had the desired effect.

3.109. The working areas and working environment of the site personnel should be designed according to ergonomic principles to enable the tasks to be performed reliably and efficiently. This should include the design of the central control room, the emergency control room, any local control stations in the plant and any areas where maintenance and testing would be carried out. Particular attention should be paid to display systems, panel layouts and workspace access for maintenance and testing operations.

3.110. The human–machine interface should be designed to provide the operators with comprehensive but easily manageable information for taking correct decisions and actions.

3.111. The need for operator intervention on a short time-scale should be kept to a minimum. Automation should be provided for all those actions that are needed within a short time. The time allowance should be evaluated on a justifiable best estimate basis.

3.112. For all operator actions, the task analysis should demonstrate that the operator has sufficient time to decide and to act, that the information necessary for the decision is simply and unambiguously presented, and that the physical environment

following the event is acceptable in the control room or at the supplementary control point and the access to that control point.

3.113. The design of the plant should be tolerant of human error. To the extent practicable, any inappropriate human actions should be rendered ineffective. For this purpose, the priority between operator action and safety system actuation should be carefully chosen. On the one hand, the operator should not be allowed to override reactor protection system actuation as long as the initiation criteria for actuation apply. On the other hand, there are situations where operator interventions into the protection system are necessary. Examples are manual bypasses for testing purposes or for adoption of actuation criteria for modifications to the operational state. Furthermore, the operator should have an ultimate possibility, under strict administrative control, to intervene in the protection system for the purposes of managing beyond design basis accidents in the event of major failures within the reactor protection system.

3.114. Written procedures should be provided for all activities carried out by the operating staff, including normal operation of the plant and recovery from abnormal occurrences and accidents, including severe accidents. Procedures for response to abnormal occurrences and accidents should preferably be symptom oriented. The procedures should be validated by walk-throughs and the use of mock-ups and simulators where appropriate.

3.115. Sufficient and reliable means of communication should be provided to enable information and instructions to be transmitted between locations to support the operator actions during normal operation and recovery following accidents. This would include communications between the main or emergency control rooms and operating personnel at remote locations who may have to take actions affecting the state of the plant, and with off-site organizations in accident situations. The means of communication should be available under all relevant accident conditions and should not interfere with the plant protection system.

3.116. The layout and identification of remotely located controls should be designed bearing in mind human factors, such as to reduce the chance of operator error in selecting the remotely located controls.

SYSTEM INTERACTIONS

3.117. Possible interactions between systems of the same plant, between plant and outside utilities and between different plants on the same site should be carefully

assessed. System interactions should be considered for all plant operating states including external hazards and severe accidents.

3.118. The analysis should take into account not only physical interconnections but also the effect of system operation, maintenance, malfunction or failure on the physical environment of other systems important to safety. Changes in the environment could affect the reliability of systems to function as intended. Examples of failures that could adversely affect the performance of other systems are failures of air conditioning for electronic equipment or failures of fluid systems causing flooding or high humidity in areas containing safety system equipment.

3.119. In the safety assessment of the design, consideration should be given to grid–plant interactions in relation to the required reliability of the power supply to the plant systems important to safety as discussed in detail in a specific IAEA Safety Guide.[12]

3.120. Structures, systems and components important to safety should not be shared between two or more nuclear power reactors. However, if this is done, it should be demonstrated by test, experiments or engineering analysis that all safety requirements can be met for all reactors in all states. In the event of accident conditions involving one of the reactors, an orderly shutdown and decay heat removal of the other reactors should be achievable. Special consideration should be given to external events which could cause accidents in more than one plant. Common support systems should be able to cope with all the affected reactors.

3.121. Other design and operating interfaces that should be checked in the safety assessment include the technical specifications and the operating procedures.

USE OF COMPUTATIONAL AIDS IN THE DESIGN PROCESS

3.122. Engineering design uses a large number of software tools, such as diagrams, monograms, formulas, algorithms and computer codes (neutronics, fluid dynamics, structural analysis, etc.). These tools, as well as the numerical models used in these tools, should be subject to adequate QA procedures, including their verification and validation along the lines of those described for computer codes in Section 4 (paras 4.236–4.244).

---

[12] Safety Series No. 50-SG-D7, Emergency Electrical Power Systems at Nuclear Power Plants (1991).

3.123. All numerical models should show their reliability through comparisons, independent analyses and qualification, with the aim of guaranteeing that their intrinsic uncertainty level complies with the reliability required for the whole design project.

4. SAFETY ANALYSIS

GENERAL GUIDANCE

4.1. The aim of the safety analysis should be by means of appropriate analytical tools to establish and confirm the design basis for the items important to safety, and to ensure that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category. The design, manufacture, construction and commissioning should be integrated with the safety analysis to ensure that the design intent has been incorporated into the as-built plant.

4.2. As part of the design process, the safety analysis should be carried out by the two organizations that have a role in the provision of safe nuclear power. These are:

— The *designer*, who uses the safety analysis as an important and integral part of the design process. This is continued through the manufacture and construction of the plant.
— The *operating organization*, which uses the safety analysis to ensure that the as-built design will perform as expected in operation, and to demonstrate that the design meets the safety requirements at any point in the plant's design life.

4.3. The safety analysis, part of the safety assessment used in plant licensing, should proceed in parallel with the design process, with iteration between the two activities. The scope and level of detail of the safety analysis should increase as the design programme progresses so that the final safety analysis reflects the final plant design as constructed.

4.4. The recommendations for carrying out a safety analysis during the design process can also be used as guidance for a periodic safety analysis of an operating plant or for the safety justification of a proposed design modification. The requirements for periodic assessments are covered under the IAEA Safety Requirements for Operation and supporting Safety Guides.

4.5. The plant design models and data (which are essential foundations for the safety analysis) should be kept up to date during the design phase and throughout the lifetime of the plant, including decommissioning. This should be the responsibility of the designer during the design phase and of the operating organization over the life of the plant.

4.6. The updating process should incorporate new information as it becomes available, address new issues as they arise, use more sophisticated tools and methods as they become accessible, and assess the performance of modifications to the design and operating procedures that might be considered over the life of the plant.

4.7. The assessment of engineering aspects important to safety described in Section 3 and the safety analysis described in the present section should be carried out in parallel.

Objectives of the safety analysis

4.8. The safety analysis should assess the performance of the plant against a broad range of operating conditions, PIEs and other circumstances (many of which may never be observed in actual plant operation), in order to obtain a complete understanding of how the plant is expected to perform in these situations. The safety analysis should also demonstrate that the plant can be kept within the safe operating regimes established by the designer.

4.9. The safety analysis should formally assess the performance of the plant under various operational and accident conditions, against goals or criteria for safety and radiological releases as may have been established by the operating organization, the regulatory body, or other national or international authorities, as applicable to the plant.

4.10. The safety analysis should identify potential weaknesses in the design, evaluate proposed design improvements and provide a demonstration that safety requirements are met and the risk from the plant is acceptably low. This should involve a comparison with risk criteria where they have been defined.

4.11. The safety analysis should support safe operation of the plant by serving as an important tool in developing and confirming plant protection and control system set points and control parameters. It should also be used to establish and validate the plant's operating specifications and limits, normal and off-normal operating procedures, maintenance and inspection requirements, and normal and emergency procedures.

4.12. The safety analysis should also support the plant management and regulatory body's decision making processes as new issues and questions arise during the life of the plant. The plant's initial safety analysis and the ability to re-perform all or part of that analysis to resolve new technical issues should be maintained over the life of the plant. This implies that the plant's actual, up to date design information and operating performance data should be factored into the plant model as necessary to support this analysis process.

4.13. The safety analysis should assist in revealing issues, plant conditions and initiating events that were not adequately considered in the early stages of design. Likewise, safety analysis can identify aspects, such as PIEs or established acceptance criteria, that are not needed (that is, on closer examination, they do not impact or contribute to the safety of the plant, because of extremely low frequency of occurrence, insignificant conditional probability or minimal impact of potential consequences).

4.14. The safety analysis should assess whether:

— Sufficient defence in depth has been provided and the levels of defence are preserved in that potential accident sequences are arrested as early as possible.
— The plant can withstand the physical and environmental conditions it would experience. This would include extremes of environmental and other conditions.
— Human factors and human performance issues have been adequately addressed.
— Long term ageing mechanisms that could detract from the plant's reliability over the plant life are identified, monitored and managed (i.e. by upgrade, refurbishment or replacement) so that safety is not affected and risk does not increase.

4.15. The safety analysis should demonstrate by test, assessment, calculation or engineering analysis that the equipment incorporated to prevent escalation of anticipated operational occurrences or design basis accidents to severe accidents and to mitigate their effects, as well as emergency operating procedures and the accident management measures, is effective in reducing risk to acceptable levels.

4.16. The safety analysis process should be highly credible, with sufficient scope, quality, completeness and accuracy to engender the confidence of the designer, the regulator, the operating organization and the public in the safety of a plant's design. The results of the safety analysis will ensure with a high level of confidence that the plant will perform as designed and that it will meet all design acceptance criteria at commissioning and over the life of the plant.

Deterministic and probabilistic assessments

4.17. The achievement of a high level of safety should be demonstrated primarily in a deterministic way. However, the safety analysis should incorporate both deterministic and probabilistic approaches. These approaches have been shown to complement each other and both should be used in the decision making process on the safety and ability of the plant to be licensed. The probabilistic approach provides insights into plant performance, defence in depth and risk that are not available in the deterministic approach.

4.18. The aim of the deterministic approach should be to address plant behaviour under specific predetermined operational states and accident conditions and to apply a specific set of rules in judging design adequacy.

4.19. In general, the deterministic analysis for design purposes should be conservative. The analysis of beyond design basis accidents is generally less conservative than that of design basis accidents.

4.20. The PSA should set out to determine all significant contributors to risk from the plant and should evaluate the extent to which the design of the overall system configuration is well balanced, there are no risk outliers and the design meets basic probabilistic targets. The PSA should preferably use a best estimate approach.

4.21. The insights gained from the deterministic analysis and the PSA should both be used in the decision making process. In general, it is usually found that these insights are consistent. In particular, where weaknesses are identified in the design or operation of the plant, this usually relates to a low level of redundancy or diversity in the safety systems provided to perform one or more of the safety functions.

4.22. There are situations where the insights gained from the deterministic analysis and the PSA are not consistent. These should be considered on a case by case basis.

Essential information

4.23. The safety analysis process should be based on plant design information that is complete and accurate. This information should cover all plant SSCs, off-site interfaces and site specific characteristics.

