IAEA
SAFETY
STANDARDS
SERIES

Safety of Nuclear Power Plants: Design

REQUIREMENTS

No. NS-R-1

INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

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.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www.iaea.org/ns/coordinet

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

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

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related sales publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series** and the **INSAG Series**. The IAEA also issues reports on radiological accidents and other special sales publications. Unpriced safety related publications are issued in the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**.

SAFETY OF NUCLEAR POWER PLANTS: DESIGN

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
BANGLADESH
BELARUS
BELGIUM
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BRAZIL
BULGARIA
BURKINA FASO
CAMBODIA
CAMEROON
CANADA
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
September 2000
STI/PUB/1099

SAFETY STANDARDS SERIES No. NS-R-1

SAFETY OF NUCLEAR POWER PLANTS: DESIGN

SAFETY REQUIREMENTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2000

VIC Library Cataloguing in Publication Data

Safety of nuclear power plants : design : safety requirements. — Vienna : International Atomic Energy Agency, 2000.
p. ; 24 cm. — (Safety standards series, ISSN 1020–525X ; no. NS-R-1)
STI/PUB/1099
ISBN 92–0–101900–9
Includes bibliographical references.

1. Nuclear power plants—Safety measures. 2. Nuclear power plants—Design and construction—Safety measures. I. International Atomic Energy Agency. II. Series.

VICL 00–00251

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 advisory bodies oversee the development of safety standards: the Advisory Commission for Safety Standards (ACSS); the Nuclear Safety Standards Advisory Committee (NUSSAC); the Radiation Safety Standards Advisory Committee (RASSAC); the Transport Safety Standards Advisory Committee (TRANSSAC); and the Waste Safety Standards Advisory Committee (WASSAC). 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 by experts 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.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The present publication supersedes the Code on the Safety of Nuclear Power Plants: Design (Safety Series No. 50-C-D (Rev. 1), issued in 1988). It takes account of developments relating to the safety of nuclear power plants since the Code on Design was last revised. These developments include the issuing of the Safety Fundamentals publication, The Safety of Nuclear Installations [1], and the present revision of various safety standards and other publications relating to safety. Requirements for nuclear safety are intended to ensure adequate protection of site personnel, the public and the environment from the effects of ionizing radiation arising from nuclear power plants. It is recognized that technology and scientific knowledge advance, and nuclear safety and what is considered adequate protection are not static entities. Safety requirements change with these developments and this publication reflects the present consensus.

OBJECTIVE

1.2. This Safety Requirements publication takes account of the developments in safety requirements by, for example, including the consideration of severe accidents in the design process. Other topics that have been given more detailed attention include management of safety, design management, plant ageing and wearing out effects, computer based safety systems, external and internal hazards, human factors, feedback of operational experience, and safety assessment and verification.

1.3. This publication establishes safety requirements that define the elements necessary to ensure nuclear safety. These requirements are applicable to safety functions and the associated structures, systems and components, as well as to procedures important to safety in nuclear power plants. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). It is recognized that in the case of other reactor types, including innovative developments in future systems, some of the requirements may not be applicable, or may need some judgement in their interpretation. Various Safety Guides will provide guidance in the interpretation and implementation of these requirements.

1.4. This publication is intended for use by organizations designing, manufacturing, constructing and operating nuclear power plants as well as by regulatory bodies.

SCOPE

1.5. This publication establishes design requirements for structures, systems and components important to safety that must be met for safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardize safety. It also establishes requirements for a comprehensive safety assessment, which is carried out in order to identify the potential hazards that may arise from the operation of the plant, under the various plant states (operational states and accident conditions). The safety assessment process includes the complementary techniques of deterministic safety analysis and probabilistic safety analysis. These analyses necessitate consideration of postulated initiating events (PIEs), which include many factors that, singly or in combination, may affect safety and which may:

— originate in the operation of the nuclear power plant itself;
— be caused by human action;
— be directly related to the nuclear power plant and its environment.

1.6. This publication also addresses events that are very unlikely to occur, such as severe accidents that may result in major radioactive releases, and for which it may be appropriate and practicable to provide preventive or mitigatory features in the design.

1.7. This publication does not address:

— external natural or human induced events that are extremely unlikely (such as the impact of a meteorite or an artificial satellite);
— conventional industrial accidents that under no circumstances could affect the safety of the nuclear power plant; or
— non-radiological effects arising from the operation of nuclear power plants, which may be subject to separate national regulatory requirements.

STRUCTURE

1.8. This Safety Requirements publication follows the relationship between principles and objectives for safety, and safety requirements and criteria. Section 2 elaborates on the safety principles, objectives and concepts which form the basis for deriving the

safety requirements that must be met in the design of the plant. The safety objectives (in italics in Section 2) are reproduced from the Safety Fundamentals publication, The Safety of Nuclear Installations [1]. Section 3 covers the principal requirements to be applied by the design organization in the management of the design process, and also requirements for safety assessment, for quality assurance and for the use of proven engineering practices and operational experience. Section 4 provides the principal and more general technical requirements for defence in depth and radiation protection. Section 5 provides general plant design requirements which supplement the principal requirements to ensure that the safety objectives are met. Section 6 provides design requirements applicable to specific plant systems, such as the reactor core, coolant systems and containment systems. Appendix I elaborates on the definition and application of the concept of a postulated initiating event. Appendix II discusses the application of redundancy, diversity and independence as measures to enhance reliability and to protect against common cause failures. The Annex elaborates on safety functions for reactors.

2. SAFETY OBJECTIVES AND CONCEPTS

SAFETY OBJECTIVES

2.1. The Safety Fundamentals publication, The Safety of Nuclear Installations [1], presents three fundamental safety objectives, upon the basis of which the requirements for minimizing the risks associated with nuclear power plants are derived. The following paras 2.2–2.6 are reproduced directly from The Safety of Nuclear Installations, paras 203–207.

2.2. **"General Nuclear Safety Objective:** *To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.*

2.3. "This General Nuclear Safety Objective is supported by two complementary Safety Objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionizing radiation.

2.4. **"Radiation Protection Objective:** *To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as*

reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.

2.5. **"Technical Safety Objective:** *To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low.*

2.6. "Safety Objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, the Radiation Protection Objective does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards."

2.7. In order to achieve these three safety objectives, in the design of a nuclear power plant, a comprehensive safety analysis is carried out to identify all sources of exposure and to evaluate radiation doses that could be received by workers at the installation and the public, as well as potential effects on the environment (see para. 4.9). The safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) event sequences that may lead to a severe accident. On the basis of this analysis, the robustness of the engineering design in withstanding postulated initiating events and accidents can be established, the effectiveness of the safety systems and safety related items or systems can be demonstrated, and requirements for emergency response can be established.

2.8. Although measures are taken to control radiation exposure in all operational states to levels as low as reasonably achievable (ALARA) and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation, there is a residual probability that an accident may happen. Measures are therefore taken to ensure that the radiological consequences are mitigated. Such measures include: engineered safety features; on-site accident management procedures established by the operating organization; and possibly off-site intervention measures established by appropriate authorities in order to mitigate radiation exposure if an accident has occurred. The design for safety of a nuclear power plant applies the principle that plant states that could result in high radiation doses or radioactive

releases are of very low probability (likelihood) of occurrence, and plant states with significant probability (likelihood) of occurrence have only minor or no potential radiological consequences. An essential objective is that the need for external intervention measures may be limited or even eliminated in technical terms, although such measures may still be required by national authorities.

THE CONCEPT OF DEFENCE IN DEPTH

2.9. The concept of defence in depth, as applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. The concept has been further elaborated since 1988 [2, 3]. Application of the concept of defence in depth throughout design and operation provides a graded protection against a wide variety of transients, anticipated operational occurrences and accidents, including those resulting from equipment failure or human action within the plant, and events that originate outside the plant.

2.10. Application of the concept of defence in depth in the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.

(1) The aim of the first level of defence is to prevent deviations from normal operation, and to prevent system failures. This leads to the requirement that the plant be soundly and conservatively designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices, such as the application of redundancy, independence and diversity. To meet this objective, careful attention is paid to the selection of appropriate design codes and materials, and to the control of fabrication of components and of plant construction. Design options that can contribute to reducing the potential for internal hazards (e.g. controlling the response to a PIE), to reducing the consequences of a given PIE, or to reducing the likely release source term following an accident sequence contribute at this level of defence. Attention is also paid to the procedures involved in the design, fabrication, construction and in-service plant inspection, maintenance and testing, to the ease of access for these activities, to the way the plant is operated and to how operational experience is utilized. This whole process is supported by a detailed analysis which determines the operational and maintenance requirements for the plant.

(2) The aim of the second level of defence is to detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions. This is in recognition of the fact that some PIEs are likely to occur over the service lifetime of a nuclear power plant, despite the care taken to prevent them. This level necessitates the provision of specific systems as determined in the safety analysis and the definition of operating procedures to prevent or minimize damage from such PIEs.

(3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or PIEs may not be arrested by a preceding level and a more serious event may develop. These unlikely events are anticipated in the design basis for the plant, and inherent safety features, fail-safe design, additional equipment and procedures are provided to control their consequences and to achieve stable and acceptable plant states following such events. This leads to the requirement that engineered safety features be provided that are capable of leading the plant first to a controlled state, and subsequently to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material.

(4) The aim of the fourth level of defence is to address severe accidents in which the design basis may be exceeded and to ensure that radioactive releases are kept as low as practicable. The most important objective of this level is the protection of the confinement function. This may be achieved by complementary measures and procedures to prevent accident progression, and by mitigation of the consequences of selected severe accidents, in addition to accident management procedures. The protection provided by the confinement may be demonstrated using best estimate methods.

(5) The fifth and final level of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials that may result from accident conditions. This requires the provision of an adequately equipped emergency control centre, and plans for the on-site and off-site emergency response.

2.11. A relevant aspect of the implementation of defence in depth is the provision in the design of a series of physical barriers to confine the radioactive material at specified locations. The number of physical barriers that will be necessary will depend on the potential internal and external hazards, and the potential consequences of failures. The barriers may, typically for water cooled reactors, be in the form of the fuel matrix, the fuel cladding, the reactor coolant system pressure boundary and the containment.

