NS-R-1 Rev 19, 31 August 2009

IAEA SAFETY STANDARDS

for protecting people and the environment

Status: Draft for Member States comments

Deadline for comments: 22 January 2010

Safety of Nuclear Power Plants: Design

DRAFT SAFETY REQUIREMENTS
DS 414

Revision of the Safety Standards Series No. NS-R-1

IAEA
International Atomic Energy Agency

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 [1.1][1] The present publication supersedes the Safety Requirements publication on Safety of Nuclear Power Plants: Design (Safety Standards Series No. NS-R-1 issued in 2000). It takes account of the recent publication of Fundamental Safety Principles [1]. 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.

1.2 It is now recognised that the design of many existing nuclear power plants, as well as the design bases of new plants have been extended to include additional measures to mitigate the consequences of more complex sequences involving multiple failures, and some severe accidents. Complementary systems and capabilities have been added to many existing plants to aid in severe accident prevention and mitigation, and most existing nuclear power plants have implemented severe accident mitigation guidance. The design of new nuclear power plants now explicitly includes consideration of severe accident scenarios.

1.3 When considering both old and new plants it is convenient to continue to maintain the distinction between design basis events, which include all planned normal operational modes of the plant and design basis accidents, and beyond design basis events that include severe accidents. For nuclear power plants of new design, measures to address severe accidents are now included within the plant design basis. It is accepted that it may not be reasonably practicable to apply all the requirements of this new publication to existing designs that are already in operation. For such designs, it is expected that a comparison will be made against the latest or current standards as part of the periodic safety review of the plant to determine whether any reasonably practicable safety improvements can be implemented and need to be implemented. For existing plants without a periodic safety review process, nonetheless a process has to be put in place within the safety organization to periodically examine whether there are any such safety improvements that can be implemented.

OBJECTIVE

1.4. [1.3] This publication establishes design requirements for structures, systems and components as well as procedures and organizational processes 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.

1.5 [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

1.6 [1.5] 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

[1] The equivalent paragraph number of Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000) has been included in square brackets. This is for ease of review and will be removed before publication.

other heat production applications (such as district heating or desalination). For application to other reactor types, this publication may be used to determine, on a technology neutral basis, the requirements that have to be considered in developing the design. In the development of the requirements for design, account is taken of postulated initiating events, which include many factors that, themselves, or in combination with others, may affect safety.

1.7 [1.7] This publication does not address:

(1) requirements that are specifically covered by other publications in the new IAEA Safety Requirements publications (for example Ref. [2]);

(2) conventional industrial accidents that under no circumstances could affect the safety of the nuclear power plant;

(3) non-radiological effects arising from the operation of nuclear power plants, which may be subject to separate national regulatory requirements; or

(4) nuclear security requirements [11].

1.8. Terms in this publication are to be understood as set out in the IAEA Safety Glossary [9].

STRUCTURE

1.9. [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 objectives, principles and concepts which form the basis for deriving the safety requirements that must be met in the design of the plant.

Each of the Sections 3, 4 and 5 contain a series of individually numbered key requirements that are identified in bold type, with additional paragraphs where appropriate, that provide further description on the means required to achieve the key requirement.

Section 3 covers the requirements to be applied by the design organization in the management of the design process.

Section 4 provides the principal technical requirements for the fundamental safety functions, defence in depth and radiation protection.

Section 5 provides general plant design requirements which supplement the principal technical requirements to ensure that the safety objectives are met and that apply to all structures, systems and components important to safety.

Section 6 provides the overall design requirements applicable to specific plant systems, such as the reactor core, coolant systems, containment systems and instrumentation and control. This Section is mainly applicable to water cooled reactors, although it may also be used as a basis for evaluating the specific requirements for other reactor designs.

2. SAFETY OBJECTIVE, SAFETY PRINCIPLES AND CONCEPTS

2.1. The Fundamental Safety Principles publication [1], establishes one fundamental safety objective and ten associated safety principles which provide the basis for and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks from nuclear power plants.