4.24. The plant design should be documented and kept up to date with the approved, as-built and as-modified plant design.

4.25. For an operating plant, the safety analysis (used, for example, for design modifications) should use plant specific operational data. This includes information on the radiological doses to operators during normal operation and routine discharges of radioactive material from the site. For plant systems, data collected should include normal operating temperatures, pressures, fluid levels and flow rates, and the transient response characteristics and timing for any operational occurrences.

4.26. The operational data should also include information on component and system performance, initiating event frequencies, component failure rate data, modes of failure, system unavailability during maintenance or testing, and component and system repair times.

4.27. For a plant in the design phase, the data used should be derived from generic data from operating plants of similar design, or from research or test results. For an operating plant, some aspects of this generic database can be enhanced over time with plant specific data from the plant's own historical operating and maintenance data and experience and inspection results.

4.28. The safety analysis should cover all the sources of radioactive material in the plant. In addition to the reactor core, this includes irradiated fuel in transit, irradiated fuel in storage and stored radioactive waste.

Acceptance criteria for safety analysis

4.29. The acceptance criteria should be defined for the deterministic assessment and the PSA. These normally reflect the criteria used by the designers or operators and are consistent with the requirements of the regulatory body.

4.30. The criteria should be sufficient to meet the General Nuclear Safety Objective, the Radiation Protection Objective and the Technical Safety Objective as given in the IAEA Safety Fundamentals [2] and Safety of Nuclear Power Plants: Design [1].

4.31. In addition, detailed criteria should be developed to help ensure that these higher level objectives are met (see paras 4.98 and 4.103 below). This will usually simplify the analysis.

4.32. Probabilistic safety criteria should be addressed where they have been specified in law or as regulatory requirements, or they should be developed where applicable. These should relate to the likelihood of accidents occurring with significant radiological consequences such as core damage, large off-site releases, and radiation doses to workers and members of the public, as appropriate.

Identification of PIEs

4.33. The starting point for the safety analysis is the set of PIEs that need to be addressed. A PIE is defined in Ref. [1] as an "identified event that leads to anticipated operational occurrences or accident conditions". PIEs include events such as equipment failure, human errors and human induced or natural events. The deterministic safety analysis and the PSA should normally use a common set of PIEs.

4.34. The set of PIEs developed for the safety analysis should be comprehensive and should be defined in such a way that they cover all credible failures of plant systems and components and human errors which could occur during any of the operating regimes of the plant (such as startup, shutdown and refuelling). This should include both internally and externally initiated events.

4.35. The set of PIEs should be identified in a systematic way. This should include adopting a structured approach to the identification of the PIEs which could include the following:

— Use of analytical methods such as hazard and operability analysis (HAZOP)[13], failure mode, effect analysis (FMEA)[14], and master logic diagrams;
— Comparison with the list of PIEs developed for safety analysis of similar plants (although this method should not be exclusively used since prior mistakes could be propagated);
— Analysis of operating experience data for similar plants.

4.36. The set of PIEs addressed should also include partial failures of equipment if these can make a significant contribution to the risk.

[13] HAZOP is a systematic process which uses a set of key words to identify the failures which could occur and could lead to PIEs.

[14] FMEA is a systematic process which considers each of the component failure modes in turn to determine if they could lead to a PIE (see Appendix V of Ref. [10]).

4.37. The set of PIEs should be reviewed as the design and safety assessments proceed and should involve an iterative process between these two activities.

4.38. The set of PIEs should also include events of very low frequency or consequences, at least at the beginning of the process. It may be possible to eliminate some PIEs. Nevertheless, the elimination of any PIEs should be fully justified and the reasons well documented. Many PIEs will remain with the analysis to the end and will only be determined to be insignificant only at the conclusion of the process.

4.39. All the PIEs should be defined quantitatively in terms of their frequency of occurrence. While the frequency of occurrence should be defined quantitatively for PSA applications, it is used qualitatively in the deterministic analysis.

Internal PIEs

4.40. The internal PIEs (those initiated inside the plant) should be developed to identify possible challenges to the fundamental safety function. The way that the safety functions are performed depends on the detailed design of the reactor. However, the categories of initiating events identified typically include the following:

— Increase or decrease in heat removal from the reactor coolant system,
— Increase or decrease in reactor coolant system flow rate,
— Reactivity and power distribution anomalies,
— Increase or decrease in reactor coolant inventory,
— Release of radioactive material from a subsystem or component.

4.41. The identification of the set of internal PIEs should also consider the various means of failure of safety systems and components and failures of non-safety systems and components that could impact a fundamental safety function or safety system. Most of these failures can be assigned to one of the above categories. However, some of these failure based PIEs do not fit in the above categories and are grouped separately. Examples of these other failures determined by PSAs performed to date include: (a) support system failures such as loss of component cooling or service water; (b) internal flooding due to failure of circulating water, service water, fire protection or elevated surge tanks; (c) false containment isolation signals resulting in loss of primary system pump cooling; and (d) inadvertent actuation of relief valves.

4.42. The identification process for the set of internal PIEs should also address the various failure modes of the reactor pressure retaining boundary. This should include

pipe breaks in all possible locations, including those which could occur outside the containment.

4.43. The internal PIEs should include the failure modes which could occur during all modes of plant operation (for example, reactivity transients during initial core criticality and loss of coolant inventory during the refuelling mode with the containment open), excluding those with negligible duration in time. Negligible duration modes should only be excluded after careful consideration and a conservative analysis that demonstrates that they are unimportant when compared with the calculated core damage frequency from other PIEs.

4.44. The set of PIEs should include those which could occur as a consequence of human errors. This could range from faulty or incomplete maintenance operations to incorrect settings of control equipment limits or wrong operator actions. These PIEs will not necessarily be similar to PIEs caused by equipment failures because they could involve common cause failures in addition to the initiating event.

4.45. The set of internal PIEs should include events such as fires, explosions, turbine missile impacts and floods of internal origin which could affect the safety of the reactor and cause failure of some of the safety system equipment which provides protection for that initiating event. These PIEs have already been discussed in Section 3.

External PIEs

4.46. The set of PIEs identified should include all the events which could arise from outside the plant which could challenge nuclear safety, including naturally occurring and human induced events. These external initiating events could lead to an internal initiating event and failure of some of the safety system equipment that would be needed to provide protection from the event. For example, an earthquake could lead to plant equipment failures in addition to the loss of off-site power.

4.47. The naturally occurring events which are credible at a given site should be included in the set of PIEs for safety analysis. This should include events such as earthquakes, fires and floods (including those caused by failure of dams, dikes or levees) occurring outside the site, extreme weather conditions (temperature, rainfall, snow, high winds) and volcanic eruptions.

4.48. The human induced external events which are credible at a given site should be included in the set of PIEs for safety analysis. This should include aircraft crashes, effects of nearby industrial plant and transportation system explosions.

4.49. Detailed recommendations for external events can be found in the IAEA Safety Requirements for siting[15] and supporting Safety Guides.

DETERMINISTIC SAFETY ANALYSIS[16]

Normal operation

4.50. The aims of the safety analysis for normal operation should be to assess that:

— Normal operation of the plant can be carried out safely,

hence confirming that:

— Radiological doses to workers and members of the public are within acceptable limits,
— Planned releases of radioactive material from the plant are within acceptable limits.

4.51. The safety analysis for normal operation should address all the plant conditions under which systems and equipment are being operated as expected, with no internal or external challenges. This includes all the phases of operation for which the plant was designed to operate in the course of normal operations and maintenance over the life of the plant, both at power and shut down.

4.52. The normal operation of a nuclear power plant typically includes the following conditions:

— Initial approach to reactor criticality;
— Normal reactor startup from shutdown through criticality to power;
— Power operation including both full and low power;
— Changes in the reactor power level including load follow modes if employed;
— Reactor shutdown from power operation;

---

[15] Safety Series No. 50-C-S (Rev. 1), Code on the Safety of Nuclear Power Plants: Siting (1988).

[16] Further information can be found in an IAEA Safety Reports Series publication entitled Accident Analysis for Nuclear Power Plants (in preparation).

— Shutdown in a hot standby mode;
— Shutdown in a cold shutdown mode;
— Shutdown in a refuelling mode or equivalent maintenance mode that opens major closures in the reactor coolant pressure boundary;
— Shutdown in other modes or plant configurations with unique temperature, pressure or coolant inventory conditions;
— Handling and storage of fresh and irradiated fuel.

4.53. The safety analysis should assess whether normal operation of the plant can be carried out safely in such a way that plant parameter values do not exceed operating limits.

4.54. The safety analysis should establish the conditions and limitations for safe operation. This would include items such as:

— Safety limits for reactor protection and control and other engineered safety systems,
— Operational limits and reference settings for the control system,
— Procedural constraints for operational control of processes,
— Identification of the allowable operating configurations.

More detailed information is given in Ref. [8].

4.55. The safety assessment of design in normal operation should verify that a reactor trip or initiation of the safety systems would occur only when required. Spurious trips or initiation of safety systems are generally detrimental to safety.

Radiological doses to workers and members of the public from normal operation

4.56. The safety analysis for normal operation should include an analysis of the overall design and operation of the plant to: predict the radiation doses likely to be received by workers and members of the public; assess that these doses are within acceptable limits; and ensure that the principle that these doses should be as low as reasonably achievable has been satisfied.

4.57. For workers on the site, the dose predictions should be based on the specific operations involved in the running and servicing of the plant. The dose predictions should include the contributions from direct radiation and from the intake of radioactive material. The analysis should take account of the duration, frequency and numbers of people involved in each of the activities. Estimates should be made of both the highest individual dose and the annual group average dose.

4.58. For members of the public, the dose predictions should include the contributions from direct radiation, intake of radioactive material and doses received through the food chain as a result of discharges of radioactive material from the plant. The doses should be estimated for the critical group.

4.59. When there are uncertainties in making the dose predictions, conservative assumptions should be made.

4.60. When the dose predictions depend on the dose rates arising from the buildup in the level of the inventories of radioactive material or from the level of contamination, the prediction should be based on the maximum values that are likely to occur during the lifetime of the plant.

4.61. The dose predictions should take account of any relevant operating experience data. This could be derived from the operation of the actual plant or similar plants.

4.62. These dose estimates should be compared with the radiological criteria developed for the plant. This should include dose limits which are legal requirements or requirements of the regulator and should take account of the current recommendations of the International Commission on Radiological Protection (ICRP).

4.63. The results of these dose estimates should be assessed to identify any weakness in the design or system of operation of the plant; improvements should be made where reasonably achievable.