3. REQUIREMENTS FOR MANAGEMENT OF SAFETY

RESPONSIBILITIES IN MANAGEMENT

3.1. The operating organization has overall responsibility for safety. However, all organizations engaged in activities important to safety have a responsibility to ensure that safety matters are given the highest priority. The design organization shall ensure that the installation is designed to meet the requirements of the operating organization, including any standardized utility requirements; that it takes account of the current state of the art for safety; that it is in accordance with the design specifications and safety analysis; that it satisfies national regulatory requirements; that it fulfils the requirements of an effective quality assurance programme; and that the safety of any design change is properly considered. Thus, the design organization shall:

(1) have a clear division of responsibilities with corresponding lines of authority and communication;
(2) ensure that it has sufficient technically qualified and appropriately trained staff at all levels;
(3) establish clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, constructors and contractors as appropriate;
(4) develop and strictly adhere to sound procedures;
(5) review, monitor and audit all safety related design matters on a regular basis;
(6) ensure that a safety culture is maintained.

MANAGEMENT OF DESIGN

3.2. The design management for a nuclear power plant shall ensure that the structures, systems and components important to safety have the appropriate characteristics, specifications and material composition so that the safety functions can be performed and the plant can operate safely with the necessary reliability for the full duration of its design life, with accident prevention and protection of site personnel, the public and the environment as prime objectives.

3.3. The design management shall ensure that the requirements of the operating organization are met and that due account is taken of the human capabilities and limitations of personnel. The design organization shall supply adequate safety design information to ensure safe operation and maintenance of the plant and to allow subsequent plant modifications to be made, and recommended practices for

incorporation into the plant administrative and operational procedures (i.e. operational limits and conditions).

3.4. The design management shall take account of the results of the deterministic and complementary probabilistic safety analyses, so that an iterative process takes place by means of which it shall be ensured that due consideration has been given to the prevention of accidents and mitigation of their consequences.

3.5. The design management shall ensure that the generation of radioactive waste is kept to the minimum practicable, in terms of both activity and volume, by appropriate design measures and operational and decommissioning practices.

PROVEN ENGINEERING PRACTICES

3.6. Wherever possible, structures, systems and components important to safety shall be designed according to the latest or currently applicable approved standards; shall be of a design proven in previous equivalent applications; and shall be selected to be consistent with the plant reliability goals necessary for safety. Where codes and standards are used as design rules, they shall be identified and evaluated to determine their applicability, adequacy and sufficiency and shall be supplemented or modified as necessary to ensure that the final quality is commensurate with the necessary safety function.

3.7. Where an unproven design or feature is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by appropriate supporting research programmes, or by examination of operational experience from other relevant applications. The development shall also be adequately tested before being brought into service and shall be monitored in service, to verify that the expected behaviour is achieved.

3.8. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes (e.g. failure to trip when necessary). Where failure of a structure, system or component has to be expected and accommodated by the design, preference shall be given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.

OPERATIONAL EXPERIENCE AND SAFETY RESEARCH

3.9. The design shall take due account of relevant operational experience that has been gained in operating plants and of the results of relevant research programmes.

SAFETY ASSESSMENT

3.10. A comprehensive safety assessment shall be carried out to confirm that the design as delivered for fabrication, as for construction and as built meets the safety requirements set out at the beginning of the design process.

3.11. The safety assessment shall be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in the scope and level of detail as the design programme progresses.

3.12. The basis for the safety assessment shall be data derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice.

INDEPENDENT VERIFICATION OF THE SAFETY ASSESSMENT

3.13. 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.

QUALITY ASSURANCE[1]

3.14. A quality assurance programme that describes the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented. This programme shall be supported by more detailed plans for each structure, system and component so that the quality of the design is ensured at all times.

3.15. Design, including subsequent changes or safety improvements, shall be carried out in accordance with established procedures that call on appropriate engineering codes and standards, and shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled.

3.16. The adequacy of design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval shall be completed before implementation of the detailed design.

[1] For further guidance, see Ref. [4].

4. PRINCIPAL TECHNICAL REQUIREMENTS

REQUIREMENTS FOR DEFENCE IN DEPTH

4.1. In the design process, defence in depth shall be incorporated as described in Section 2. The design therefore:

(1) shall provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment;
(2) shall be conservative, and the construction shall be of high quality, so as to provide confidence that plant failures and deviations from normal operations are minimized and accidents prevented;
(3) shall provide for control of the plant behaviour during and following a PIE, using inherent and engineered features, i.e. uncontrolled transients shall be minimized or excluded by design to the extent possible;
(4) shall provide for supplementing control of the plant, by the use of automatic activation of safety systems in order to minimize operator actions in the early phase of PIEs and by operator actions;
(5) shall provide for equipment and procedures to control the course and limit the consequences of accidents as far as practicable;
(6) shall provide multiple means for ensuring that each of the fundamental safety functions, i.e. control of the reactivity, heat removal and the confinement of radioactive materials, is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any PIEs.

4.2. To ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable:

(1) challenges to the integrity of physical barriers;
(2) failure of a barrier when challenged;
(3) failure of a barrier as a consequence of failure of another barrier.

4.3. The design shall be such that the first, or at most the second, level of defence is capable of preventing escalation to accident conditions for all but the most improbable PIEs.

4.4. The design shall take into account the fact that the existence of multiple levels of defence is not a sufficient basis for continued power operation in the absence of one level of defence. All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.

SAFETY FUNCTIONS

4.5. The objective of the safety approach shall be: to provide adequate means to maintain the plant in a normal operational state; to ensure the proper short term response immediately following a PIE; and to facilitate the management of the plant in and following any design basis accident, and in those selected accident conditions beyond the design basis accidents.

4.6. To ensure safety, the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and, to the extent practicable, on the occurrence of those selected accident conditions that are beyond the design basis accidents:

(1) control of the reactivity;
(2) removal of heat from the core; and
(3) confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

An example of a detailed subdivision of these three fundamental safety functions is given in the Annex.

4.7. A systematic approach shall be followed to identify the structures, systems and components that are necessary to fulfil the safety functions at the various times following a PIE.

ACCIDENT PREVENTION AND PLANT SAFETY CHARACTERISTICS

4.8. The plant design shall be such that its sensitivity to PIEs is minimized. The expected plant response to any PIE shall be those of the following that can reasonably be achieved (in order of importance):

(1) a PIE produces no significant safety related effect or produces only a change in the plant towards a safe condition by inherent characteristics; or
(2) following a PIE, the plant is rendered safe by passive safety features or by the action of safety systems that are continuously operating in the state necessary to control the PIE; or
(3) following a PIE, the plant is rendered safe by the action of safety systems that need to be brought into service in response to the PIE; or
(4) following a PIE, the plant is rendered safe by specified procedural actions.

RADIATION PROTECTION AND ACCEPTANCE CRITERIA

4.9. In order to achieve the three safety objectives given in paras 2.2–2.5 in the design of a nuclear installation, all actual and potential sources of radiation shall be identified and properly considered, and provision shall be made to ensure that sources are kept under strict technical and administrative control.

4.10. Measures shall be provided to ensure that the radiation protection and technical safety objectives as given in paras 2.4 and 2.5 are achieved, and that radiation doses to the public and to site personnel in all operational states, including maintenance and decommissioning, do not exceed prescribed limits and are as low as reasonably achievable.

4.11. The design shall have as an objective the prevention or, if this fails, the mitigation of radiation exposures resulting from design basis accidents and selected severe accidents. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed acceptable limits and are as low as reasonably achievable.

4.12. Plant states that could potentially result in high radiation doses or radioactive releases shall be restricted to a very low likelihood of occurrence, and it shall be ensured that the potential radiological consequences of plant states with a significant likelihood of occurrence shall be only minor. Radiological acceptance criteria for the design of a nuclear power plant shall be specified on the basis of these requirements.

4.13. There is usually a limited number of sets of radiological acceptance criteria, and it is common practice to associate these with categories of plant states. These categories generally include those for normal operation, anticipated operational occurrences, design basis accidents and severe accidents. The radiological acceptance criteria for these categories shall, as a minimum level of safety, meet the requirements of the regulatory body.

5. REQUIREMENTS FOR PLANT DESIGN

SAFETY CLASSIFICATION

5.1. All structures, systems and components, including software for instrumentation and control (I&C), that are items important to safety shall be first identified and then

classified on the basis of their function and significance with regard to safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

5.2. The method for classifying the safety significance of a structure, system or component shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgement, with account taken of factors such as:

(1) the safety function(s) to be performed by the item;
(2) the consequences of failure to perform its function;
(3) the probability that the item will be called upon to perform a safety function;
(4) the time following a PIE at which, or the period throughout which, it will be called upon to operate.

5.3. Appropriately designed interfaces shall be provided between structures, systems and components of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class.

GENERAL DESIGN BASIS

5.4. The design basis shall specify the necessary capabilities of the plant to cope with a specified range of operational states and design basis accidents within the defined radiological protection requirements. The design basis shall include the specification for normal operation, plant states created by the PIEs, the safety classification, important assumptions and, in some cases, the particular methods of analysis.

5.5. Conservative design measures shall be applied and sound engineering practices shall be adhered to in the design bases for normal operation, anticipated operational occurrences and design basis accidents so as to provide a high degree of assurance that no significant damage will occur to the reactor core and that radiation doses will remain within prescribed limits and will be ALARA.

5.6. In addition to the design basis, the performance of the plant in specified accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design. The assumptions and methods used for these evaluations may be on a best estimate basis.

Categories of plant states

5.7. The plant states shall be identified and grouped into a limited number of categories according to their probability of occurrence. The categories typically cover normal operation, anticipated operational occurrences, design basis accidents and severe accidents. Acceptance criteria shall be assigned to each category that take account of the requirement that frequent PIEs shall have only minor or no radiological consequences, and that events that may result in severe consequences shall be of very low probability.

Postulated initiating events

5.8. In the design of the plant, it shall be recognized that challenges to all levels of defence in depth may occur and design measures shall be provided to ensure that the necessary safety functions are accomplished and the safety objectives can be met. These challenges stem from the PIEs, which are selected on the basis of deterministic or probabilistic techniques or a combination of the two. Independent events, each having a low probability, are normally not anticipated in the design to occur simultaneously.

Internal events

5.9. An analysis of the PIEs (see Appendix I) shall be made to establish all those internal events which may affect the safety of the plant. These events may include equipment failures or maloperation.

Fires and explosions

5.10. Structures, systems and components important to safety shall be designed and located so as to minimize, consistent with other safety requirements, the probabilities and effects of fires and explosions caused by external or internal events. The capability for shutdown, residual heat removal, confinement of radioactive material and monitoring of the state of the plant shall be maintained. These requirements shall be met by suitable incorporation of redundant parts, diverse systems, physical separation and design for fail-safe operation such that the following objectives are achieved:

(1) to prevent fires from starting;
(2) to detect and extinguish quickly those fires which do start, thus limiting the damage;

(3) to prevent the spread of those fires which have not been extinguished, thus minimizing their effects on essential plant functions.