2.2. The fundamental safety objective and the ten principles have to be achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:

(1) To control the radiation exposure of people and the release of radioactive material to the environment;

(2) To prevent events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation; and

(3) To mitigate the consequences of such events if they were to occur.

2.3. "The fundamental safety objective applies for all facilities and activities, and for all stages over the lifetime of a facility or radiation source, including planning, siting, design, manufacturing, construction, commissioning and operation, as well as decommissioning and closure. This includes the associated transport of radioactive material and management of radioactive waste" (Ref. [1], para. 2.2).

2.4. "Ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances, the appropriate application of all relevant principles is required" (Ref. [1], para. 2.3).

2.5. This publication establishes requirements contributing to those principles that are considered to be particularly important in the design of nuclear power plants.

RADIATION PROTECTION

2.6. In order to implement the safety principles, it is necessary 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, should they occur.

2.7. The principles also require that nuclear power plants are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, this 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 regulatory and operational limits as well as radiation protection standards.

SAFETY IN DESIGN

2.8. To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, it is necessary to take measures:

(1) to prevent accidents having harmful consequences resulting from loss of control over the reactor core and other sources of radiation, and to mitigate their consequences should they occur;
(2) 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
(3) to ensure that the likelihood of accidents with serious radiological consequences is extremely low, and that the radiological consequences of such accidents are mitigated.

2.9. [2.7] In order to demonstrate that the fundamental safety objective [1] in the design of a nuclear power plant is achieved, 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 as a result of the operation of the plant. 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) beyond design basis 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 plant equipment important to safety can be demonstrated, and requirements for emergency response can be established.

2.10. [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; complementary measures; and accident management procedures established by the operating organization; and possibly off-site intervention measures established by appropriate authorities supported as required by the operating organization, 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 to mitigate high radiological consequences has to be limited or even eliminated in technical terms, although such measures may still be required by national authorities.

THE CONCEPT OF DEFENCE IN DEPTH

2.11. [2.9] The primary means of preventing and mitigating the consequences of accidents is the implementation of ‘defence in depth’ [4], [5]. This concept is applied to all safety activities, whether organizational, behavioural or design related, to ensure that they are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. 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.

2.12. [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 harmful effects to people or the environment and ensuring appropriate protection and mitigation in the event that prevention fails. The independent effectiveness, i.e. the capability to achieve the specified objective of each of the different levels of defence, is a necessary element of defence in depth and is achieved by incorporating practices such as redundancy, independence and diversity.

(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 sited, designed, constructed, maintained and operated in accordance with appropriate quality levels and engineering practices. To meet these objectives, 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, as well as plant commissioning. Design options that reduce the potential for internal hazards 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, and the quality control requirements of operational and maintenance practices.

(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 postulated initiating events 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/ features as determined in the safety analysis and the definition of operating procedures to prevent or minimize damage from such postulated initiating events.

(3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events 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 for the provisions of the previous levels, 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 inherent and/or 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 plant conditions with very low probability of occurrence in which the design basis accidents 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 while achieving the management and mitigation of severe accident consequences. This may be achieved by taking account of available design margins, complementary measures

and procedures to prevent accident progression, and by mitigation of the consequences of selected severe plant conditions, in addition to accident management procedures.

(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 severe plant conditions. This requires the provision of an adequately equipped emergency control centre, and plans for the on-site and off-site emergency response.

2.13. [2.11]A relevant aspect of the implementation of defence in depth is the provision in the design of a series of both physical barriers as well as a combination of active and passive features contributing to their effectiveness in confining the radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term, the effectiveness of the individual barriers, the potential internal and external hazards, and the potential consequences of failures.