Planned releases of radioactive material from the plant

4.64. The safety analysis for normal operation should include an estimate of the plant's planned releases of radioactive material.

4.65. These estimates of the planned releases of radioactive material should be compared with the radiological criteria developed for the plant, including any legal requirements or requirements of the regulator, and reviewed against ALARA principles. The design and operation of the plant should be assessed and improvements made when improvements are reasonably practicable in order to reduce the planned releases.

Anticipated operational occurrences and design basis accidents

4.66. The plant conditions considered in the design basis analysis include anticipated operational occurrences and design basis accidents (DBAs). The division is based on the frequency of the occurrence.

4.67. Anticipated operational occurrences are those events that are more complex than the manoeuvres which are carried out during normal operation and that have the potential to challenge the safety of the reactor. These occurrences might be expected to occur at least once during the lifetime of the plant. Generally they have a frequency of occurrence greater than 10^{-2} per reactor-year.

4.68. Design basis accidents have a lower frequency than anticipated operational occurrences. They would not be expected to occur during the lifetime of the plant but, in accordance with the principle of defence in depth, they have been considered in the design of the nuclear power plant. The DBAs have a frequency of occurrence in the range of 10^{-2} to 10^{-5} per reactor-year, although there are some groups of PIEs that are traditionally included in the design basis analysis that may have lower frequencies.

4.69. The aim of the design basis analysis should be to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety systems. This is done by carrying out a conservative analysis which should take account of the uncertainties in the modelling.

Postulated initiating events leading to anticipated operational occurrences

4.70. For many PIEs the control systems will compensate for the effects of the event without a reactor trip or other demand being place on the safety systems (Level 2 of defence in depth). However, the anticipated operational occurrences category should include all the PIEs which might be expected to occur during the lifetime of the plant and for which operation can resume after rectification of the fault.

4.71. Typical examples of PIEs leading to anticipated operational occurrences could include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and the actual design of the plant systems:

— *Increase in reactor heat removal:* inadvertent opening of steam relief valves; secondary pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate.
— *Decrease in reactor heat removal:* feedwater pump trips; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, turbine trip, loss of external load, loss of power, loss of condenser vacuum).
— *Decrease in reactor coolant system flow rate:* trip of one main coolant pump; inadvertent isolation of one main coolant system loop (if applicable).
— *Reactivity and power distribution anomalies:* inadvertent control rod withdrawal; boron dilution due to a malfunction in the volume control system (for a PWR); wrong positioning of a fuel assembly.

— *Increase in reactor coolant inventory:* malfunctions of the chemical and volume control system.
— *Decrease in reactor coolant inventory:* very small loss of coolant accident (LOCA) due to the failure of an instrument line.
— *Release of radioactive material from a subsystem or component:* minor leakage from a radioactive waste system.

Postulated initiating events leading to DBAs

4.72. The subset of PIEs which are considered as leading to DBAs should be identified. All the PIEs identified as initiators of anticipated operational occurrences should also be considered potential initiators for DBAs. Although it is not usual to include PIEs with a very low frequency of occurrence, the establishment of any threshold limit should consider the safety targets established for the specific reactor.

4.73. Typical examples of PIEs leading to DBAs could include those given below. This list is broadly indicative. The actual list will depend on the type of reactor and actual design:

— Increase in reactor heat removal: steam line breaks.
— Decrease in reactor heat removal: feedwater line breaks.
— Decrease in reactor coolant system flow rate: trip of all main coolant pumps; main coolant pump seizure or shaft break.
— Reactivity and power distribution anomalies: uncontrolled control rod withdrawal; control rod ejection; boron dilution due to the startup of an inactive loop (for a PWR).
— Increase in reactor coolant inventory: inadvertent operation of emergency core cooling.
— Decrease in reactor coolant inventory: a spectrum of possible LOCAs; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system.
— Release of radioactive material from a subsystem or component: overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system.

4.74. It should be noted that some of the accident initiators that have been treated historically as DBAs may have a frequency that is lower than 10^{-5} per year. This may be the case for PIEs such as a large break LOCA for plants designed and built to modern standards. The regulatory rules, however, may still request that such PIEs be considered in the category of DBAs.

Grouping

4.75. A large number of PIEs will be identified by following the guidance provided above. It is not necessary to analyse all of these PIEs. The normal practice is to group them and, for each group, to choose bounding cases for analysis.

4.76. The bounding cases should identify the accidents which give the most severe challenges to each of the main safety functions identified. In some cases, one accident may be most severe in terms of one safety parameter (for example, peak reactor coolant system pressure) and another may be most severe in terms of another safety parameter (for example, peak fuel temperature). In such cases, all these accident sequences are carried through the design process as limiting cases.

4.77. The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.

Objectives of anticipated operational occurrences and DBA analysis

4.78. The safety analysis of anticipated operational occurrences and DBAs should demonstrate that the safety systems are able to fulfil the safety requirements in that they can:

— Shut down the reactor and maintain it in the safe shutdown condition during and after DBA conditions.
— Remove residual heat from the core after reactor shutdown from all operational states and all DBA conditions.
— Reduce the potential for the release of radioactive material and ensure that any releases are below prescribed limits during operational states and below acceptable limits during DBA conditions.

4.79. The safety analysis should show that plant and radiological limits are not exceeded. In particular, it should be demonstrated that some or all of the barriers to the release of radioactive material from the plant will maintain their integrity to the extent required.

4.80. The safety analysis should establish the design capabilities and protection system set points to ensure that the fundamental safety functions are always maintained. The design basis events are the basis for the design of the reactivity control systems, the reactor coolant system, the engineered safety features (for example, the emergency core cooling system, the containment system and containment protection

systems), the electric power systems, and various auxiliary systems important to safety.

4.81. The time periods evaluated for events should be sufficient to determine all the consequences of the design basis events. This implies that the calculations for plant transients be extended beyond the point where the plant has been brought to shutdown and the safety cooling systems actuated (i.e. until a long term stable state has been reached).

4.82. For new plants and plants undergoing a periodic safety assessment, a comprehensive identification and assessment of all design basis events should be carried out. For modifications of existing plants, the assessment should focus on those design basis events that are affected by the modification.

4.83. For modifications to, or reassessment of, an existing plant, the methodology and assumptions used in the original design may need to be changed for several reasons:

— The original design basis or acceptance criteria may no longer be adequate.
— The safety analysis tools used may have been superseded by more sophisticated methods.
— The original design basis may no longer be met.

4.84. The safety analysis carried out for anticipated operational occurrences is essentially the same as for accidents. However, for the former, the analysis need not have all the conservatism of the analysis for DBAs. For example, the analysis of anticipated operational occurrences would not necessarily assume the unavailability of all non-safety systems and equipment.

4.85. In addition, the anticipated operational occurrences should not lead to any unnecessary challenges to safety equipment primarily designed for protection in the event of DBAs.

Methods and assumptions for the analysis of anticipated operational occurrences and DBAs

Methods

4.86. The safety analysis of anticipated operational occurrences and DBAs should use suitable neutron physics, thermal-hydraulic, structural and radiological computer

codes to determine the response of the reactor to the operational occurrences and accidents considered.

4.87. The computer codes which are used to carry out the anticipated operational occurrences and DBA analysis should be properly verified and validated. This includes the codes used to predict the behaviour of the reactor core, thermal-hydraulic codes and the radiological release and consequence codes. In addition, the analysts and users of the codes should be suitably qualified, experienced and trained.

4.88. The computer codes for the safety analysis of DBAs/anticipated operational occurrences and should draw on the operating experience that can be derived from similar nuclear power plants and relevant experimental data. Since anticipated operational occurrences are expected to occur once or more during the lifetime of a plant, there is some accumulated basis of operating experience and data for these transients.

4.89. The computer code model parameters, initial conditions and equipment availability assumptions that underlie their use have traditionally been highly conservative with bounding, conservative values used for all analysis parameters. However, in the past this has sometimes led to misleading sequences of events, unrealistic time-scales being predicted, and some physical phenomena being missed. Bearing in mind these shortcomings and the current maturity of best estimate codes, they should be used in a safety analysis in combination with a reasonably conservative selection of input data and a sufficient evaluation of the uncertainties of the results.

4.90. It may also be acceptable to use a combination of a best estimate computer code and realistic assumptions on initial and boundary conditions. Such an approach should be based on statistically combined uncertainties for plant conditions and code models to establish, with a specified high probability, that the calculated results do not exceed the acceptance criteria.

4.91. The safety analysis should be subject to an adequate QA programme. In particular, all sources of data should be referenced and documented, and the whole process should be recorded and archived to allow independent checking.

Assumptions

4.92. The conservative assumptions made for the design basis analysis should typically include the following:

— The initiating event occurs at an unfavourable time as regards initial reactor conditions including power level, residual heat level, reactivity conditions, reactor coolant system temperature, pressure and inventory.
— Any control systems should be assumed to operate only if their functioning would aggravate the effects of the initiating event. No credit should be taken for the operation of the control systems in mitigating the effects of the initiating event.
— All plant systems and equipment not designated and maintained as safety grade (full QA, seismic and equipment qualification) should be assumed to fail in the manner that causes the most severe effects for the PIE being analysed.
— The worst single failure should be assumed to occur in the operation of the safety groups required for the initiating event. For redundant systems it is often assumed that the minimum number of trains start and run.
— The safety systems should be assumed to operate at their minimum performance levels. For reactor trip and safety system actuation systems, this should assume that the action occurs at the worst end of the possible band.
— Any structure, system or component that cannot be considered fully operable or that reaches a limit during the accident for which the designer did not prove full operability should be assumed to be unavailable.
— The actions of the plant staff to prevent or mitigate the accident should only be modelled if it can be shown that there is sufficient time for them to carry out the requested actions, ample information is available for event diagnosis (considering the effects of the initiating event and the single failure criterion), adequate written procedures are available, and sufficient training has been provided. Plant staff actions are typically assumed to occur no sooner than ten minutes after the event begins.

4.93. The conservative assumptions made should take account of uncertainties in the initial conditions of the reactor, including safety system actuation set points.

4.94. The design basis analysis should include any failures which could occur as a consequence of the initiating event (and are thus part of the PIE). These include the following:

— If the initiating event is a failure of part of an electrical distribution system, the DBA analysis should assume the unavailability of all the equipment powered from that part of the distribution system.
— If the initiating event is an energetic event, such as the failure of a pressurized system that leads to the release of hot water or pipe whip, the definition of the DBA should include failure of the equipment which could be affected.