5.11. A fire hazard analysis of the plant shall be carried out to determine the necessary rating of the fire barriers, and fire detection and fire fighting systems of the necessary capability shall be provided.

5.12. Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located so as to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety, and does not simultaneously affect redundant safety groups, thereby rendering ineffective the measures taken to comply with the 'single failure' criterion.

5.13. Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, particularly in locations such as the containment and the control room.

Other internal hazards

5.14. The potential for internal hazards such as flooding, missile generation, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site shall be taken into account in the design of the plant. Appropriate preventive and mitigatory measures shall be provided to ensure that nuclear safety is not compromised. Some external events may initiate internal fires or floods and may lead to the generation of missiles. Such interaction of external and internal events shall also be considered in the design, where appropriate.

5.15. If two fluid systems that are operating at different pressures are interconnected, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded, on the assumption that a single failure occurs.

External events

5.16. The design basis natural and human induced external events shall be determined for the proposed combination of site and plant. All those events with which significant radiological risk may be associated shall be considered. A combination of deterministic and probabilistic methods shall be used to select a subset of external events which the plant is designed to withstand, and from which the design bases are determined.

5.17. Natural external events which shall be considered include those which have been identified in site characterization, such as earthquakes, floods, high winds, tornadoes, tsunami (tidal waves) and extreme meteorological conditions. Human induced external events that shall be considered include those that have been identified in site characterization and for which design bases have been derived. The list of these events shall be reassessed for completeness at an early stage of the design process.

Site related characteristics[2]

5.18. In determining the design basis of a nuclear power plant, various interactions between the plant and the environment, including such factors as population, meteorology, hydrology, geology and seismology, shall be taken into account. The availability of off-site services upon which the safety of the plant and protection of the public may depend, such as the electricity supply and fire fighting services, shall also be taken into account.

5.19. Projects for nuclear power plants to be sited in tropical, polar, arid or volcanic areas shall be assessed with a view to identifying special design features which may be necessary as a result of the characteristics of the site.

Combinations of events

5.20. Where combinations of randomly occurring individual events could credibly lead to anticipated operational occurrences or accident conditions, they shall be considered in the design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.

Design rules

5.21. The engineering design rules for structures, systems and components shall be specified and shall comply with the appropriate accepted national standard engineering practices (see para. 3.6), or those standards or practices already used internationally or established in another country and whose use is applicable and also accepted by the national regulatory body.

[2] For further guidance, see Ref. [5].

5.22. The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events.

Design limits

5.23. A set of design limits consistent with the key physical parameters for each structure, system or component shall be specified for operational states and design basis accidents.

Operational states

5.24. The plant shall be designed to operate safely within a defined range of parameters (for example, of pressure, temperature, power), and a minimum set of specified support features for safety systems (for example, auxiliary feedwater capacity and an emergency electrical power supply) shall be assumed to be available. The design shall be such that the response of the plant to a wide range of anticipated operational occurrences will allow safe operation or shutdown, if necessary, without the necessity of invoking provisions beyond the first, or at the most the second, level of defence in depth.

5.25. The potential for accidents to occur in low power and shutdown states, such as startup, refuelling and maintenance, when the availability of safety systems may be reduced, shall be addressed in the design, and appropriate limitations on the unavailability of safety systems shall be specified.

5.26. The design process shall establish a set of requirements and limitations for safe operation, including:

(1) safety system settings;
(2) control system and procedural constraints on process variables and other important parameters;
(3) requirements for maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, with the ALARA principle taken into consideration;
(4) clearly defined operational configurations, including operational restrictions in the event of safety system outages.

These requirements and limitations shall be a basis for the establishment of operational limits and conditions under which the operating organization will be authorized to operate the plant.

Design basis accidents

5.27. A set of design basis accidents shall be derived from the listing of PIEs (see Appendix I) for the purpose of setting the boundary conditions according to which the structures, systems and components important to safety shall be designed.

5.28. Where prompt and reliable action is necessary in response to a PIE, provision shall be made to initiate the necessary actions of safety systems automatically, in order to prevent progression to a more severe condition that may threaten the next barrier. Where prompt action is not necessary, manual initiation of systems or other operator actions may be permitted, provided that the need for the action be revealed in sufficient time and that adequate procedures (such as administrative, operational and emergency procedures) be defined to ensure the reliability of such actions.

5.29. The operator actions that may be necessary to diagnose the state of the plant and to put it into a stable long term shutdown condition in a timely manner shall be taken into account and facilitated by the provision of adequate instrumentation to monitor the plant status and controls for manual operation of equipment.

5.30. Any equipment necessary in manual response and recovery processes shall be placed at the most suitable location to ensure its ready availability at the time of need and to allow human access in the anticipated environmental conditions.

Severe accidents

5.31. Certain very low probability plant states that are beyond design basis accident conditions and which may arise owing to multiple failures of safety systems leading to significant core degradation may jeopardize the integrity of many or all of the barriers to the release of radioactive material. These event sequences are called severe accidents. Consideration shall be given to these severe accident sequences, using a combination of engineering judgement and probabilistic methods, to determine those sequences for which reasonably practicable preventive or mitigatory measures can be identified. Acceptable measures need not involve the application of conservative engineering practices used in setting and evaluating design basis accidents, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria. On the basis of operational experience, relevant safety analysis and results from safety research, design activities for addressing severe accidents shall take into account the following:

(1) Important event sequences that may lead to a severe accident shall be identified using a combination of probabilistic methods, deterministic methods and sound engineering judgement.

(2) These event sequences shall then be reviewed against a set of criteria aimed at determining which severe accidents shall be addressed in the design.
(3) Potential design changes or procedural changes that could either reduce the likelihood of these selected events, or mitigate their consequences should these selected events occur, shall be evaluated and shall be implemented if reasonably practicable.
(4) Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and anticipated operational states, and the use of additional temporary systems, to return the plant to a controlled state and/or to mitigate the consequences of a severe accident, provided that it can be shown that the systems are able to function in the environmental conditions to be expected.
(5) For multiunit plants, consideration shall be given to the use of available means and/or support from other units, provided that the safe operation of the other units is not compromised.
(6) Accident management procedures shall be established, taking into account representative and dominant severe accident scenarios.

DESIGN FOR RELIABILITY OF STRUCTURES, SYSTEMS AND COMPONENTS

5.32. Structures, systems and components important to safety shall be designed to be capable of withstanding all identified PIEs (see Appendix I) with sufficient reliability.

Common cause failures

5.33. The potential for common cause failures of items important to safety shall be considered to determine where the principles of diversity, redundancy and independence should be applied to achieve the necessary reliability.

Single failure criterion

5.34. The single failure criterion shall be applied to each safety group incorporated in the plant design.

5.35. To test compliance of the plant with the single failure criterion, the pertinent safety group shall be analysed in the following way. A single failure (and all its consequential failures) shall be assumed in turn to occur for each element of the safety group until all

possible failures have been analysed. The analyses of each pertinent safety group shall then be conducted in turn until all safety groups and all failures have been considered. (In this Safety Requirements publication, safety functions, or systems contributing to performing those safety functions, for which redundancy is necessary to achieve the necessary reliability have been identified by the statement 'on the assumption of a single failure'.) The assumption of a single failure in that system is part of the process described. At no point in the single failure analysis is more than one random failure assumed to occur.

5.36. Spurious action shall be considered as one mode of failure when applying the concept to a safety group or system.

5.37. Compliance with the criterion shall be considered to have been achieved when each safety group has been shown to perform its safety function when the above analyses are applied, under the following conditions:

(1) any potentially harmful consequences of the PIE for the safety group are assumed to occur; and
(2) the worst permissible configuration of safety systems performing the necessary safety function is assumed, with account taken of maintenance, testing, inspection and repair, and allowable equipment outage times.

5.38. Non-compliance with the single failure criterion shall be exceptional, and shall be clearly justified in the safety analysis.

5.39. In the single failure analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.

Fail-safe design

5.40. The principle of fail-safe design shall be considered and incorporated into the design of systems and components important to safety for the plant as appropriate: if a system or component fails, plant systems shall be designed to pass into a safe state with no necessity for any action to be initiated.

Auxiliary services

5.41. Auxiliary services that support equipment forming part of a system important to safety shall be considered part of that system and shall be classified accordingly. Their reliability, redundancy, diversity and independence and the provision of features for isolation and for testing of functional capability shall be commensurate with the reliability of the system that is supported. Auxiliary services necessary to maintain the plant in a safe state may include the supply of electricity, cooling water and compressed air or other gases, and means of lubrication.

Equipment outages

5.42. The design shall be such as to ensure, by the application of measures such as increased redundancy, that reasonable on-line maintenance and testing of systems important to safety can be conducted without the necessity to shut down the plant. Equipment outages, including unavailability of systems or components due to failure, shall be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system shall be included in this consideration in order to ensure that the safety function can still be achieved with the necessary reliability. The time allowed for equipment outages and the actions to be taken shall be analysed and defined for each case before the start of plant operation and included in the plant operating instructions.

PROVISION FOR IN-SERVICE TESTING, MAINTENANCE, REPAIR, INSPECTION AND MONITORING

5.43. Structures, systems and components important to safety, except as described in para. 5.44, shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability over the lifetime of the nuclear power plant to demonstrate that reliability targets are being met. The plant layout shall be such that these activities are facilitated and can be performed to standards commensurate with the importance of the safety functions to be performed, with no significant reduction in system availability and without undue exposure of the site personnel to radiation.

5.44. If the structures, systems and components important to safety cannot be designed to be able to be tested, inspected or monitored to the extent desirable, then the following approach shall be followed:

— other proven alternative and/or indirect methods such as surveillance of reference items or use of verified and validated calculational methods shall be specified; and
— conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.

EQUIPMENT QUALIFICATION

5.45. A qualification procedure shall be adopted to confirm that the items important to safety are capable of meeting, throughout their design operational lives, the demands for performing their functions while being subject to the environmental conditions (of vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity or any likely combination thereof) prevailing at the time of need. The environmental conditions to be considered shall include the variations expected in normal operation, anticipated operational occurrences and design basis accidents. In the qualification programme, consideration shall be given to ageing effects caused by various environmental factors (such as vibration, irradiation and extreme temperature) over the expected lifetime of the equipment. Where the equipment is subject to external natural events and is needed to perform a safety function in or following such an event, the qualification programme shall replicate as far as practicable the conditions imposed on the equipment by the natural phenomenon, either by test or by analysis or by a combination of both.

5.46. In addition, any unusual environmental conditions that can reasonably be anticipated and could arise from specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme. To the extent possible, equipment (such as certain instrumentation) that must operate in a severe accident should be shown, with reasonable confidence, to be capable of achieving the design intent.