THE CONCEPT OF MAINTAINING THE INTEGRITY OF DESIGN OF THE PLANT THROUGHOUT THE OPERATING LIFE

2.14. During the development of a design many organizations are involved and each needs to satisfy the technical requirements relevant to their particular responsibilities. The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks [1]. For a nuclear power plant this will be the plant owner or the plant operating organization if different from and contracted to the plant owner. It is recognized that the design, construction and installation of a plant may be shared between a number of organizations: the architect-engineer; the vendor of the reactor and its supporting systems; the supplier of major components; the designer of electrical support systems; and other systems that are important to the safety of the plant. The International Nuclear Safety Group [3] recommends that the operating organization sets up a formal process to maintain the integrity of the plant design throughout its lifetime, i.e. during the operational phase and into decommissioning. There must therefore be a formally designated entity within the operating organization that takes responsibility for this process.

2.15. In practice the design is only complete when the full plant specification (including site details) is produced for its procurement and licensing. Reference [3] underlines the need for a formally designated entity that has overall responsibility for the design process, approves design changes and is responsible for ensuring that the requisite knowledge is maintained. It also introduces the concept of “responsible designers” to whom the formally designated entity may assign responsibilities for parts of the plant. Prior to a plant being ordered, the responsibilities for the design will rest with the design entity organization but once the plant is ordered the ultimate responsibility will lie with the licence holder, however, the detailed knowledge will rest with the responsible designers. This balance will change when the plant is put into service since much of the detailed knowledge will be transferred to the operating organization’s design entity in the operating organization’s technical offices or the offices of the partnering responsible designers, through the safety report, design manuals and other design documentation. To facilitate this it is useful to establish the formally designated entity structure at an early stage.

2.16. The management system requirements placed on the formally designated entity will also apply to the responsible designers, but the overall responsibility for the integrity of the design of all the plant will rest with the formally designated entity and hence the operating organization.

3. MANAGEMENT OF SAFETY IN DESIGN

Requirement 1: Responsibility of the operating organization

The operating organization shall establish a formally designated entity that has overall responsibility for the continuing integrity of the plant design throughout its lifetime starting from the design stage.

3.1. Where responsibility for the design of specific parts of the plant is assigned to other external organizations (referred to as responsible designers), the tasks and functions of the formally designated entity and any responsible designer have to be established in the management system of the designated entity.

3.2. The formally designated entity has to ensure that:

(1) a series of functions is established and implemented to ensure that the plant design meets the safety, reliability and quality acceptance criteria in accordance with the applicable codes and standards, laws, regulations and jurisdictional requirements. Such functions include design verification, definition of engineering standards, approval of key engineering documents and maintaining a positive safety culture;

(2) the relevant knowledge of the design that is needed for safe operation and maintenance of the plant is available and maintained up to date by the operating organization, taking account of past operational experience and validated research findings;

(3) design configuration control is maintained;

(4) the necessary interfaces with responsible designers or suppliers engaged in design work are established and controlled;

(5) the necessary engineering and scientific skills and knowledge are maintained within the operating organization;

(6) all design changes to the plant are reviewed, verified, documented and approved; and

(7) adequate documentation is maintained to facilitate future decommissioning.

Requirement 2: Management system processes[2]

[3.14] **Management system processes that describe the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented during all design phases.**

3.3. [3.14] The processes include provisions for each structure, system and component so that the quality of its design, as well as overall plant design is ensured at all times. This includes the means for identification and correction of design deficiencies, checking adequacy of design, and control of design changes.

3.4. [3.15] Design, including subsequent changes, modifications or safety improvements, have to be in accordance with established procedures that call on appropriate engineering codes and standards, and incorporate applicable requirements and design bases. Design interfaces have to be identified and controlled.

[2] For further requirements, see Ref. [6]

3.5. [3.16] The adequacy of the design, including design tools and design inputs and outputs, has to be verified and validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval have to be completed as soon as practicable during the design and construction process, and in any case before operation of the plant.