— For internal events such as fire or flood or external events such as earthquakes, the definition of the design basis event should include failure of all the equipment which is neither designed to withstand the effects of the event nor protected from it.

4.95. In view of the very conservative nature of these assumptions, the design basis analysis often provides a robust demonstration that there are large margins before safety limits would be exceeded. However, caution is necessary in using the analysis, as this outcome is not always the case.

4.96. The safety analysis of the anticipated operational occurrences should also include many of the conservative assumptions of the deterministic DBA analysis, especially those which relate to the systems for maintaining critical safety functions during these transients. However, it is not necessary to assume that all non-safety systems and equipment are unavailable and that credit cannot be taken for the control systems in mitigating the effects of the initiating event unless the PIE makes these systems unavailable.

4.97. The results of the assessment should be structured and presented in an appropriate format to provide a good understanding of the course of the event and to allow easy checking of the individual acceptance criteria.

Acceptance criteria

4.98. Acceptance criteria should be developed for events and conditions within the design basis as set forth in Ref. [1]. These criteria should ensure that an adequate level of defence in depth is maintained by preventing damage to barriers against the release of radioactive material and preventing unacceptable radiological releases.

4.99. Acceptance criteria should be developed in two levels as follows:

— Global/high level criteria which relate to doses to the public or the prevention of consequential pressure boundary failure in an accident. These are often defined in law or by the regulatory body.
— Detailed criteria defined by the designer or analyst. These are chosen to be sufficient but not necessary to meet the global acceptance criteria. In addition, the analyst may set targets at a more detailed level (more demanding acceptance criteria) to simplify the analysis (for example, to avoid having to do very sophisticated calculations). The range and conditions of applicability of each specific criterion should be clearly specified.

4.100. The acceptance criteria should relate to the conditions associated with the accident — for example, the frequency of an initiating event or reactor design and plant conditions. Different criteria are generally needed to judge the vulnerability of individual barriers and for various aspects of the accident. More stringent criteria are often applied for events with a higher frequency of occurrence.

4.101. The radiological acceptance criteria for anticipated operational occurrences are typically more restrictive since their frequencies are higher. In general, there should be no failures of any of the physical barriers (fuel matrix, fuel cladding, reactor coolant pressure boundary or containment) and no fuel damage (or no additional fuel damage if minor fuel leakage, within operational limits, already exists).

4.102. The global acceptance criterion for DBAs should be either no off-site radiological impact or only minor radiological impact outside the exclusion area. The definition of minor radiological impact should be set by the regulatory body, but typically corresponds to very restrictive dose limits in order to exclude the need for off-site emergency actions.

4.103. The detailed acceptance criteria could include the following:

— An event should not generate a subsequent more serious plant condition without the occurrence of a further independent failure. Thus an anticipated operational occurrence by itself should not generate a DBA, and such an accident by itself should not generate a beyond design basis accident.
— There should be no consequential loss of function of the safety systems needed to mitigate the consequences of an accident.
— Systems used for accident mitigation should be designed to withstand the maximum loads, stresses and environmental conditions for the accidents analysed. This should be assessed by separate analyses covering environmental conditions (i.e. temperature, humidity or chemical environment) and thermal and mechanical loads on plant structures and components.
— The pressure in the primary and secondary systems should not exceed the relevant design limits for the existing plant conditions. Additional overpressure analysis may be needed to study the influence of failures on safety and relief valves.
— The number of fuel cladding failures which could occur should be established for each type of PIE to allow the global radiological criteria to be met.
— In LOCAs with fuel uncovering and heatup, a coolable geometry and structural integrity of the fuel rods should be maintained.
— No event should cause the temperature, pressure or pressure differences within the containment to exceed values which have been used as the containment design basis.

Beyond design basis and severe accident considerations

4.104. Accidents that are more severe than DBAs are termed beyond design basis accidents. These can have a range of consequences as follows:

— They fall within the envelope of the conservative acceptance criteria for the DBAs, although a best estimate analysis may be needed to demonstrate this.
— They exceed the conservative acceptance criteria for DBAs but would not result in significant fuel damage or primary circuit failure limits being exceeded based on best estimate analysis.
— Due to multiple failures and/or operator errors, safety systems fail to perform one or more of their safety functions leading to significant core damage that challenges the integrity of the remaining barriers to the release of radioactive material from the plant. These are termed severe accidents. Severe accidents could further escalate to:

  • core damage plus failure of the primary circuit, but not the containment
  • core damage plus failure of the primary circuit and the containment, resulting in a large release of radioactive material to the environment and challenging off-site emergency response measures.

4.105. The safety analysis should aim to quantify a plant safety margin and demonstrate that a degree of defence in depth is provided for this class of accidents. This would include such measures where reasonably achievable:

— To prevent the escalation of events into severe accidents, control the progression of severe accidents and limit the releases of radioactive material through the provision of additional equipment and accident management procedures.
— To mitigate the radiological consequences that might occur through the provision of plans for on-site and off-site emergency response.

For those hypothetical severe accident sequences (e.g. high pressure core melt in PWRs) that could lead to early failure of the containment, it should be demonstrated that they can be excluded with a very high degree of confidence.

Selection of severe accidents for safety analysis

4.106. The severe accident analysis should address a set of representative sequences in which the safety systems have malfunctioned and some of the barriers

to the release of radioactive material have failed or have been bypassed. These sequences should be selected by adding additional failures or incorrect operator responses to the DBA sequences (to include safety system failure) and to the dominant accident sequences from the PSA.

4.107. The significant event sequences that could lead to severe accidents should be identified using a combination of probabilistic and deterministic methods and sound engineering judgement.

4.108. The most rigorous way of identifying severe accident sequences is to use the results of the Level 1 PSA (see para. 4.124). However, it might also be possible to identify representative or bounding sequences from an understanding of the physical phenomena involved in severe accident sequences, the margin existing in the design, and the amount of system redundancy remaining in the DBAs.

4.109. Examples of severe accident initiators include the following:

— Complete loss of the residual heat removal from the reactor core,
— LOCA with a complete loss of the emergency core cooling,
— Complete loss of electrical power for an extended period.

4.110. The details of the severe accident sequences that need to be analysed will differ depending on the design of the reactor safety systems.

4.111. The assessment of severe accidents should account for the full design capabilities of the plant, including the use of some safety and non-safety systems beyond their originally intended function to return the potential severe accident to a controlled state and/or to mitigate its consequences. If credit is taken for extraordinary use of systems, there should be a reasonable basis to assume they can and will be used as analysed.

Methods and assumptions for severe accident analysis

4.112. There is no widespread agreement on the best approach to severe accident analysis and acceptance criteria. However, there is a clear tendency for the following or similar criteria to be adopted for new advanced reactor designs. The severe accident analysis should generally be carried out using best estimate assumptions, data, methods and decision criteria. Where this is not possible, reasonably conservative assumptions should be made which take account of the uncertainties in the understanding of the physical processes being modelled.

4.113. The severe accident analysis should model the wide range of physical processes that could occur following core damage and that could lead to a release of radioactive material to the environment. These should include, where appropriate:

— Core degradation processes and fuel melting;
— Fuel–coolant interactions (including steam explosions);
— In-vessel melt retention;
— Vessel melt-through;
— Distribution of heat inside the primary circuit;
— High pressure melt ejection/direct containment heating;
— Generation and combustion of hydrogen;
— Failure or bypass of the containment;
— Core–concrete interaction;
— Release and transport of fission products;
— Ability to cool in-vessel and ex-vessel core melt.

4.114. The analysis would typically involve a multitiered approach using different codes, including detailed system and containment analysis codes, more simplified risk assessment and 'separate effects' codes, and source term and radiological impact studies. Use of a full selection of codes will ensure that all the expected phenomena are adequately analysed.

4.115. The assessment should ensure that the reactor core, primary circuit and containment are modelled accurately. These models are particularly significant to the analysis and are influential in determining the course of the accident.

Acceptance criteria

4.116. The acceptance criteria for severe accidents are usually formulated in terms of risk criteria (probabilistic safety criteria). These are discussed in paras 4.219–4.231. However, there is only limited agreement on what these criteria should be.

Deterministic acceptance criteria have also been specified in a number of countries, typically as follows:

— Containment failure should not occur in the short term following a severe accident,
— There should be no short term health effects following a severe accident,
— The long term health effects/release of ^{137}Cs should be below prescribed limits following a severe accident.

Consideration of severe accidents in the design

4.117. The aim of severe accident analysis should be:

— To evaluate the ability of the design to withstand severe accidents and to identify particular vulnerabilities. This includes assessment of equipment that could be used in accident management and instrumentation that could monitor the course of the accident.
— To assess the need for features that could be incorporated in the plant design[17] to provide defence in depth for severe accidents.
— To identify accident management measures that could be carried out to mitigate accident effects.
— To develop an accident management programme to be followed in beyond design basis accidents and severe accident conditions.
— To provide input for off-site emergency planning.

4.118. The consideration of severe accidents should be done at the design stage for new plants. However, for currently operating plants, a severe accident management programme should be developed that makes full use of all available equipment and procedures to mitigate the consequences of the accident. Such measures could include the use of alternate or diverse systems, procedures and methods to use non-safety grade equipment, and the use of external equipment for temporary replacement of a standard component. Details on the development and implementation of the accident management programmes are dealt with in a separate IAEA publication [9].

4.119. The effectiveness of the above design features and accident management measures in reducing risk should be evaluated by the PSA.

Emergency planning

4.120. The severe accident analysis should also provide input to civil authorities for off-site emergency planning and response.

---

[17] These design features might include the following:
— Core catcher or core spreading area and basemat concrete that is resistant to core melt damage.
— Hydrogen recombiners sized to cope with the rate of hydrogen generation that could occur following a severe accident.
— Filtered containment venting system that would be operated in the longer term to prevent failure of the containment due to overpressurization following a severe accident.

4.121. The results of the severe accident analysis should be used to identify source terms which could be used as a basis for off-site emergency planning.

4.122. The source terms could also be used to demonstrate the effectiveness of sheltering, taking potassium iodide tablets, food bans and evacuation.

PROBABILISTIC SAFETY ANALYSIS

Introduction

4.123. Probabilistic safety analysis provides a comprehensive, structured approach to identifying accident scenarios and deriving numerical estimates of risks. PSAs for nuclear power plants are normally performed at three levels as follows:

4.124. **Level 1 PSA,** which identifies the sequence of events that can lead to core damage, estimates the core damage frequency and provides insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage.