AGEING

5.47. Appropriate margins shall be provided in the design for all structures, systems and components important to safety so as to take into account relevant ageing and wear-out mechanisms and potential age related degradation, in order to ensure the capability of the structure, system or component to perform the necessary safety function throughout its design life. Ageing and wear-out effects in all normal operating conditions, testing, maintenance, maintenance outages, and plant states in a PIE and post-PIE shall also be taken into account. Provision shall also be made for

monitoring, testing, sampling and inspection, to assess ageing mechanisms predicted at the design stage and to identify unanticipated behaviour or degradation that may occur in service.

HUMAN FACTORS

Design for optimal operator performance

5.48. The design shall be 'operator friendly' and shall be aimed at limiting the effects of human errors. Attention shall be paid to plant layout and procedures (administrative, operational and emergency), including maintenance and inspection, in order to facilitate the interface between the operating personnel and the plant.

5.49. The working areas and working environment of the site personnel shall be designed according to ergonomic principles.

5.50. Systematic consideration of human factors and the human–machine interface shall be included in the design process at an early stage and shall continue throughout the entire process, to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided.

5.51. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times. Similar provisions shall be made for the supplementary control room.

5.52. Verification and validation of aspects of human factors shall be included at appropriate stages to confirm that the design adequately accommodates all necessary operator actions.

5.53. To assist in the establishment of design criteria for information display and controls, the operator shall be considered to have dual roles: that of a systems manager, including accident management, and that of an equipment operator.

5.54. In the systems manager role, the operator shall be provided with information that permits the following:

(1) the ready assessment of the general state of the plant in whichever condition it is, whether in normal operation, in an anticipated operational occurrence or in an accident condition, and confirmation that the designed automatic safety actions are being carried out; and

(2) the determination of the appropriate operator initiated safety actions to be taken.

5.55. As equipment operator, the operator shall be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the necessary safety actions can be initiated safely.

5.56. The design shall be aimed at promoting the success of operator actions with due regard for the time available for action, the physical environment to be expected and the psychological demands to be made on the operator. The need for intervention by the operator on a short time-scale shall be kept to a minimum. It shall be taken into account in the design that the necessity for such intervention is only acceptable provided that the designer can demonstrate that the operator has sufficient time to make a decision and to act; that the information necessary for the operator to make the decision to act is simply and unambiguously presented; and that following an event the physical environment in the control room or in the supplementary control room and on the access route to that supplementary control room is acceptable.

OTHER DESIGN CONSIDERATIONS

Sharing of structures, systems and components between reactors

5.57. Structures, systems and components important to safety shall generally not be shared between two or more reactors in nuclear power plants. If in exceptional cases such structures, systems and components important to safety are shared between two or more reactors, it shall be demonstrated that all safety requirements are met for all reactors under all operational states (including maintenance) and in design basis accidents. In the event of a severe accident involving one of the reactors, an orderly shutdown, cooling down and removal of residual heat shall be achievable for the other reactor(s).

Systems containing fissile or radioactive materials

5.58. All systems within a nuclear power plant that may contain fissile or radioactive materials shall be designed to ensure adequate safety in operational states and in design basis accidents.

Power plants used for cogeneration, heat generation or desalination

5.59. Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent transport of

radioactive materials from the nuclear plant to the desalination or district heating unit under any condition of normal operation, anticipated operational occurrences, design basis accidents and selected severe accidents.

Transport and packaging for fuel and radioactive waste

5.60. The design shall incorporate appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste. Consideration shall be given to access to facilities and lifting and packaging capabilities.

Escape routes and means of communication

5.61. The nuclear power plant shall be provided with a sufficient number of safe escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other building services essential to the safe use of these routes. The escape routes shall meet the relevant international requirements for radiation zoning and fire protection and the relevant national requirements for industrial safety and plant security.

5.62. Suitable alarm systems and means of communication shall be provided so that all persons present in the plant and on the site can be warned and instructed, even under accident conditions.

5.63. The availability of means of communication necessary for safety, within the nuclear power plant, in the immediate vicinity and to off-site agencies, as stipulated in the emergency plan, shall be ensured at all times. This requirement shall be taken into account in the design and the diversity of the methods of communication selected.

Control of access

5.64. The plant shall be isolated from the surroundings by suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, provision shall be made in the design of the buildings and the layout of the site for personnel and/or equipment for the control of access, and attention shall be paid to guarding against the unauthorized entry of persons and goods to the plant.

5.65. Unauthorized access to, or interference for any reason with, structures, systems and components important to safety shall be prevented. Where access is necessary for

maintenance, testing or inspection purposes, it shall be ensured in the design that the necessary activities can be performed without significantly reducing the reliability of safety related equipment.

Interactions of systems

5.66. If there is a significant probability that it will be necessary for systems important to safety to operate simultaneously, their possible interaction shall be evaluated. In the analysis, account shall be taken not only of physical interconnections, but also of the possible effects of one system's operation, maloperation or failure on the physical environment of other essential systems, in order to ensure that changes in the environment do not affect the reliability of system components in functioning as intended.

Interactions between the electrical power grid and the plant

5.67. In the design of the plant, account shall be taken of power grid–plant interactions, including the independence of and number of power supply lines to the plant, in relation to the necessary reliability of the power supply to plant systems important to safety.

Decommissioning

5.68. At the design stage, special consideration shall be given to the incorporation of features that will facilitate the decommissioning and dismantling of the plant. In particular, account shall be taken in the design of:

(1) the choice of materials, such that eventual quantities of radioactive waste are minimized and decontamination is facilitated;
(2) the access capabilities that may be necessary; and
(3) the facilities necessary for storing radioactive waste generated in both operation and decommissioning of the plant.

SAFETY ANALYSIS

5.69. 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 (see para. 5.7), and that defence in depth has been effected.

5.70. The computer programs, analytical methods and plant models used in the safety analysis shall be verified and validated, and adequate consideration shall be given to uncertainties.

Deterministic approach

5.71. The deterministic safety analysis shall include the following:

(1) confirmation that operational limits and conditions are in compliance with the assumptions and intent of the design for normal operation of the plant;
(2) characterization of the PIEs (see Appendix I) that are appropriate for the design and site of the plant;
(3) analysis and evaluation of event sequences that result from PIEs;
(4) comparison of the results of the analysis with radiological acceptance criteria and design limits;
(5) establishment and confirmation of the design basis; and
(6) demonstration that the management of anticipated operational occurrences and design basis accidents is possible by automatic response of safety systems in combination with prescribed actions of the operator.

5.72. The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified. The safety analysis of the plant design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and shall be consistent with the current or 'as built' state.

Probabilistic approach

5.73. A probabilistic safety analysis of the plant shall be carried out in order:

(1) to provide a systematic analysis to give confidence that the design will comply with the general safety objectives;
(2) to demonstrate that a balanced design has been achieved such that no particular feature or PIE makes a disproportionately large or significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety;
(3) to provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behaviour ('cliff edge effects') will be prevented;

(4) to provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;
(5) to provide assessments of the probabilities of occurrence and the consequences of external hazards, in particular those unique to the plant site;
(6) to identify systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences;
(7) to assess the adequacy of plant emergency procedures; and
(8) to verify compliance with probabilistic targets, if set.

6. REQUIREMENTS FOR DESIGN OF PLANT SYSTEMS

REACTOR CORE AND ASSOCIATED FEATURES

General design

6.1. The reactor core and associated coolant, control and protection systems shall be designed with appropriate margins to ensure that the specified design limits are not exceeded and that radiation safety standards are applied in all operational states and in design basis accidents, with account taken of the existing uncertainties.

6.2. The reactor core and associated internal components located within the reactor vessel shall be designed and mounted in such a way that they will withstand the static and dynamic loading expected in operational states, design basis accidents and external events to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure cooling of the core.

6.3. The maximum degree of positive reactivity and its maximum rate of increase by insertion in operational states and design basis accidents shall be limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained and no significant damage will occur to the reactor core.

6.4. It shall be ensured in the design that the possibility of recriticality or reactivity excursion following a PIE is minimized.

6.5. The reactor core and associated coolant, control and protection systems shall be designed to enable adequate inspection and testing throughout the service lifetime of the plant.

Fuel elements and assemblies

6.6. Fuel elements and assemblies shall be designed to withstand satisfactorily the anticipated irradiation and environmental conditions in the reactor core in combination with all processes of deterioration that can occur in normal operation and in anticipated operational occurrences.

6.7. The deterioration considered shall include that arising from: differential expansion and deformation; external pressure of the coolant; additional internal pressure due to the fission products in the fuel element; irradiation of fuel and other materials in the fuel assembly; changes in pressures and temperatures resulting from changes in power demand; chemical effects; static and dynamic loading, including flow induced vibrations and mechanical vibrations; and changes in heat transfer performance that may result from distortions or chemical effects. Allowance shall be made for uncertainties in data, calculations and fabrication.

6.8. Specified fuel design limits, including permissible leakage of fission products, shall not be exceeded in normal operation, and it shall be ensured that operational states that may be imposed in anticipated operational occurrences cause no significant further deterioration. Leakage of fission products shall be restricted by design limits and kept to a minimum.

6.9. Fuel assemblies shall be designed to permit adequate inspection of their structure and component parts after irradiation. In design basis accidents, the fuel elements shall remain in position and shall not suffer distortion to an extent that would render post-accident core cooling insufficiently effective; and the specified limits for fuel elements for design basis accidents shall not be exceeded.

6.10. The aforementioned requirements for reactor and fuel element design shall also be maintained in the event of changes in fuel management strategy or in operational states over the operational lifetime of the plant.

Control of the reactor core

6.11. The provisions of paras 6.3–6.10 shall be met for all levels and distributions of neutron flux that can arise in all states of the core, including those after shutdown and during or after refuelling, and those arising from anticipated operational

occurrences and design basis accidents. Adequate means of detecting these flux distributions shall be provided to ensure that there are no regions of the core in which the provisions of paras 6.3–6.10 could be breached without being detected. The design of the core shall sufficiently reduce the demands made on the control system for maintaining flux shapes, levels and stability within specified limits in all operational states.

6.12. Provision shall be made for the removal of non-radioactive substances, including corrosion products, which may compromise the safety of the system, for example by clogging coolant channels.

Reactor shutdown

6.13. Means shall be provided to ensure that there is a capability to shut down the reactor in operational states and design basis accidents, and that the shutdown condition can be maintained even for the most reactive core conditions. The effectiveness, speed of action and shutdown margin of the means of shutdown shall be such that the specified limits are not exceeded. For the purpose of reactivity control and flux shaping in normal power operation, a part of the means of shutdown may be used provided that the shutdown capability is maintained with an adequate margin at all times.

