

IAEA SAFETY STANDARDS SERIES

Safety of Nuclear Power Plants: Design

REQUIREMENTS

No. NS-R-1



INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA



Documents

Document Sharing Hub

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



Documents

Document Sharing Hub

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

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

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

© IAEA, 2000

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria.

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	1
	Background (1.1)	1
	Objective (1.2–1.4)	1
	Scope (1.5–1.7)	2
	Structure (1.8)	2
2.	SAFETY OBJECTIVES AND CONCEPTS	3
	Safety objectives (2.1–2.8)	3
	The concept of defence in depth (2.9–2.11)	5
3.	REQUIREMENTS FOR MANAGEMENT OF SAFETY	7
	Responsibilities in management (3.1)	7
	Management of design (3.2–3.5)	7
	Proven engineering practices (3.6–3.8)	8
	Operational experience and safety research (3.9)	8
	Safety assessment (3.10–3.12)	9
	Independent verification of the safety assessment (3.13)	9
	Quality assurance (3.14–3.16)	9
4.	PRINCIPAL TECHNICAL REQUIREMENTS	10
	Requirements for defence in depth (4.1–4.4)	10
	Safety functions (4.5–4.7)	11
	Accident prevention and plant safety characteristics (4.8)	11
	Radiation protection and acceptance criteria (4.9–4.13)	12
5.	REQUIREMENTS FOR PLANT DESIGN	12
	Safety classification (5.1–5.3)	12
	General design basis (5.4–5.31)	13
	Design for reliability of structures, systems and components (5.32–5.42)	19
	Provision for in-service testing, maintenance, repair, inspection and monitoring (5.43–5.44)	21
	Equipment qualification (5.45–5.46)	22

Ageing (5.47)	22
Human factors (5.48–5.56)	23
Other design considerations (5.57–5.68)	24
Safety analysis (5.69–5.73)	26
 6. REQUIREMENTS FOR DESIGN OF PLANT SYSTEMS	 28
Reactor core and associated features (6.1–6.20)	28
Reactor coolant system (6.21–6.42)	31
Containment system (6.43–6.67)	35
Instrumentation and control (6.68–6.86)	39
Emergency control centre (6.87)	43
Emergency power supply (6.88–6.89)	43
Waste treatment and control systems (6.90–6.95)	43
Fuel handling and storage systems (6.96–6.98)	44
Radiation protection (6.99–6.106)	46
 APPENDIX I: POSTULATED INITIATING EVENTS	 49
 APPENDIX II: REDUNDANCY, DIVERSITY AND INDEPENDENCE	 53
 REFERENCES	 57
 ANNEX: SAFETY FUNCTIONS FOR BOILING WATER REACTORS, PRESSURIZED WATER REACTORS AND PRESSURE TUBE REACTORS	 59
 GLOSSARY	 61
CONTRIBUTORS TO DRAFTING AND REVIEW	65
ADVISORY BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS	 67

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 ASSURANCE¹

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