4.125. **Level 2 PSA,** which identifies ways in which radioactive releases from the plant can occur and estimates their magnitude and frequency. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures such as the use of a reactor containment.

4.126. **Level 3 PSA,** which estimates public health and other societal risks such as the contamination of land or food.

4.127. Level 1 PSAs have now been carried out for most nuclear power plants worldwide. However, in recent years, the emerging standard is for Level 2 PSAs to be carried out for many types of nuclear power plants. To date, relatively few Level 3 PSAs have been carried out.

Use of PSA as part of the decision making process

4.128. The results of PSA should be used as part of the design process to assess the level of safety of the plant. The insights gained from PSA should be considered along with those from the deterministic analysis to make decisions about the safety of the plant. This should be an iterative process aimed at ensuring that national requirements and criteria are met, the design (as defined in para. 4.139) is balanced and the risk is as low as reasonably achievable.

4.129. The results of the PSA should be used to identify weaknesses in the design or operation of the plant. These would be identified by considering the contributions to the risk from groups of initiating events and from measures of the importance of the safety systems and human error contributions 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.

4.130. In addition, the results of the PSA should be compared with the probabilistic safety criteria when these have been defined for the plant. This should be done for all the probabilistic criteria defined for the plant, including those which address system reliability, core damage, releases of radioactive material, worker health effects, public health effects and off-site consequences such as land contamination and food bans.

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

4.132. The results of the Level 2 PSA should be used to determine if sufficient provision has been made to mitigate the effects of a core damage should it occur. This would address whether the containment is adequately robust and the protection systems such as hydrogen mixing/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. In addition, the Level 2 PSA should be used to identify accident management measures which could be carried out to mitigate the effects of the molten core. This could include identifying additional measures which could be taken to introduce water into the reactor containment.

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

Requirement for a PSA

4.134. 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.

4.135. For a new plant, the PSA should ideally be started during the conceptual design to check that the level of redundancy and diversity provided in the safety systems is adequate, continued through the more detailed design phase to assess more detailed design issues, and used to support the operation of the plant. During the design phase, there should be an iterative process to ensure that the insights gained from the PSA are fed back into the design process.

4.136. 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 database may be different. 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 it would be reasonable to implement to reduce risk.

4.137. The PSA should address the actual or intended design or operation of the design of the plant which should be clearly identified as the starting point 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 will have been completed.

4.138. The PSA should set out to: identify all the fault sequences which contribute to risk; determine if there are weaknesses in the design or operation of the plant; and 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 events or shutdown states) then conclusions made 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 incorrect.

4.139. The PSA should determine if the safety systems contain an adequate level of redundancy and diversity, if there is sufficient defence in depth and if the overall design is balanced. In a balanced design the PSA should show that:

— No particular feature of the design makes a disproportionately large contribution to risk;
— No group of initiating events makes a disproportionately large contribution to risk;
— The achievement of an overall low level of risk does not rely on contributors which have a significant uncertainty;
— The first two levels of defence carry the primary burden of safety;
— Within each level of defence, none of the safety systems is disproportionately more significant than the others.

A lack of balance is usually an indication that there are opportunities for reasonably practicable risk reduction.

Scope of the PSA

4.140. The PSA should address the contributions to risk arising from all the modes of operation of the plant. However, it may be convenient to analyse at power and shutdown modes separately (and not to the same level).

4.141. If the PSA is only carried out to Level 1, then the reactor core is, by definition, the focus of the analysis. If the PSA is carried out to Level 2 or Level 3, then the scope of the PSA may include contributions to risk arising from other sources of radioactive material on the site, such as used fuel and radioactive waste. These ex-core sources should be included whenever the intention is to address the total risk from the plant to an individual near the site.

4.142. The PSA should take as its starting point the complete set of PIEs including both internal and external PIEs. The analysis should then go on to identify the complete range of fault sequences which would contribute to the risk. These fault sequences should address component failures, component unavailability during maintenance or testing, human errors, common cause failures and, if possible, take into account the ageing of components.

PSA methods

4.143. A large number of PSAs have been carried out to date for a variety of nuclear power plant designs. As a consequence, the methods for PSAs are very well developed, particularly those for a Level 1 PSA. It is recognized that there are uncertainties inherent in the PSA process. Uncertainties are not unique to PSA, they are also present in the deterministic safety analyses. However, the PSA methodologies have the capability to recognize and to quantify a large fraction of these uncertainties. For any new PSA being undertaken, the methods used should conform with current best international practice.

4.144. The PSA should preferably use best estimate methods throughout. This would include the analysis carried out to support the safety systems' success criteria, the modelling of the phenomena which would occur inside the containment following core damage, and the transport of radioactive material released to the environment. When this is not possible, reasonably conservative assumptions should be used.

Level 1 PSA: Analysis of core damage frequency

4.145. The aim of the Level 1 analysis should be to determine the overall frequency of core damage. This requires a definition of what constitutes core damage and translation of this definition into safety system failure criteria. More information on the procedures for conducting a Level 1 PSA is given in Ref. [10]. The analysis should identify the fault sequences which make the greatest contribution to frequency, identify the safety systems which are most important to preventing core damage and determine if changes can be made to the design or operation of the plant to reduce the risk.

Postulated initiating events

4.146. The starting point for the PSA should be the complete list of PIEs which could lead directly or in combination with other failures to a challenge to nuclear safety. The consequential failures which are included in the deterministic analysis are, in the PSA, taken into account in the analysis of the event sequence and the systems analysis.

4.147. The set of PIEs addressed should include all internal and external events, including the low frequency events which could occur but have not been taken into account during the design of the plant.

4.148. This analysis should include the PIEs which could occur during all the modes of operation of the plant and could lead to a release of radioactive material from any of the sources on the site.

Specification of safety system requirements

4.149. For each of the PIEs identified, the safety functions that need to be performed to prevent core damage should be identified. These safety functions are the same as those addressed in the design basis analysis — that is, detection of the initiating event, reactor shutdown, residual heat removal and containment protection. However, the limits above which the safety function would be considered to have failed would be realistic limits rather than the conservative limits defined for the design basis analysis.

4.150. The safety systems needed to perform these safety functions should be specified. This should be based on best estimate transient analysis rather

than the conservative analysis carried out for the design basis analysis. The number of trains of redundant and diverse systems that are required to operate should be specified.

4.151. PIEs can be identified which need the same or very similar safety system interventions. To reduce the amount of analysis, it is normal to group these PIEs and analyse them together in the PSA. (This is similar but not identical to the grouping for deterministic analysis described in paras 4.75 to 4.77.) The initiating event group is then represented by the initiating event with the most onerous safety system response and the frequency is taken to be the sum of the individual initiating events in the group. Where PIEs are grouped, the grouping should be done in such a way that it does not introduce an unacceptable level of pessimism into the analysis. This could happen for example when the representative event chosen has a low frequency and all the other events in the group have significantly less onerous safety system demands but a much greater summed frequency.

Analysis of the event sequence

4.152. In the analysis of the event sequence, logical models are constructed for groups of initiating events to identify the fault sequences leading to core damage that could occur. These logical models start with the fundamental safety function and consider the required safety functions for the group of initiating events, the safety systems and the individual components in the safety systems. The logical models determine how component failures can combine to lead to safety function failure and core damage.

4.153. The analysis of the event sequence carried out for a group of initiating events should aim to identify all the combinations of success or failure of the safety system equipment which would lead to a failure to maintain the plant within safe limits in such a manner that core damage would occur.

4.154. In most current PSAs, the analysis of the event sequence is carried out by a combination of event tree and fault tree analysis since this has been empirically found to be the most efficient way of handling the large logical models that are necessary for a nuclear power plant. However, it is possible to carry out the analysis using fault trees or event trees alone, and, for specific event analysis, dynamic time dependent analysis techniques can be used.

4.155. A systematic assessment should be carried out to identify the failures of safety system equipment (and of safety related or non-safety related equipment, if

these failures could affect the sequence) which could occur as a consequence of the initiating event; these failures should be included in the logical models which represent the event sequences which could occur.

4.156. The analysis of the event sequence should cover all the combinations of safety system equipment that can operate to perform the required safety functions.

4.157. Since some of the safety systems incorporated in a nuclear power plant share common actuation systems or common support systems such as electrical power, control and instrumentation equipment and cooling systems, this introduces functional dependences between safety systems. A systematic assessment of the design and operation of the plant should be carried out to ensure that all such interdependences are identified and modelled explicitly in the analysis of the event sequence or systems analyses.

Safety system failure analysis

4.158. The event sequence analysis should be extended down to the level of individual basic events. These basic events typically include component failures, component unavailability during maintenance or testing, common cause failures of redundant equipment and operator errors.

4.159. The system failure analysis should address all the relevant failure modes of individual items of safety system equipment. These failure modes would normally have been identified by the failure modes and effects analysis carried out as part of the design assessment. Any failures consequential to the PIE should also be included in the system model (if not already fully accounted for in the event sequence models).

4.160. All the necessary support systems should be identified and included in the systems failure analysis and the interdependences which arise due to common support systems should be represented explicitly in the logical models.

4.161. During the lifetime of the plant, individual items or trains of equipment may be taken out of service for testing, maintenance or repair and this will reduce the availability of the safety system to perform safety functions. Such equipment outages should be taken into account explicitly in the PSA. This can be done either by introducing basic events into the logical models to represent equipment outages or by carrying out multiple runs of the PSA.

Data

4.162. To quantify the analysis, data are needed for the following items:

— Initiating event frequencies,
— Equipment failure probabilities,
— Equipment outage frequency and duration,
— Common cause failure probabilities,
— Human error probabilities.

4.163. The initiating event frequencies and equipment failure probabilities used should be appropriate to the design or operation of the plant. If possible, plant specific data should be used. When this is not possible, data from the operation of similar plants should be used. Again, when this is not possible, generic data should be used when these can be shown to be relevant. For initiating events with a low frequency, a judgement should be made.

4.164. In specifying the equipment failure rates, the boundaries of the equipment should be specified and all the relevant failure modes should be included. For a pump, this includes failure to start, failure to run for the specified mission time and leakage from the pump seals.

4.165. The statistical data used should cover all the relevant causes of initiating events and all the relevant equipment failure modes.

4.166. For some of the items addressed in the PSA, in particular the frequency of remote initiating events such as pressure vessel failures or severe earthquakes, there is no relevant operating experience. If these are not considered to give a significant contribution to risk, they can be screened out as long as justification is provided. Otherwise, judgements on their frequencies should be made and the basis for the judgement given. In particular, the methods for performing probabilistic seismic hazard assessments are well developed and can be adapted to any site.