6.14. The means for shutting down the reactor shall consist of at least two different systems to provide diversity.

6.15. At least one of the two systems shall be, on its own, capable of quickly rendering the nuclear reactor subcritical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure. Exceptionally, a transient recriticality may be permitted provided that the specified fuel and component limits are not exceeded.

6.16. At least one of these two systems shall be, on its own, capable of rendering the reactor subcritical from normal operational states, in anticipated operational occurrences and in design basis accidents, and of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the core.

6.17. In judging the adequacy of the means of shutdown, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or could result in a common cause failure.

6.18. The means of shutdown shall be adequate to prevent or withstand inadvertent increases in reactivity by insertion during the shutdown, including refuelling in this state. In meeting this provision, deliberate actions that increase reactivity in the shutdown state (such as absorber movement for maintenance, dilution of boron content and refuelling actions) and a single failure in the shutdown means shall be taken into account.

6.19. Instrumentation shall be provided and tests shall be specified to ensure that the shutdown means are always in the state stipulated for the given plant condition.

6.20. In the design of reactivity control devices, account shall be taken of wear-out, and effects of irradiation, such as burnup, changes in physical properties and production of gas.

REACTOR COOLANT SYSTEM

Design of the reactor coolant system

6.21. The reactor coolant system, its associated auxiliary systems, and the control and protection systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded in operational states. Provision shall be made to ensure that the operation of pressure relief devices, even in design basis accidents, will not lead to unacceptable releases of radioactive material from the plant. The reactor coolant pressure boundary shall be equipped with adequate isolation devices to limit any loss of radioactive fluid.

6.22. The component parts containing the reactor coolant, such as the reactor pressure vessel or the pressure tubes, piping and connections, valves, fittings, pumps, circulators and heat exchangers, together with the devices by which such parts are held in place, shall be designed in such a way as to withstand the static and dynamic loads anticipated in all operational states and in design basis accidents. The materials used in the fabrication of the component parts shall be selected so as to minimize activation of the material.

6.23. The reactor pressure vessel and the pressure tubes shall be designed and constructed to be of the highest quality with respect to materials, design standards, capability of inspection and fabrication.

6.24. The pressure retaining boundary for reactor coolant shall be designed so that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate

in a regime of high resistance to unstable fracture with fast crack propagation, to permit timely detection of flaws (such as by application of the leak before break concept). Designs and plant states in which components of the reactor coolant pressure boundary could exhibit brittle behaviour shall be avoided.

6.25. The design shall reflect consideration of all conditions of the boundary material in operational states, including those for maintenance and testing, and under design basis accident conditions, with account taken of the expected end-of-life properties affected by erosion, creep, fatigue, the chemical environment, the radiation environment and ageing, and any uncertainties in determining the initial state of the components and the rate of possible deterioration.

6.26. The design of the components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall be such as to minimize the likelihood of failure and associated consequential damage to other items of the primary coolant system important to safety in all operational states and in design basis accidents, with due allowance made for deterioration that may occur in service.

In-service inspection of the reactor coolant pressure boundary

6.27. The components of the reactor coolant pressure boundary shall be designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the boundary. Provision shall be made to implement a material surveillance programme for the reactor coolant pressure boundary, particularly in locations of high irradiation, and for other important components as appropriate, in order to determine the metallurgical effects of factors such as irradiation, stress corrosion cracking, thermal embrittlement and ageing of structural materials.

6.28. It shall be ensured that it is possible to inspect or test either directly or indirectly the components of the reactor coolant pressure boundary, according to the safety importance of those components, so as to demonstrate the absence of unacceptable defects or of safety significant deterioration.

6.29. Indicators for the integrity of the reactor coolant pressure boundary (such as leakage) shall be monitored. The results of such measurements shall be taken into consideration in the determination of which inspections are necessary for safety.

6.30. If the safety analysis of the nuclear power plant indicates that particular failures in the secondary cooling system may result in serious consequences, it shall be ensured that it is possible to inspect the relevant parts of the secondary cooling system.

Inventory of reactor coolant

6.31. Provision shall be made for controlling the inventory and pressure of coolant to ensure that specified design limits are not exceeded in any operational state, with volumetric changes and leakage taken into account. The systems performing this function shall have adequate capacity (flow rate and storage volumes) to meet this requirement. They may be composed of components needed for the processes of power generation or may be specially provided for performing this function.

Cleanup of the reactor coolant

6.32. Adequate facilities shall be provided for removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel. The capability of the necessary systems shall be based on the specified fuel design limit on permissible leakage with a conservative margin to ensure that the plant can be operated with a level of circuit activity which is as low as reasonably practicable, and that radioactive releases meet the ALARA principle and are within the prescribed limits.

Removal of residual heat from the core

6.33. Means for removing residual heat shall be provided. Their safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified fuel design limits and the design basis limits of the reactor coolant pressure boundary are not exceeded.

6.34. Interconnections and isolation capabilities and other appropriate design features (such as leak detection) shall be provided to fulfil the requirements of para. 6.33 with sufficient reliability, on the assumptions of a single failure and the loss of off-site power, and with the incorporation of suitable redundancy, diversity and independence.

Emergency core cooling

6.35. Core cooling shall be provided in the event of a loss of coolant accident so as to minimize fuel damage and limit the escape of fission products from the fuel. The cooling provided shall ensure that:

(1) the limiting parameters for the cladding or fuel integrity (such as temperature) will not exceed the acceptable value for design basis accidents (for applicable reactor designs);
(2) possible chemical reactions are limited to an allowable level;

(3) the alterations in the fuel and internal structural alterations will not significantly reduce the effectiveness of the means of emergency core cooling; and
(4) the cooling of the core will be ensured for a sufficient time.

6.36. Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable redundancy and diversity in components shall be provided in order to fulfil these requirements with sufficient reliability for each PIE, on the assumption of a single failure.

6.37. Adequate consideration shall be given to extending the capability to remove heat from the core following a severe accident.

Inspection and testing of the emergency core cooling system

6.38. The emergency core cooling system shall be designed to permit appropriate periodic inspection of important components and to permit appropriate periodic testing to confirm the following:

(1) the structural integrity and leaktight integrity of its components;
(2) the operability and performance of the active components of the system in normal operation, as far as feasible; and
(3) the operability of the system as a whole under the plant states specified in the design basis, to the extent practicable.

Heat transfer to an ultimate heat sink

6.39. Systems shall be provided to transfer residual heat from structures, systems and components important to safety to an ultimate heat sink. This function shall be carried out at very high levels of reliability in operational states and in design basis accidents. All systems that contribute to the transport of heat (by conveying heat, by providing power or by supplying fluids to the heat transport systems) shall be designed in accordance with the importance of their contribution to the function of heat transfer as a whole.

6.40. The reliability of the systems shall be achieved by an appropriate choice of measures including the use of proven components, redundancy, diversity, physical separation, interconnection and isolation.

6.41. Natural phenomena and human induced events shall be taken into account in the design of the systems and in the possible choice of diversity in the ultimate heat sinks and in the storage systems from which fluids for heat transfer are supplied.

6.42. Adequate consideration shall be given to extending the capability to transfer residual heat from the core to an ultimate heat sink so as to ensure that, in the event of a severe accident, acceptable temperatures can be maintained in structures, systems and components important to the safety function of confinement of radioactive materials.

CONTAINMENT SYSTEM

Design of the containment system

6.43. A containment system shall be provided in order to ensure that any release of radioactive materials to the environment in a design basis accident would be below prescribed limits. This system may include, depending on design requirements: leaktight structures; associated systems for the control of pressures and temperatures; and features for the isolation, management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.

6.44. All identified design basis accidents shall be taken into account in the design of the containment system. In addition, consideration shall be given to the provision of features for the mitigation of the consequences of selected severe accidents in order to limit the release of radioactive material to the environment.

Strength of the containment structure

6.45. The strength of the containment structure, including access openings and penetrations and isolation valves, shall be calculated with sufficient margins of safety on the basis of the potential internal overpressures, underpressures and temperatures, dynamic effects such as missile impacts, and reaction forces anticipated to arise as a result of design basis accidents. The effects of other potential energy sources, including, for example, possible chemical and radiolytic reactions, shall also be considered. In calculating the necessary strength of the containment structure, natural phenomena and human induced events shall be taken into consideration, and provision shall be made to monitor the condition of the containment and its associated features.

6.46. Provision for maintaining the integrity of the containment in the event of a severe accident shall be considered. In particular, the effects of any predicted combustion of flammable gases shall be taken into account.

Capability for containment pressure tests

6.47. The containment structure shall be designed and constructed so that it is possible to perform a pressure test at a specified pressure to demonstrate its structural integrity before operation of the plant and over the plant's lifetime.

Containment leakage

6.48. The containment system shall be designed so that the prescribed maximum leakage rate is not exceeded in design basis accidents. The primary pressure withstanding containment may be partially or totally surrounded by a secondary confinement for the collection and controlled release or storage of materials that may leak from the primary containment in design basis accidents.

6.49. The containment structure and equipment and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested at the design pressure after all penetrations have been installed. Determination of the leakage rate of the containment system at periodic intervals over the service lifetime of the reactor shall be possible, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.

6.50. Adequate consideration shall be given to the capability to control any leakage of radioactive materials from the containment in the event of a severe accident.

Containment penetrations

6.51. The number of penetrations through the containment shall be kept to a practical minimum.

6.52. All penetrations through the containment shall meet the same design requirements as the containment structure itself. They shall be protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles, jet forces and pipe whip.

6.53. If resilient seals (such as elastomeric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have the capability for leak testing at the containment design pressure, independent of the determination of the leak rate of the containment as a whole, to demonstrate their continued integrity over the lifetime of the plant.

6.54. Adequate consideration shall be given to the capability of penetrations to remain functional in the event of a severe accident.

Containment isolation

6.55. Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a design basis accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed prescribed limits. These lines shall be fitted with at least two adequate containment isolation valves arranged in series (normally with one outside and the other inside the containment, but other arrangements may be acceptable depending on the design), and each valve shall be capable of being reliably and independently actuated. Isolation valves shall be located as close to the containment as is practicable. Containment isolation shall be achievable on the assumption of a single failure. If the application of this requirement reduces the reliability of a safety system that penetrates the containment, other isolation methods may be used.

6.56. Each line that penetrates the primary reactor containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one adequate containment isolation valve. This valve shall be outside the containment and located as close to the containment as practicable.

6.57. Adequate consideration shall be given to the capability of isolation devices to maintain their function in the event of a severe accident.