Requirement 3: Design of the plant

[3.2] **The design 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 required reliability for the full duration of its design life.**

3.6. [3.3] The design has to ensure that the requirements of the owner and the operating organization; the requirements of the regulatory authority; and the requirements of national nuclear safety legislation, as well as applicable national and international standards are met, and that due account is taken of the human capabilities and limitations. Adequate safety design information has to be provided to ensure safe operation and maintenance of the plant, and to allow subsequent plant modifications to be made, and recommended practices have to be provided for incorporation into the plant administrative and operational procedures (i.e. operational limits and conditions).

3.7. [3.9] The design has to take due account of relevant experience that has been gained in construction and the operation of other plants and of the results of relevant research programmes.

3.8. [3.4] The design has to take account of the results of the deterministic and probabilistic safety analyses, and an iterative process has to take place by means of which it is ensured that due consideration has been given to the prevention of accidents and mitigation of their consequences.

3.9. [3.5] The design has to ensure that the generation of radioactive waste and radioactive discharges are kept to the minimum practicable, in terms of both activity and volume, by appropriate design measures and operational and decommissioning practices, where the effects could span generations.

Requirement 4: Proven engineering practices

[3.6] **Structures, systems and components important to safety shall be designed according to the latest, currently applicable standards.**

3.10. [3.6] Structures, systems and components important to safety have to be of a design proven in previous equivalent applications, and optimized to provide the highest level of safety that can reasonably be achieved [1]

3.11. [3.6] Codes and standards that are used as design rules have to be identified and evaluated to determine their applicability, adequacy and sufficiency and have to be supplemented or modified as necessary to ensure that the final quality is commensurate with the appropriate safety function.

3.12. [3.7] Where an unproven design or feature is introduced or there is a departure from an established engineering practice, safety has to be demonstrated to be adequate by appropriate supporting research programmes, performance tests with specific acceptance criteria, or by examination of operational experience from other relevant applications. The development also has to be adequately tested to the extent practical before being brought into service, and monitored in service, to verify that the expected behaviour is achieved.

3.13. [3.8] In the selection of equipment, consideration has to 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 can not be excluded by the design, preference is given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.

Requirement 5: Safety assessment[3]

[3.10] **Comprehensive deterministic and probabilistic safety assessments shall be carried out throughout the design process to ensure that all relevant safety requirements are met by the design of the plant throughout all stages of the plant's life to confirm that the design meets requirements as delivered for fabrication, as for construction, as built, as operated and as modified.**

3.14. [3.11]The safety assessment is 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.

Requirement 6: Provisions for construction

Structures, systems and components important to safety shall be designed to be manufactured, constructed, assembled, installed and erected according to established processes that ensure the achievement of the requested performance and reliability defined in the design specifications.

3.15. The provisions have to take due account of relevant experience that has been gained in the construction of other similar plants and the associated structures, systems and components.

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

4. PRINCIPAL TECHNICAL REQUIREMENTS

Requirement 7: Application of defence in depth

The design and the design process shall incorporate the concept of defence in depth to all organizational, behavioral and design activities to ensure that they are subject to overlapping layers of provisions, so that if a failure or deviation from normal operation were to occur, it would be detected and compensated for, or corrected.

4.1. This process is applied throughout the design to provide a series of levels of defence aimed at preventing accidents and the uncontrolled release of radioactive materials to the environment.

4.2. The design has to 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 have to be available at all times, although some permissible relaxations are specified for the various operational modes other than power operation.

4.3. [4.1] The design therefore has to:

(1) provide multiple physical barriers to the uncontrolled release of radioactive materials to the environment, adequate protection of these barriers, and assurance of their effectiveness by the use of passive and/or active features;

(2) be conservative, and the construction has to be of high quality, so as to provide confidence that plant failures and deviations from normal operations are minimized, accidents are prevented as far as practicable, that the activation of safety systems is minimized and that there are no cliff edge effects introduced into the plant response to accidents;

(3) provide for control of the plant behaviour during and following a failure or deviation from normal operation, using inherent and engineered features, i.e. uncontrolled transients are minimized or excluded by design to the extent possible;

(4) 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 failures or deviations from normal operation;

(5) provide for equipment and procedures to control the course and limit the consequences of accidents as far as practicable; and

(6) provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation.