Common cause failure

4.167. There is the potential for redundant items of equipment within a safety system to fail due to a common cause and this limits the reliability of the system. Such common cause failures (CCFs) can be modelled in the analysis at the safety system level or at an individual component level. One way of doing so is to model CCF at a safety system level by introducing a basic event into the logical model which represents the CCF of the system. There are a number of approaches in which the

CCF probability can be estimated which include the use of operating experience data and theoretical models such as the beta factor and multiple Greek letter methods.

4.168. Common cause failures which could occur within redundant safety systems should be modelled in the analysis. Justification should be provided for the CCF models and data used in the PSA. Wherever possible, this should take into account the operating experience for similar systems.

4.169. Previous analysis and operating experience has indicated that there is a limit on the failure probability of non-diverse safety systems which would be in the range of about 10^{-3} to 10^{-5} failures per demand, depending on the level of redundancy provided and other design and operational factors. This should be reflected in the analysis.

Human reliability analysis

4.170. Human errors can affect both the cause and the frequency of an event sequence. They can take place before, during or after initiation of the event sequence and can either mitigate or aggravate an accident. These should be modelled in the PSA. Data on human reliability should be derived from sources such as event reports, maintenance reports, PSA reports and simulator observations.

4.171. Human errors which can lead to initiating events should be identified and included as part of the initiating event frequency.

4.172. Human errors which can lead to safety system failures and loss of critical safety functions should be modelled explicitly in the event sequence and safety system failure analysis.

4.173. The human error probabilities used should reflect the factors which can influence the performance of the operator, including the level of stress, the time available to carry out the task, the availability of operating procedures, the level of training and environmental conditions. These should be identified by the task analysis carried out as part of the design evaluation.

Quantification of the analysis

4.174. The logical model developed should be quantified using the data to determine the overall core damage frequency and the contributions from initiating event groups. There are a number of computer codes currently available which can be used to perform this analysis.

4.175. In the quantification of the analysis, the importance of initiating event groups, component failures, safety system failure and operator errors should be derived to identify where the contributions to the risk are coming from and where there may be weaknesses in the design or operation of the safety systems. This could use quantitative measures of importance (such as Birnbaum and Fussell-Vesely — see Ref. [10]) where applicable. This should be supported by sensitivity studies where there are uncertainties in the models and data.

Results of the analysis of core damage frequency

4.176. The results of the analysis should be assessed to gain confidence that they provide an adequate representation of the risk from the plant. If there are areas where it is judged that the risk estimates are excessively conservative or optimistic, the analysis should be revised to make it more realistic. Excessive conservatism can occur if the safety system success criteria are based on conservative design basis transient analysis and conservative critical safety function success criteria rather than on the best estimates recommended for the PSA. Excessive optimism can occur if potential initiating events are inappropriately screened out.

4.177. The results of the analysis should be compared with the safety criteria for core damage frequency proposed for the plant (where these have been specified). If the core damage frequency estimated for the plant is unacceptably high, changes should be made to the design or operation of the plant to reduce the risk.

4.178. Even if the core damage frequency is acceptably low, the results of the PSA should be reviewed systematically to identify any relative weakness in the design and operation of the plant and to identify improvements which could be made to reduce the frequency of core damage. These changes should be made where it is reasonably achievable to do so. The judgement on what is reasonably achievable will depend on whether the reactor is at the design stage or in operation, and on the cost of making the changes. This process would be repeated to try to reduce the core damage frequency down to or below the design target (where this has been defined) and to produce a balanced design.

Level 2 PSA: Analysis of accident progression from core damage to release of radioactive material

4.179. This part of the analysis considers the progression of the accident from the onset of core damage and considers the phenomena that could occur and would lead to

containment failure and a release of radioactive material to the environment. Detailed information on the procedures for carrying out a Level 2 PSA is given in Ref. [11].

4.180. The analysis considers the effectiveness in the design and accident management measures provided to mitigate the effects of core damage and provides estimates of the frequency of a large release of radioactive material to the environment which can be compared with probabilistic criteria (where they have been defined).

Definition of plant damage states

4.181. The fault sequences identified in the Level 1 PSA which would lead to core damage should be grouped into plant damage states (PDSs) which are defined in terms of the factors which influence the containment response or the releases of radioactive material to the environment. These factors typically include the type of initiating event that has occurred, the reactor coolant system pressure, the status of the emergency core cooling and containment protection systems and the integrity of the containment.

Modelling of core damage progression

4.182. The analysis of the accident progression from core damage to radioactive material release should model the significant phenomena which challenge the integrity of the containment or influence the release of radioactive material. These phenomena are identified in para. 4.113 and are described more fully in the literature (see, for example, IAEA and OECD NEA reports on Level 2 PSA, Refs [11, 12], respectively).

4.183. The analysis should use a logical approach which models how the event sequences progress from core damage to a radiological release. This is usually done by event tree analysis which models the accident sequence in a number of time frames and uses a set of nodal questions to model the sequence of events which occur. The construction of the event trees needs to be supported by thermal-hydraulic calculations and modelling of fission product release and transport inside the containment.

4.184. The event tree analysis should have sufficient time frames and nodes to allow the significant phenomena which could occur inside the containment to be addressed. The emerging standard is to specify about 20–30 nodes, although some analyses have used many more nodes than this (for example, NUREG-1150 [13]). These nodal questions will be the same for the event trees drawn for each of the PDSs;

however, the actual event trees will be different in detail for each of the states defined owing to the different initial conditions characterized by the PDS.

4.185. The end points of the event trees identify the sequence of events which has occurred and the state of the containment. The possibilities are that the containment is intact or that it has failed. The possible modes of failure are: bypass, isolation failure (these two failure modes are modelled in the PDS definition), leakage, rupture or basemat melt-through. The resulting release of radioactive material will also depend on whether containment failure has occurred early or late in the event sequence.

Data

4.186. The relevant data for the quantification of the event tree analysis are the conditional probabilities for the branch points. There is considerable uncertainty in the phenomena that would occur and consequently the probabilities used are often based on expert judgement.

4.187. The assessment should confirm that the framework for making these expert judgements is sound and the basis for the judgement is stated and shown to be valid as far as possible. This should take account of the thermal-hydraulic analysis that has been carried out, analyses for other similar plants and applicable research data. The quantification of the containment event trees should take account of the interdependences between the various phenomena that are being modelled.

Containment performance analysis

4.188. One of the important issues that needs to be addressed is how the containment will behave due to the loading placed on it as a result of the core damage and how failure will occur.

4.189. Direct bypass of the containment (for example, due to a steam generator tube rupture or to an interfacing systems LOCA which discharges outside the containment) and failure of the containment isolation system should be addressed in the analysis. This would normally be included in the definition of the PDSs.

4.190. A structural analysis should be carried out to determine how the containment will behave due to pressure and temperature conditions that could arise from steam explosions, non-condensable gases or hydrogen burns. This should be based on the actual design of the containment taking account of doors, penetrations, seals and other possible weak areas. The possible failure modes of the containment should be identified and the conditional probability that containment failure will occur should

be estimated as a function of pressure and temperature. This information can then be used to estimate the conditional failure probabilities used to quantify the event trees.

4.191. An analysis should also be carried out to determine how the containment basemat might fail as a result of the molten core–concrete interaction which would occur after pressure vessel failure. Estimates should be made of the conditional probability of basemat failure as a function of the residual heat level and the cooling available to the molten material. Special care should be taken when the basemat of the containment has additional compartments above so that penetration of the basemat could lead to a radioactive release via unfiltered pathways.

Source term analysis

4.192. There are usually a large number of end points in the event tree analysis and these are normally grouped into release and/or source term categories which have similar radiological characteristics and off-site consequences.

4.193. The definition of the release categories should include factors such as the quantity of each of the isotopes included, the time, duration, location, energy content and particle size distribution.

4.194. The source terms should be determined for each of the release categories defined. This should take account of the factors which affect the source term, including the volatility of the radionuclides, releases from the fuel, retention of fission products within the reactor coolant system and retention of fission products inside the containment.

4.195. The frequency of each of the release categories should be calculated by summing the frequencies of each of the end points on the event trees assigned to it. When the scope of the PSA includes releases from all sources of radioactive material on the site, the releases from these ex-core sources should be taken into account at this point. This may involve the definition of additional release categories which would typically have lower off-site impact but higher frequency than those from a damaged core.

Results of the Level 2 PSA

4.196. The results of the Level 2 PSA are usually presented in the form of a table of source term categories or release categories together with their frequencies of occurrence. The source term and/or release categories are defined in terms of their composition of radionuclides (grouped into fission product groups in accordance with

their common chemical and physical characteristics) together with the characteristics of the release (time of occurrence after the onset of the accident, duration, height and energy content). From this information the frequency of a large release or a large early release can be derived for comparison with probabilistic criteria (where defined). 'Large' is defined as being greater than a specified quantity of radioactive material often defined in terms of a fraction of the radioactive inventory of the core.

4.197. As with other parts of the PSA, the results of the Level 2 analysis should be used to identify the principal contributors to risk and changes that can be made to the design or operation of the plant to reduce risk. This should take into account the significant phenomenological uncertainties inherent in a Level 2 PSA. These measures could include hydrogen control systems (which have an adequate capacity to cope with the rate of hydrogen generation after a core damage), filtered containment venting systems to prevent overpressurization of the containment in the longer term or dedicated systems for a molten core cooling. These should be incorporated into the design when it is reasonably achievable to do so, taking the costs and benefits into account.

On-site accident management

4.198. During the course of the accident, operator actions can be taken to prevent further progress of the accident or to reduce its effects. Examples of such accident management measures often included in the analysis are opening relief valves to reduce the primary circuit pressure and avoid molten material being ejected from the reactor pressure vessel under high pressure, and adding water to the containment after the molten core has exited from the primary circuit, to provide a cooling medium.

4.199. The Level 2 PSA should be used to identify what accident management measures are possible to mitigate the effects of a molten core. These measures should include the actions that can be taken to support the containment function or to limit the releases of radioactive material that could occur. These accident management measures should be incorporated into the emergency operating instructions for the plant and training should be provided for the plant operators who have the responsibility to carry out these accident management measures. The severe accident management measures should be compatible with the equipment, instrumentation and diagnostic aids which the plant operators could reasonably use in such situations.