Containment air locks

6.58. Access by personnel to the containment shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor operations and in design basis accidents. Where provision is made for entry of personnel for surveillance purposes during certain low power operations, provisions for ensuring the safety of personnel in such operations shall be specified in the design. These requirements shall also apply to equipment air locks, where provided.

6.59. Adequate consideration shall be given to the capability of containment air locks to maintain their function in the event of a severe accident.

Internal structures of the containment

6.60. The design shall provide for ample flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in design basis accidents do not result in damage to the pressure bearing structure or to other systems of importance in limiting the effects of design basis accidents.

6.61. Adequate consideration shall be given to the capability of internal structures to withstand the effects of a severe accident.

Removal of heat from the containment

6.62. The capability to remove heat from the reactor containment shall be ensured. The safety function shall be fulfilled of reducing the pressure and temperature in the containment, and maintaining them at acceptably low levels, after any accidental release of high energy fluids in a design basis accident. The system performing the function of removing heat from the containment shall have adequate reliability and redundancy to ensure that this can be fulfilled, on the assumption of a single failure.

6.63. Adequate consideration shall be given to the capability to remove heat from the reactor containment in the event of a severe accident.

Control and cleanup of the containment atmosphere

6.64. Systems to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment shall be provided as necessary:

(1) to reduce the amount of fission products that might be released to the environment in design basis accidents; and
(2) to control the concentration of hydrogen, oxygen and other substances in the containment atmosphere in design basis accidents in order to prevent deflagration or detonation which could jeopardize the integrity of the containment.

6.65. Systems for cleaning up the containment atmosphere shall have suitable redundancy in components and features to ensure that the safety group can fulfil the necessary safety function, on the assumption of a single failure.

6.66. Adequate consideration shall be given to the control of fission products, hydrogen and other substances that may be generated or released in the event of a severe accident.

Coverings and coatings

6.67. The coverings and coatings for components and structures within the containment system shall be carefully selected, and their methods of application specified, to ensure fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of coverings and coatings.

INSTRUMENTATION AND CONTROL

General requirements for instrumentation and control systems important to safety

6.68. Instrumentation shall be provided to monitor plant variables and systems over the respective ranges for normal operation, anticipated operational occurrences, design basis accidents and severe accidents in order to ensure that adequate information can be obtained on the status of the plant. Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information on the plant necessary for its reliable and safe operation. Provision shall be made for automatic recording of measurements of any derived parameters that are important to safety, such as the subcooling margin of the coolant water. Instrumentation shall be environmentally qualified for the plant states concerned and shall be adequate for measuring plant parameters and thus classifying events for the purposes of emergency response.

6.69. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the course of design basis accidents and the status of essential equipment; and for predicting, as far as is necessary for safety, the locations and quantities of radioactive materials that could escape from the locations intended in the design. The instrumentation and recording equipment shall be adequate to provide information as far as practicable for determining the status of the plant in a severe accident and for taking decisions in accident management.

6.70. Appropriate and reliable controls shall be provided to maintain the variables referred to in para. 6.68 within specified operational ranges.

Control room

6.71. A control room shall be provided from which the plant can be safely operated in all its operational states, and from which measures can be taken to maintain the

plant in a safe state or to bring it back into such a state after the onset of anticipated operational occurrences, design basis accidents and severe accidents. Appropriate measures shall be taken and adequate information provided to safeguard the occupants of the control room against consequent hazards, such as undue radiation levels resulting from an accident condition or the release of radioactive material or explosive or toxic gases, which could hinder necessary actions by the operator.

6.72. Special attention shall be given to identifying those events, both internal and external to the control room, which may pose a direct threat to its continued operation, and the design shall provide for reasonably practicable measures to minimize the effects of such events.

6.73. The layout of the instrumentation and the mode of presentation of information shall provide the operating personnel with an adequate overall picture of the status and performance of the plant. Ergonomic factors shall be taken into account in the design of the control room.

6.74. Devices shall be provided to give in an efficient way visual and, if appropriate, also audible indications of operational states and processes that have deviated from normal and could affect safety.

Supplementary control room

6.75. Sufficient instrumentation and control equipment shall be available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat can be removed, and the essential plant variables can be monitored should there be a loss of ability to perform these essential safety functions in the control room.

Use of computer based systems in systems important to safety

6.76. If the design is such that a system important to safety is dependent upon the reliable performance of a computer based system, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the life-cycle of the system, and in particular the software development cycle. The entire development shall be subject to an appropriate quality assurance programme.

6.77. The level of reliability necessary shall be commensurate with the safety importance of the system. The necessary level of reliability shall be achieved by means of

a comprehensive strategy that uses various complementary means (including an effective regime of analysis and testing) at each phase of development of the process, and a validation strategy to confirm that the design requirements for the system have been fulfilled.

6.78. The level of reliability assumed in the safety analysis for a computer based system shall include a specified conservatism to compensate for the inherent complexity of the technology and the consequent difficulty of analysis.

Automatic control

6.79. Various safety actions shall be automated so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or design basis accidents. In addition, appropriate information shall be available to the operator to monitor the effects of the automatic actions.

Functions of the protection system

6.80. The protection system shall be designed:

(1) to initiate automatically the operation of appropriate systems, including, as necessary, the reactor shutdown systems, in order to ensure that specified design limits are not exceeded as a result of anticipated operational occurrences;
(2) to detect design basis accidents and initiate the operation of systems necessary to limit the consequences of such accidents within the design basis; and
(3) to be capable of overriding unsafe actions of the control system.

Reliability and testability of the protection system

6.81. The protection system shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed. Redundancy and independence designed into the protection system shall be sufficient at least to ensure that:

(1) no single failure results in loss of protection function; and
(2) the removal from service of any component or channel does not result in loss of the necessary minimum redundancy, unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

6.82. The protection system shall be designed to ensure that the effects of normal operation, anticipated operational occurrences and design basis accidents on

redundant channels do not result in loss of its function; or else such a loss shall be demonstrated to be acceptable on some other basis. Design techniques such as testability, including a self-checking capability where necessary, fail-safe behaviour, functional diversity and diversity in component design or principles of operation shall be used to the extent practicable to prevent loss of a protection function.

6.83. The protection system shall, unless its adequate reliability is ensured by some other means, be designed to permit periodic testing of its functioning when the reactor is in operation, including the possibility of testing channels independently to determine failures and losses of redundancy that may have occurred. The design shall permit all aspects of functionality from the sensor to the input signal to the final actuator to be tested in operation.

6.84. The design shall be such as to minimize the likelihood that operator action could defeat the effectiveness of the protection system in normal operations and expected operational occurrences, but not to negate correct operator actions in design basis accidents.

Use of computer based systems in protection

6.85. Where a computer based system is intended to be used in a protection system, the following requirements shall supplement those of paras 6.76–6.78:

(1) the highest quality of and best practices for hardware and software shall be used;
(2) the whole development process, including control, testing and commissioning of design changes, shall be systematically documented and reviewable;
(3) in order to confirm confidence in the reliability of the computer based systems, an assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and
(4) where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.

Separation of protection and control systems

6.86. Interference between the protection system and the control systems shall be prevented by avoiding interconnections or by suitable functional isolation. If signals are used in common by both the protection system and any control system, appropriate separation (such as by adequate decoupling) shall be ensured and it shall be demonstrated that all safety requirements of paras 6.80–6.85 are fulfilled.

EMERGENCY CONTROL CENTRE

6.87. An on-site emergency control centre, separated from the plant control room, shall be provided to serve as meeting place for the emergency staff who will operate from there in the event of an emergency. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there. The room should provide means of communication with the control room, the supplementary control room and other important points in the plant, and with the on-site and off-site emergency response organizations. Appropriate measures shall be taken to protect the occupants for a protracted time against hazards resulting from a severe accident.

EMERGENCY POWER SUPPLY

6.88. After certain PIEs, various systems and components important to safety will need emergency power. It shall be ensured that the emergency power supply is able to supply the necessary power in any operational state or in a design basis accident, on the assumption of the coincidental loss of off-site power. The need for power will vary with the nature of the PIE, and the nature of the safety duty to be performed will be reflected in the choice of means for each duty; in respect of number, availability, duration, capacity and continuity, for example.

6.89. The combined means to provide emergency power (such as by means of water, steam or gas turbine, diesel engines or batteries) shall have a reliability and form that are consistent with all the requirements of the safety systems to be supplied, and shall perform their functions on the assumption of a single failure. It shall be possible to test the functional capability of the emergency power supply.

WASTE TREATMENT AND CONTROL SYSTEMS

6.90. Adequate systems shall be provided to treat radioactive liquid and gaseous effluents in order to keep the quantities and concentrations of radioactive discharges within prescribed limits. The ALARA principle shall be applied.

6.91. Adequate systems shall be provided for the handling of radioactive wastes and for storing these safely on the site for a period of time consistent with the availability of the disposal route on the site. Transport of solid wastes from the site shall be effected according to the decisions of competent authorities.

Control of releases of radioactive liquids to the environment

6.92. The plant shall include suitable means to control the release of radioactive liquids to the environment so as to conform to the ALARA principle and to ensure that emissions and concentrations remain within prescribed limits.

Control of airborne radioactive material

6.93. A ventilation system with an appropriate filtration system shall be provided:

(1) to prevent unacceptable dispersion of airborne radioactive substances within the plant;
(2) to reduce the concentration of airborne radioactive substances to levels compatible with the need for access to the particular area;
(3) to keep the level of airborne radioactive substances in the plant below prescribed limits, the ALARA principle being applied in normal operation, anticipated operational occurrences and design basis accidents; and
(4) to ventilate rooms containing inert or noxious gases without impairing the capability to control radioactive releases.

Control of releases of gaseous radioactive material to the environment

6.94. A ventilation system with an appropriate filtration system shall be provided to control the release of airborne radioactive substances to the environment and to ensure that it conforms to the ALARA principle and is within prescribed limits.

6.95. Filter systems shall be sufficiently reliable and so designed that under the expected prevailing conditions the necessary retention factors are achieved. Filter systems shall be designed such that the efficiency can be tested.

FUEL HANDLING AND STORAGE SYSTEMS

Handling and storage of non-irradiated fuel

6.96. The handling and storage systems for non-irradiated fuel shall be designed:

(1) to prevent criticality by a specified margin by physical means or processes, preferably by the use of geometrically safe configurations, even under plant states of optimum moderation;

(2) to permit appropriate maintenance, periodic inspection and testing of components important to safety; and
(3) to minimize the probability of loss of or damage to the fuel.

Handling and storage of irradiated fuel

6.97. The handling and storage systems for irradiated fuel shall be designed:

(1) to prevent criticality by physical means or processes, preferably by the use of geometrically safe configurations, even under plant states of optimum moderation;
(2) to permit adequate heat removal in operational states and in design basis accidents;
(3) to permit inspection of irradiated fuel;
(4) to permit appropriate periodic inspection and testing of components important to safety;
(5) to prevent the dropping of spent fuel in transit;
(6) to prevent unacceptable handling stresses on the fuel elements or fuel assemblies;
(7) to prevent the inadvertent dropping of heavy objects such as spent fuel casks, cranes or other potentially damaging objects on the fuel assemblies;
(8) to permit safe storage of suspect or damaged fuel elements or fuel assemblies;
(9) to provide proper means for radiation protection;
(10) to adequately identify individual fuel modules;
(11) to control soluble absorber levels if used for criticality safety;
(12) to facilitate maintenance and decommissioning of the fuel storage and handling facilities;
(13) to facilitate decontamination of fuel handling and storage areas and equipment when necessary; and
(14) to ensure that adequate operating and accounting procedures can be implemented to prevent any loss of fuel.

6.98. For reactors using a water pool system for fuel storage, the design shall provide the following:

(1) means for controlling the chemistry and activity of any water in which irradiated fuel is handled or stored;
(2) means for monitoring and controlling the water level in the fuel storage pool and for detecting leakage; and
(3) means to prevent emptying of the pool in the event of a pipe break (that is, anti-syphon measures).

RADIATION PROTECTION[3]

General requirements

6.99. Radiation protection is directed to preventing any avoidable radiation exposure and to keeping any unavoidable exposures as low as reasonably achievable. This objective shall be accomplished in the design by means of the following:

(1) appropriate layout and shielding of structures, systems and components containing radioactive materials;
(2) paying attention to the design of the plant and equipment so as to minimize the number and duration of human activities undertaken in radiation fields and reduce the likelihood of contamination of the site personnel;
(3) making provision for the treatment of radioactive materials in an appropriate form and condition, for either their disposal, their storage on the site or their removal from the site; and
(4) making arrangements to reduce the quantity and concentration of radioactive materials produced and dispersed within the plant or released to the environment.

6.100. Full account shall be taken of the potential buildup of radiation levels with time in areas of personnel occupancy and of the need to minimize the generation of radioactive materials as wastes.

Design for radiation protection

6.101. Suitable provision shall be made in the design and layout of the plant to minimize exposure and contamination from all sources. Such provision shall include adequate design of structures, systems and components in terms of: minimizing exposure during maintenance and inspection; shielding from direct and scattered radiation; ventilation and filtration for control of airborne radioactive materials; limiting the activation of corrosion products by proper specification of materials; means of monitoring; control of access to the plant; and suitable decontamination facilities.

6.102. The shielding design shall be such that radiation levels in operating areas do not exceed the prescribed limits, and shall facilitate maintenance and inspection so as to minimize exposure of maintenance personnel. The ALARA principle shall be applied.

[3] For further guidance, see Ref. [6].

6.103. The plant layout and procedures shall provide for the control of access to radiation areas and areas of potential contamination, and for minimizing contamination from the movement of radioactive materials and personnel within the plant. The plant layout shall provide for efficient operation, inspection, maintenance and replacement as necessary to minimize radiation exposure.

6.104. Provision shall be made for appropriate decontamination facilities for both personnel and equipment and for handling any radioactive waste arising from decontamination activities.

Means of radiation monitoring

6.105. Equipment shall be provided to ensure that there is adequate radiation monitoring in operational states, design basis accidents and, as practicable, severe accidents:

(1) Stationary dose rate meters shall be provided for monitoring the local radiation dose rate at places routinely occupied by operating personnel and where the changes in radiation levels in normal operation or anticipated operational occurrences may be such that access shall be limited for certain periods of time. Furthermore, stationary dose rate meters shall be installed to indicate the general radiation level at appropriate locations in the event of design basis accidents and, as practicable, severe accidents. These instruments shall give sufficient information in the control room or at the appropriate control position that plant personnel can initiate corrective action if necessary.
(2) Monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by personnel and where the levels of activity of airborne radioactive materials may on occasion be expected to be such as to necessitate protective measures. These systems shall give an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected.
(3) Stationary equipment and laboratory facilities shall be provided for determining in a timely manner the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment, in operational states and in accident conditions.
(4) Stationary equipment shall be provided for monitoring the effluents prior to or during discharge to the environment.
(5) Instruments shall be provided for measuring radioactive surface contamination.
(6) Facilities shall be provided for monitoring of individual doses to and contamination of personnel.

6.106. In addition to the monitoring within the plant, arrangements shall also be made to determine radiological impacts, if any, in the vicinity of the plant, with particular reference to:

(1) pathways to the human population, including the food-chain;
(2) the radiological impact, if any, on local ecosystems;
(3) the possible accumulation of radioactive materials in the physical environment; and
(4) the possibility of any unauthorized discharge routes.

Appendix I

POSTULATED INITIATING EVENTS

I.1. This appendix elaborates on the definition and application of the concept of the postulated initiating event (PIE).

I.2. A PIE is defined as an event identified in design as leading to anticipated operational occurrences or accident conditions. This means that a PIE is not an accident itself; it is the event that initiates a sequence and 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.

I.3. A PIE may be of a type that has minor consequences, such as the failure of a redundant component, or it may have serious consequences, such as the failure of a major pipe in the reactor coolant system. It is a main objective of the design to achieve plant characteristics that ensure that the majority of the PIEs have minor or even insignificant consequences; and that if the remainder lead to design basis accidents, the consequences are acceptable; or if they lead to severe accidents, the consequences are limited by design features and accident management.

I.4. A full range of events needs to be postulated in order to ensure that all credible events with potential for serious consequences and significant probability have been anticipated and can be withstood by the design of the plant. There are no firm criteria to govern the selection of PIEs; rather the process is a combination of iteration between the design and analysis, engineering judgement and experience from previous plant design and operation. Exclusion of a specific event sequence needs to be justified.

I.5. The number of PIEs to be used in the development of the performance requirements for the items important to safety and in the overall safety assessment of the plant should be limited to make the task practical, and this is done by restricting the detailed analysis to a number of representative event sequences[4]. The representative event sequences identify bounding cases and provide the basis for numerical design limits for structures, systems and components important to safety.

[4] The phrase ‘event sequence’ or ‘sequence of events’ is used to refer to the combination of a PIE and subsequent operator actions or actions for items important to safety.

I.6. Some PIEs may be specified deterministically, on the basis of a variety of factors such as experience of previous plants, particular requirements of national licensing bodies or perhaps the magnitude of potential consequences. Other PIEs may be specified by means of systematic methods such as a probabilistic analysis because particular features of the design, the location of the plant or operational experience enable their characteristics to be quantified in probabilistic terms.

TYPES OF PIE

Internal events

Equipment failures

I.7. Initiating events can be individual equipment failures that could directly or indirectly affect the safety of the plant. The list of these events adequately represents all credible failures of plant systems and components.

I.8. The types of failure that need to be considered depend on the kind of system or component involved. A failure in the broadest sense is either the loss of ability of the system or component to perform its function or the performance of an undesirable function. For example, a pipe failure could be a leak, a rupture or the blockage of a flow path. For an active component such as a valve, the failure could take the form of not opening or closing when necessary, opening or closing when not necessary, partial opening or closing, or opening or closing at the wrong speed. For a device such as an instrument transducer, the failure could take the form of error outside the permitted error band, absence of output, constant maximum output, erratic output or a combination thereof.

I.9. With the increasing use of computer based systems in safety applications and safety critical applications, a hardware failure or an incorrect software programme may lead to significant control actions; this possibility should be considered.

Human error

I.10. In many cases the consequences of human errors will be similar to the consequences of failures of components. Human errors may range from faulty or incomplete maintenance operations, to incorrect setting of control equipment limits or wrong or omitted operator actions (errors of commission and errors of omission).

Other internal events

I.11. Fires, explosions and floods of internal origin also have the potential to be important influences on the safety performance of the plant and are normally included in the compilation of the list of PIEs.

External events

I.12. Examples of external events and the determination of the relevant design basis input for the plant are given in the Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1) [5], and its related Safety Guides. These events generally necessitate the design of plant items for additional vibratory, impact and impulse type loads.

I.13. If the likelihood of failure of a structure, system or component important to safety due to natural or human induced external events can be inferred to be acceptably low because of adequate design and construction, failure caused by that event need not be included in the design basis for the plant.

Combinations of events

I.14. Care needs to be taken in combining individual events in analysing accidents to ensure that there is some rationale for the particular combination. A random combination of events may represent an extremely unlikely scenario that should be shown in the probabilistic safety analysis to be sufficiently rare as to be discounted rather than being taken as a postulated accident. In probabilistic safety analysis, an approach using best estimate analysis is adopted for severe accidents while conservatism should be applied in the analytical approach for postulated accidents that have a relatively higher likelihood of occurrence.

I.15. In determining which events to combine, it is useful to consider three time periods:

— a long term period, before the particular event being considered;
— a near term period, including occurrence of the event and its short term effects, and
— the post-event recovery period.

I.16. It may be assumed that corrective action has been taken for an event that occurs in the long term period prior to the occurrence of another event if proper provision for its identification has been incorporated into the plant design and if the time needed

for the corrective action is short. In such instances, combinations of such events need not be considered.

I.17. For the near term period (usually having a duration of hours), the expected probabilities of occurrence of the individual events may be such that a randomly occurring combination would be considered not a credible scenario.

I.18. For the post-event recovery period (of days or longer), additional events may need to be taken into account, depending upon the length of the recovery period and the expected probabilities of the events. For the recovery period, it may be realistic to assume that the severity of an event that has to be taken in a combination is not as great as would need to be assumed for the same kind of event considered over a time period corresponding to the lifetime of the plant. For example, in the recovery period for a loss of coolant accident, if a random combination with an earthquake needs to be considered, the severity could be taken as less than the severity of the design basis earthquake for the plant.

Appendix II

REDUNDANCY, DIVERSITY AND INDEPENDENCE

II.1. This appendix presents several design measures that may be used, if necessary in combination, to achieve and maintain the necessary reliability commensurate with the importance of the safety functions to be fulfilled within the relevant levels of defence in depth.

II.2. Although no universal quantitative targets can be expressed for the individual reliability requirements for each level of defence in depth, the greatest emphasis should be placed on the first level. This is also consistent with the objective of the operating organization that there should be high availability of the plant for power production.

II.3. As a guideline or for use as acceptance criteria agreed upon with the regulatory body, maximum unavailability limits for certain safety systems may be established to ensure the necessary reliability for the performance of safety functions.