Level 3 PSA: Analysis of off-site consequences

4.200. The analysis of the off-site consequences models the release of radionuclides from the nuclear power plant, their transfer through the environment and

their public health and economic consequences. More detailed information on the procedures for carrying out a Level 3 PSA is given in Ref. [14]. The analysis should (a) provide estimates of the individual risk of death for a member of the public living close to the site, (b) address a number of off-site consequences including early and late health effects to members of the public and (c) consider other economic consequences.

Source term grouping

4.201. As discussed in paras 4.192–4.196 above, the fault sequences identified in the Level 2 PSA are normally grouped into release categories which have similar characteristics in terms of their challenges to atmospheric dispersion and off-site consequences. The set of release categories defined should represent the spectrum of releases of radioactive material which could occur from the plant. These categories are normally defined in terms of the composition of radionuclides released which are classified in terms of their volatility. In addition, the release category would also define the time which elapses between the occurrence of the initiating event and the onset of the release and the duration of the release, since these are relevant to off-site emergency planning. The frequency of the release category should be calculated from the sum of all the containment event tree end points included in the release category.

Atmospheric dispersion modelling

4.202. A number of computer codes are available for carrying out the off-site consequences analysis. These need plant and site specific data to be input, including release categories and frequencies for the plant and meteorological, population, agricultural and economic data for the site and its surroundings. The codes model the transport of radionuclides in the environment including atmospheric dispersion, deposition, resuspension, food chain pathways and model exposure pathways (cloud shine, inhalation, contamination, ground deposition, resuspension and ingestion) to determine the health effects to the public and the off-site economic consequences. (A review of the available computer codes for off-site consequence analysis has been carried out by the IAEA [14].)

Meteorological data

4.203. Meteorological data should be specified for the site. These should be based on data collected close to the site over a number of years and typically include wind direction, wind speed, stability category, rainfall and mixing layer depth. (The precise data would depend on the computer code used.)

Population, agricultural and economic data

4.204. Population, agricultural and economic data should be specified for the site. This data would normally be based on national information supplemented by local surveys close to the site. The data necessary would depend on the choice of health effects and economic factors to be included in the analysis. How the information is set up for processing would depend on the specific needs of the computer code used.

Results of the societal risk estimates

4.205. The results of the societal risk estimates should be compared with the risk criteria where these have been defined for the plant.

4.206. The results of the societal risk estimates should be provided to civil authorities as a technical input to their decision making process on off-site emergency planning provisions.

Off-site emergency planning

4.207. Emergency planning and preparedness refer to the activities which can be carried out on and off the nuclear power plant site to protect workers and members of the public from the effects of a release of radioactive material from the plant. Countermeasure strategies should be investigated using the Level 3 PSA when available. This analysis should include a consideration of the benefits of short term measures such as sheltering, evacuation and taking potassium iodide tablets; and the need for long term countermeasures such as food bans, relocation and land decontamination. This analysis should also consider the way in which the countermeasures are initiated — whether automatically, depending on the state of the plant, or on the basis of the dose.

4.208. The results of the Level 3 PSA should be used to provide input to formulating the emergency plan and to assess the relative effectiveness of the emergency response planning aspects.

Validation of the PSA

4.209. The analysis necessitates a number of calculation methods. These range from the logical event and fault tree models used in the event sequence analysis, to the models of phenomena which could occur within the containment following a core

damage and the models for the transport of radionuclides in the environment to determine their effects on health and the economy. These calculation methods should be validated to demonstrate that they are an adequate representation of the processes taking place. This is addressed in the section below on Assessment of the Computer Codes Used.

4.210. It is becoming standard practice for the operating organization to commission an independent peer review of the PSA from an outside body, often from a different country, to provide a degree of assurance that the scope, modelling and data are adequate and to ensure that they conform to current best practices worldwide in PSA.

Use of the PSA

Presentation of the results of the PSA

4.211. The results of the PSA should be examined to identify the fault sequences which provide the highest contribution to risk. In some cases a contributor may be indicated by the PSA as being dominant, but further examination may suggest that its dominance is due to excessively conservative assumptions in that part of the PSA rather than a relative reflection of the reactor design. In such a case, consideration should be given to revising these parts of the analysis to provide a better estimate of risk.

Living PSA

4.212. The PSA should be used during the lifetime of the plant to provide an input into the decision making process. During 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, as for instance a change in plant configuration during maintenance and testing. These modifications could have an impact on the level of risk of the plant. Statistical data on initiating event frequencies and component failure probabilities 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.

4.213. Consequently, the PSA should be kept sufficiently up to date during the lifetime of the plant to make it useful for the decision making process. Updating

should take into account changes in the design and operation of the plant, new technical information, more sophisticated methods and tools that become available, and new data derived from the operation of the plant. The status of the PSA should be reviewed regularly to ensure that it is maintained as a representative model of the plant.

4.214. Data should be collected by the plant operators throughout the lifetime of the plant to check or update the analysis. These should include statistical data on initiating event frequencies, component failure rates and plant unavailability during periods of testing, maintenance or repair. The analysis should be assessed in the light of the new data.

4.215. The development of a 'living PSA' should be encouraged to assist the decision making process during normal operation of the plant. This includes activities such as the planning of maintenance outages where the PSA would be used to help to ensure that the risk from these activities is adequately low. Experience has shown that such a living PSA can be of substantial benefit to the operating organization, and its use is generally welcomed by the regulators.

Limitations of PSA

4.216. PSA is a key part of the design assessment and safety analysis process, since it provides an integrated risk model for the entire plant and allows a consistent evaluation of both the frequency and consequences of possible accident scenarios. However, there are limitations in PSA which need to be understood.

4.217. In particular, PSA should not be seen as a replacement for the engineering design assessment or the deterministic design approach. Rather, PSA should be seen as providing insights related to the level of risk arising from the plant. These risk insights should be used to complement those from the deterministic analysis in the decision making process.

4.218. There are uncertainties in the models and data used in PSA. This uncertainty is relatively small for component failure probabilities derived from a large database or relevant operating experience. However, it can be much larger and even unquantifiable in a number of other areas, including the following:

— Initiating event frequencies and component failure rates where no operating experience data exist,
— Frequency and ground motions associated with large earthquakes,

— Modelling of common cause failures,
— Modelling of human errors,
— Modelling of the phenomena which would occur in severe accidents,
— Estimating the off-site consequences of releases of radioactive material from the plant.

This uncertainty needs to be recognized in using the results of the PSA in the decision making process. The results of the PSA should be supported by an uncertainty analysis or, at least, by sensitivity studies.

Probabilistic safety criteria

Setting up criteria

4.219. Where the results of the PSA are to be used in support of the decision making process, a formal framework for doing this should be established. The details of this process will depend on the purpose of the particular PSA application, the nature of the decision, and the PSA results to be used. When the numerical results of the PSA are to be used some reference values against which these results can be compared should be established.

4.220. When the aim of the PSA is to identify the dominant contributors to risk or to choose between various design options and plant configurations, a reference value may not be needed.

4.221. However, when the aim of the PSA is to assist in reaching a judgement on whether (i) the calculated risk is acceptable, (ii) a proposed change to the design or operation of the plant is acceptable, or (iii) a change is needed to reduce the level of risk, then probabilistic safety criteria should be developed to provide guidance to designers, operators and regulators on the level of safety desired for the plant. These criteria will also serve to define the goals that the designers, operators and regulators will have to meet in fulfilling their respective roles in the provision of safe nuclear power.

4.222. A PSA will yield numerical measures of risk at various levels according to the level of consequences calculated. Probabilistic safety criteria may be set in relation to any or all of these measures as follows:

— The failure probability of safety functions or safety systems (Level 0);
— The frequency of core damage (Level 1);

— The frequency of a specific release (e.g. quantity, isotopes) of radioactive material from the plant or frequency as a function of magnitude (Level 2);
— The frequency of specific health effects to members of the public or environmental consequences (Level 3).

4.223. One possible framework for the definition of probabilistic safety criteria is given in Ref. [15], 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 countries, there is no international consensus on its application and it is more usual to find probabilistic safety criteria identified as targets, goals, objectives, guidelines or reference values for orientation. In addition, there is no international consensus on the numerical values for the levels of risk which correspond to the threshold of tolerability and the design targets.

Numerical values

4.224. Based on current experience with nuclear power plant design and operation, INSAG has proposed numerical values that can be achieved by current and proposed designs of nuclear power plants.

4.225. *Safety function or safety system failure probability:* Probabilistic targets can be set at a safety function or a safety system level. These are useful to check that the level of redundancy and diversity provided is adequate. Such targets will be plant design specific so that no guidance is provided here. The safety assessment should check 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 attention should be paid to the safety systems in question to see whether any reasonably practicable improvements can be made.

4.226. *Core damage frequency:* For this, INSAG (Ref. [4]) has proposed the following objectives:

— 10^{-4} per reactor–year for existing plants,
— 10^{-5} per reactor–year for future plants.

4.227. The 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 countries, these numerical values have been used either formally or informally as probabilistic safety criteria.

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

— As absolute quantities (in Bq) of the most significant nuclides released,
— As a fraction of the inventory of the core,
— As a specified dose to the most exposed person off the site,
— As a release giving 'unacceptable consequences'.

4.229. Probabilistic safety criteria have also been proposed by INSAG for a large radioactive release [4]. The following objectives are given:

— 10^{-5} per reactor-year for existing plants,
— 10^{-6} per reactor-year for future plants.[18]

4.230. Although there is no consensus on what constitutes a large off-site release, similar numerical criteria have been specified in a number of countries.

4.231. *Health effects to members of the public:* INSAG has given no guidance on the targets for health effects for members of the public. In some countries the target for the risk of a death of a member of the public is taken to be 10^{-6} per reactor-year.

SENSITIVITY STUDIES AND UNCERTAINTY ANALYSIS

4.232. Use of the best estimate codes as recommended for both deterministic and probabilistic safety analysis should be complemented by sensitivity studies and/or by uncertainty analysis.

[18] INSAG-3 Rev. 1 [4], rather than probabilistic safety criteria, states the following objective for future nuclear power plants: "Another objective for these future plants is the practical elimination of accident sequences that could lead to large early radioactive release, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analysis so that their consequences would necessitate only protective measures limited in area and in time."

4.233. Sensitivity studies, which include systematic variation of the code input variables and modelling parameters, should be used to identify the important parameters necessary for the analysis and to show that there is no abrupt change in the result of the analysis for a realistic variation of inputs ('cliff edge' effects).