COMMON CAUSE FAILURES

II.4. Failure of a number of devices or components to perform their functions may occur as a result of a single specific event or cause. Such failures may affect a number of different items important to safety simultaneously. The event or cause may 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.

II.5. Common cause failures may also occur when a number of the same type of components fail at the same time. This may be due to reasons such as a change in ambient conditions, saturation of signals, repeated maintenance error or design deficiency.

II.6. Appropriate measures to minimize the effects of common cause failures, such as the application of redundancy, diversity and independence, are taken as far as practicable in the design.

REDUNDANCY

II.7. Redundancy, the use of more than the minimum number of sets of equipment to fulfil a given safety function, is an important design principle for achieving high

reliability in systems important to safety, and for meeting the single failure criterion for safety systems. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function. For example, three or four pumps might be provided for a particular function when any two would be capable of carrying it out. For the purposes of redundancy, identical or diverse components may be used.

DIVERSITY

II.8. The reliability of some systems can be enhanced by using the principle of diversity to reduce the potential for certain common cause failures.

II.9. Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. Such attributes could be different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers, for example.

II.10. Care should be exercised to ensure that any diversity used actually achieves the desired increase in reliability in the as-built design. For example, to reduce the potential for common cause failures the designer should examine the application of diversity for any similarity in materials, components and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse components or systems are used, there should be a reasonable assurance that such additions are of overall benefit, taking into account the disadvantages such as the extra complication in operational, maintenance and test procedures or the consequent use of equipment of lower reliability.

INDEPENDENCE

II.11. The reliability of systems can be improved by maintaining the following features for independence in design:

— independence among redundant system components;
— independence between system components and the effects of PIEs such that, for example, a PIE does not cause the failure or loss of a safety system or safety function that is necessary to mitigate the consequences of that event;
— appropriate independence between or among systems or components of different safety classes; and
— independence between items important to safety and those not important to safety.

II.12. Independence is accomplished in the design of systems by using functional isolation and physical separation:

(1) *Functional isolation*

Functional isolation should be used to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems resulting from normal or abnormal operation or failure of any component in the systems.

(2) *Physical separation and layout of plant components*

System layout and design should use physical separation as far as practicable to increase assurance that independence will be achieved, particularly in relation to certain common cause failures.

Physical separation includes:

— separation by geometry (such as distance or orientation);
— separation by barriers; or
— separation by a combination of these.

The choice of means of separation will depend on the PIEs considered in the design basis, such as effects of fire, chemical explosion, aircraft crash, missile impact, flooding, extreme temperature or humidity, as applicable.

II.13. Certain areas of the plant tend to be natural centres of convergence for equipment or wiring of various levels (categories) of importance to safety. Examples of such centres may be containment penetrations, motor control centres, cable spreading rooms, equipment rooms, the control rooms and the plant process computers. Appropriate measures to avoid common cause failures should be taken, as far as practicable, in such locations.

REFERENCES

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

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

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANISATION, NUCLEAR ENERGY AGENCY OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

Annex

SAFETY FUNCTIONS FOR BOILING WATER REACTORS, PRESSURIZED WATER REACTORS AND PRESSURE TUBE REACTORS

A–1. This annex gives an example of a detailed subdivision of the three fundamental safety functions defined in para. 4.6.

A–2. These safety functions include those necessary to prevent accident conditions as well as those necessary to mitigate the consequences of accident conditions. They can be fulfilled, as appropriate, using structures, systems or components provided for normal operation, those provided to prevent anticipated operational occurrences from leading to accident conditions or those provided to mitigate the consequences of accident conditions.

A–3. A review of various reactor designs shows that current design safety requirements can be met by having structures, systems or components that perform the following safety functions:

(1) to prevent unacceptable reactivity transients;
(2) to maintain the reactor in a safe shutdown condition after all shutdown actions;
(3) to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;
(4) to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;
(5) to maintain sufficient reactor coolant inventory for core cooling in and after all PIEs considered in the design basis;
(6) to remove heat from the core[1] after a failure of the reactor coolant pressure boundary in order to limit fuel damage;
(7) to remove residual heat (see footnote 1) in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;
(8) to transfer heat from other safety systems to the ultimate heat sink[2];

[1] This safety function applies to the first step of the heat removal system(s). The remaining step(s) are encompassed in safety function (8).

[2] This is a support function for other safety systems when they must perform their safety functions.

(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;
(10) to maintain acceptable integrity of the cladding of the fuel in the reactor core;
(11) to maintain the integrity of the reactor coolant pressure boundary;
(12) to limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;
(13) to limit the radiation exposure of the public and site personnel in and following design basis accidents and selected severe accidents that release radioactive materials from sources outside the reactor containment;
(14) to limit the discharge or release of radioactive waste and airborne radioactive materials to below prescribed limits in all operational states;
(15) to maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;
(16) to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;
(17) to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;
(18) to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;
(19) to prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of a safety function.

A–4. This list of safety functions may be used as a basis for determining whether a structure, system or component performs or contributes to one or more safety functions and to provide a basis for assigning an appropriate gradation of importance to the safety structures, systems and components that contribute to the various safety functions.

GLOSSARY

active component. A component whose functioning depends on an external input such as actuation, mechanical movement or supply of power.

common cause failure. Failure of two or more structures, systems or components due to a single specific event or cause.

diversity. The presence of two or more redundant components or systems to perform an identified function, where the different components or systems have different attributes so as to reduce the possibility of common cause failure.

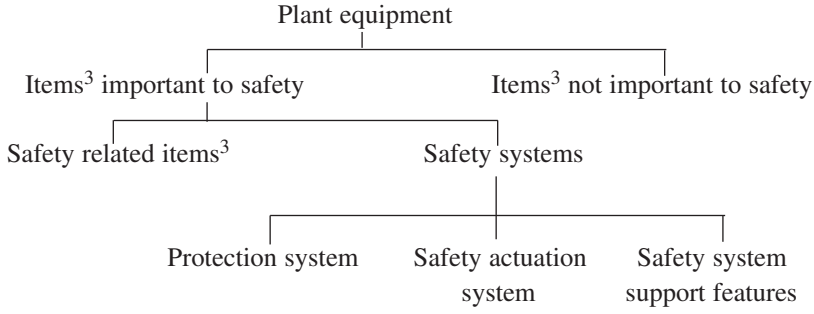
functional isolation. Prevention of influences from the mode of operation or failure of one circuit or system on another.

items important to safety. An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public.

passive component. A component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power.

physical separation. Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.

plant equipment:



[3] In this context, an 'item' is a structure, system or component.

plant states:

operational states		**accident conditions**			
				beyond design basis accidents	
normal operation	anticipated operational occurrences	(a)	design basis accidents	(b)	severe accidents
					accident management

(a) Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.
(b) Beyond design basis accidents without significant core degradation.

accident conditions. Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

accident management. The taking of a set of actions during the evolution of a beyond design basis accident:

— to prevent the escalation of the event into a severe accident;
— to mitigate the consequences of a severe accident; and
— to achieve a long term safe stable state.

anticipated operational occurrence. An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

design basis accident. Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

normal operation. Operation within specified operational limits and conditions.

operational states. States defined under normal operation and anticipated operational occurrences.

severe accidents. Accident conditions more severe than a design basis accident and involving significant core degradation.

postulated initiating event[4]**.** An event identified during design as capable of leading to anticipated operational occurrences or accident conditions.

protection system. System which monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

safety function. A specific purpose that must be accomplished for safety.

safety group. 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.

safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

safety system settings. The levels at which protective devices are automatically actuated in the event of anticipated operational occurrences or accident conditions, to prevent safety limits being exceeded.

single failure. A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.

ultimate heat sink. A medium to which the residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient.

[4] For further information, see Appendix I.

CONTRIBUTORS TO DRAFTING AND REVIEW

Allen, P.	Atomic Energy of Canada Limited, Canada
Cowley, J.S.	Her Majesty's Nuclear Installations Inspectorate, United Kingdom
De Munk, P.	Ministry of Social Affairs and Employment, Netherlands
Feron, F.	Division pour la Sûreté des Installations Nucléaires, France
Foskolos, K.	Paul Scherrer Institute, Switzerland
Frisch, W.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Gasparini, M.	International Atomic Energy Agency
Hardin, W.	Nuclear Regulatory Commission, United States of America
Kavun, O.	Atomenergoprojekt, Russian Federation
Omoto, A.	Tokyo Electric Power Company, Japan
Park, D.	Institute of Nuclear Safety, Republic of Korea
Price, E.G.	Atomic Energy of Canada Limited, Canada
Simon, M.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Tripputi, I.	Ente Nazionale per l'Energia Elettrica, Italy
Vidard, M.	Electricité de France/Septen, France

ADVISORY BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS

Nuclear Safety Standards Advisory Committee

Belgium: Govaerts, P. (Chair); *Brazil*: da Silva, A.J.C.; *Canada*: Wigfull, P.; *China*: Lei, Y., Zhao, Y.; *Czech Republic*: Stuller, J.; *Finland*: Salminen, P.; *France*: Saint Raymond, P.; *Germany*: Wendling, R.D., Sengewein, H., Krüger, W.; *India*: Venkat Raj, V.; *Japan*: Tobioka, T.; *Republic of Korea*: Moon, P.S.H.; *Netherlands*: de Munk, P., Versteeg, J.; *Russian Federation*: Baklushin, R.P.; *Sweden*: Viktorsson, C., Jende, E.; *United Kingdom*: Willby, C., Pape, R.P.; *United States of America*: Morris, B.M.; *IAEA*: Lacey, D.J. (Co-ordinator); *OECD Nuclear Energy Agency*: Frescura, G., Royen, J.

Advisory Commission for Safety Standards

Argentina: Beninson, D.; *Australia*: Lokan, K., Burns, P., *Canada*: Bishop, A. (Chair), Duncan, R.M.; *China*: Huang, Q., Zhao, C.; *France*: Lacoste, A.-C., Asty, M.; *Germany*: Hennenhöfer, G., Wendling, R.D.; *Japan*: Sumita, K., Sato, K.; *Republic of Korea*: Lim, Y.K.; *Slovak Republic*: Lipár, M., Misák, J.; *Spain*: Alonso, A., Trueba, P.; *Sweden*: Holm, L.-E.; *Switzerland*: Prêtre, S.; *United Kingdom*: Williams, L.G., Harbison, S.A.; *United States of America*: Travers, W.D., Callan, L.J., Taylor, J.M.; *IAEA*: Karbassioun, A. (Co-ordinator); *International Commission on Radiological Protection*: Valentin, J.; *OECD Nuclear Energy Agency*: Frescura, G.