4.234. Uncertainty studies in the framework of deterministic safety analysis are meant as statistical combinations of the influence of the plant conditions, code models and associated phenomena on the results. These studies should be used to confirm that the actual plant parameters will be bounded by the results of calculation plus uncertainty with a specified high confidence. A combination of sensitivity studies, code to code comparisons, code to data comparisons and expert judgements are typically used to estimate uncertainties.

4.235. Uncertainty analysis should be also prepared for the PSA as it is a key component. The identification and analysis of uncertainties is a fundamental strength of the PSA. Uncertainties are also present in the deterministic analysis, but they are not commonly acknowledged or analysed. Rather, conservatism is deliberately used in an attempt to account for uncertainty. The degree of uncertainty in deterministic analyses is not uniform, however, and can lead to uneven analysis. The strength of the PSA methodology is that it complements the deterministic approach and allows full expression of uncertainties. For such a case, uncertainties should also reflect ranges of the initiating event probability and component failure probability.

ASSESSMENT OF THE COMPUTER CODES USED

4.236. The safety analysis uses a large number of computer codes. These typically include:

- Radiological analysis codes to estimate the doses to workers,
- Neutron physics codes which model the behaviour of the reactor core,
- Fuel behaviour codes which model the behaviour of the fuel elements during normal operation and following accidents,
- Thermal-hydraulic codes which model the behaviour of the reactor core and the associated coolant systems during normal operation and following accidents,
- Thermal-hydraulic codes which model the behaviour of containment pressure and temperature after a LOCA or secondary line break,

— Structural codes which model stress–strain behaviour of components and structures under loads and load combinations,
— Severe accident analysis codes which model the progression of an accident sequence from core damage through to containment failure,
— Radiological analysis codes which model the transport of radioactive material within and from the plant to determine its effect on workers and members of the public,
— Probabilistic codes which develop a logical model to identify the accident sequences which could occur following PIEs and estimate their frequencies.

4.237. Many of the computer codes now being developed combine several of the above models in the same code.

4.238. All the computer codes used in the safety analysis should be validated and verified. The methods used in the computer code for the calculation should be adequate for the purpose and the controlling physical and logical equations should be correctly implemented into computer code.

4.239. Regarding the computer codes, it should be confirmed that:

— The physical models used to describe the processes are justified together with the associated simplifying assumptions.
— The correlations used to represent physical processes are justified and their limits of applicability identified.
— The limits of application of the code have been identified. This is important when the calculational method is only designed to model physical processes over a defined range and should not be applied outside this range.
— The numerical methods used would provide a sufficiently accurate solution.
— A systematic approach has been used for the design, coding, testing and documentation of the computer code.
— The source coding has been assessed relative to the code specification. (It is recognized that this may not be achievable for very large codes.)

4.240. Regarding the outputs of the computer codes, it should be confirmed that the predictions of the code have been compared with:

— Experimental data for the significant phenomena modelled. This would typically include a comparison against ‘separate effects’ and larger ‘integral’ experiments.
— Plant data, including tests carried out during commissioning or startup and operational occurrences or accidents.

— Other codes which have been developed independently and use different methods. This is particularly important in modelling severe accident phenomena.
— Standard problems and/or numerical benchmarks with sufficiently accurate results being obtained.

4.241. Each code should be validated for each application made in the safety analysis.

4.242. It is noted that for some of the codes which have been developed, a validation package already exists. However, this may be incomplete for codes that are being developed and for codes which model some of the severe accident phenomena which are not so well understood.

4.243. Regarding the users of the code, it should be ensured that:

— The users have received adequate training and that they understand the code,
— The users are sufficiently experienced in the use of the code and fully understand its uses and limitations,
— The users have adequate guidance in the use of the code,
— The users (whenever possible) have used the code on standard problems before starting the safety analysis work.

4.244. Regarding the use of the computer code, it should be confirmed that:

— The nodalization and the plant models provide a good representation of the behaviour of the plant,
— The input data are correct,
— The output of the code is understood and used correctly.

5. INDEPENDENT VERIFICATION

5.1. The purpose of the independent safety verification is to establish that the safety assessment satisfies the applicable safety requirements. While the verification may be conveniently subdivided in phases to be performed at various significant stages of the design, a final independent verification of the safety assessment should always be performed after the design is complete.

5.2. The conduct of the independent verification may largely follow the methods of the safety assessment discussed in Sections 2–4 of this Safety Guide. However, the scope of the independent verification could be narrower than the safety assessment since it would focus on the most significant safety issues and requirements, rather than all of them.

5.3. Independent verifications are performed separately both by the plant owner-operator, who generally conducts an independent review of the design organization, and by the regulatory body.

5.4. The owner is fully responsible for his independent verification even if parts of it are entrusted to separate organizations.

5.5. Independent design assessment activities are a part of the overall QA programme and are a prime concern during nuclear power plant design. However, as represented in Fig. 1, the independent verification is considered as a separate additional check to ensure a safe and proper design. The group performing the independent verification may take into account any QA reviews which have previously been conducted in determining the extent and scope of its verification.

5.6. As previously mentioned, this Safety Guide primarily addresses design verification activities performed before the beginning of plant construction and focuses on activities performed by the design organization or on its behalf. It may, however, be applied by analogy to other subsequent verification activities.

5.7. The verification of the safety assessment should be carried out by experts who are familiar with current developments in reactor technology and safety analysis. The reviewers should be independent of the designers of the plant.

5.8. The reviewers performing the independent verification should verify that the process of the safety assessment is adequate. They should be provided with all the relevant design documents including calculational models, data and assumptions. In addition, the reviewers should be provided full access to the plant site in order to walk down critical areas to confirm that the safety assessment adequately represents the actual physical facility.

5.9. A sample, non-exhaustive, list of items subject to review is as follows:

— Selection of PIEs,
— Applied industrial standards,
— Relevant safety and radiation protection assessment issues,

— The worst initial plant condition assumed for the initiating event to bound all similar cases,
— Combination of individual events and their failure effects,
— Identification of consequential failures,
— Assumed operation of safety and non-safety systems and components during the course of events,
— Assumed operator action,
— Selection of validated computer codes applicable to the particular analysis,
— Reliability data and their applicability to the particular analysis,
— Construction of event trees and fault trees in PSA,
— Common cause failures,
— Use of an atmospheric dispersion model of each particular form of radioactive release,
— Uncertainty analysis,
— Adequacy of the process of the analysis for events beyond design basis.

5.10. An independent check of selected computer calculations should be conducted to ensure that the analysis is correct. If sufficient verification and validation of the original code have not been performed, then an alternative code should be used to verify its accuracy.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[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, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standard Series No. NS-G-2.2, IAEA, Vienna (2000).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes in Nuclear Power Plants: A Guidebook, Technical Reports Series No. 368, IAEA, Vienna (1994).

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Safety Series No. 50-P-8, IAEA, Vienna (1995).

[12] OECD NUCLEAR ENERGY AGENCY, Level 2 PSA Methodology and Severe Accident Management, OECD/GD(97)198, OECD, Paris (1997).

[13] UNITED STATES NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, Rep. NUREG-1150, Division of Systems Research, USNRC, Washington, DC (1990).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA, Vienna (1996).

[15] 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).

CONTRIBUTORS TO DRAFTING AND REVIEW

Couch, D.P.	Pacific Northwest National Laboratory, United States of America
Del Nero, G.	Agenzia Nazionale per la Protezione dell'Ambiente, Italy
De Munk, P.	Ministry of Social Affairs, Nuclear Safety Department, Netherlands
Fil, N.	OKB Gidropress, Russian Federation
Foskolos, K.	Paul Scherrer Institut, Switzerland
Gasparini, M.	International Atomic Energy Agency
Misak, J.	International Atomic Energy Agency
Kabanov, L.	International Nuclear Safety Centre of Russian Minatom, Russian Federation
Krishnan, V.S.	Atomic Energy of Canada Limited, Canada
Krugmann, U.	Siemens AG/KWU Erlangen, Germany
Lee, J.H.	Korea Institute of Nuclear Safety, Republic of Korea
Omoto, A.	Tokyo Electric Power Company, Japan
Petrangeli, G.	Agenzia Nazionale per la Protezione dell'Ambiente, Italy
Rohar, S.	Nuclear Regulatory Authority, Slovakia
Shepherd, C.H.	Her Majesty's Nuclear Installation Inspectorate, United Kingdom
Simon, M.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Vidard, M.	Electricité de France, France
Vine, G.	Electric Power Research Institute, United States of America
Wilson, J.N.	Nuclear Regulatory Commission, United States of America

BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS

Nuclear Safety Standards Committee

Argentina: Sajaroff, P.; *Belgium*: Govaerts, P. (Chair); *Brazil*: Salati de Almeida, I.P.; *Canada*: Malek, I.; *China:* Zhao, Y.; *Finland:* Reiman, L.; *France*: Saint Raymond, P.; *Germany*: Wendling, R.D.; *India*: Venkat Raj, V.; *Italy*: Del Nero, G.; *Japan*: Hirano, M.; *Republic of Korea*: Lee, J.-I.; *Mexico*: Delgado Guardado, J.L.; *Netherlands*: de Munk, P.; *Pakistan*: Hashimi, J.A.; *Russian Federation*: Baklushin, R.P.; *Spain*: Lequerica, I.; *Sweden*: Jende, E.; *Switzerland*: Aberli, W.; *Ukraine*: Mikolaichuk, O.; *United Kingdom*: Hall, A.; *United States of America*: Murphy, J; *European Commission*: Gómez-Gómez, J.A.; *IAEA*: Hughes, P. (Co-ordinator); *International Organization for Standardization*: d'Ardenne, W.; *OECD Nuclear Energy Agency*: Royen, J.

Commission for Safety Standards

Argentina: D'Amato, E.; *Brazil*: Caubit da Silva, A.; *Canada*: Bishop, A., Duncan, R.M.; *China*: Zhao, C.; *France*: Lacoste, A.-C., Gauvain, J.; *Germany*: Renneberg, W., Wendling, R.D.; *India*: Sukhatme, S.P.; *Japan*: Suda, N.; *Republic of Korea*: Kim, S.-J.; *Russian Federation*: Vishnevskiy, Y.G.; *Spain*: Martin Marquínez, A.; *Sweden*: Holm, L.-E.; *Switzerland*: Jeschki, W.; *Ukraine*: Smyshlayaev, O.Y.; *United Kingdom*: Williams, L.G. (Chair), Pape, R.; *United States of America*: Travers, W.D.; *IAEA*: Karbassioun, A. (Co-ordinator); *International Commission on Radiological Protection*: Clarke, R.H.; *OECD Nuclear Energy Agency*: Shimomura, K.