4.4. [4.2] To ensure that the overall safety concept of defence in depth is maintained, the design has to be such as to prevent as far as practicable:

(1) challenges to the integrity of physical barriers;

(2) failure of one or more barriers when challenged; and

(3) failure of a barrier as a consequence of failure of another barrier.

4.5. [4.3] The design has to be such that the first, or at most the second, level of defence is capable of preventing escalation to accident conditions for all failures or deviations from normal operation that are likely to occur during the service lifetime of the nuclear power plant.

Requirement 8: Fundamental safety functions

[4.6] **The following fundamental safety functions shall be ensured in all plant states of the design basis, including to the extent practicable, plant states beyond the design basis:**

(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.

4.6. [4.7] A systematic approach has to be followed to identify the structures, systems and components and inherent features that are necessary to fulfill the fundamental safety functions for all the levels of the defence in depth, following a failure or deviation from normal operation.

4.7. Monitoring of plant status has to be provided to ensure that the required safety functions are achieved, and that in the event of their actuation in the course of accident management, complementary functions are also achieved.

Requirement 9: Radiation protection and acceptance criteria

[4.11] **The design shall be such that radiation doses to the public and to site personnel do not exceed prescribed limits and are as low as reasonably achievable.**

4.8. [4.9] All actual and potential sources of radiation have to be identified and properly considered, and provision has to be made to ensure that sources are kept under strict technical and administrative control.

4.9. [4.12] The design has to ensure that plant states that could potentially result in high radiation doses or high radioactive releases have a very low likelihood of occurrence, and that the potential radiological consequences of plant states with a significant likelihood of occurrence are only minor.

4.10. [4.13]In addition to the objective of keeping radiation doses as low as reasonably achievable, a limited number of sets of radiological acceptance criteria associated with the different categories of plant states have to be established. The radiological acceptance criteria for these categories meet the requirements of the regulatory body as a minimum level of safety.

4.11. [6.22]The materials used in the fabrication of the component parts have to be selected so as to minimize as far as reasonably practicable, activation of the material.

5. REQUIREMENTS FOR PLANT DESIGN

DESIGN ENGINEERING

Requirement 10: Design basis of items important to safety

[5.4] **The design basis of all structures, systems and components important to safety shall specify the necessary capabilities for maintaining their functionality in normal operation, anticipated operational occurrences, accident conditions, conditions generated by internal and external hazards, within the defined radiological protection requirements.**

5.1. The design basis for each stage in the lifetime of the plant (construction, commissioning, operation, and decommissioning) has to be systematically documented, and has to provide the necessary information for the operating organization to operate the plant safely.

5.2. [5.4] The design basis includes the specification for all operational states and accident conditions, the safety classification, reliability, important assumptions, and the particular methods of analysis. The means of addressing and quantifying uncertainties is also included in the design basis.

Requirement 11: Design limits and acceptance criteria

[5.23] **A set of design basis limits consistent with the key physical parameters for each structure, system or component important to safety shall be specified for all operational states and accident conditions.**

5.3. The design limits have to be consistent with the current applicable standards and codes, as well as relevant regulatory requirements.

5.4. [5.7] Event sequences are grouped into a limited number of categories that correspond to plant states, according to their probability of occurrence.

5.5. [5.7] Acceptance criteria are assigned to each plant state such that frequent states have only minor or no radiological consequences and that states that may result in serious consequences are of very low probability.

5.6. [5.7] The categories typically cover:

(1) normal operation;

(2) anticipated operational occurrences, which are expected to occur during the life of the plant;

(3) design basis accidents; and

(4) beyond design basis accidents including severe accidents.

Requirement 12: Postulated initiating events

[4.7] **The design shall apply a systematic approach to identify a comprehensive set of postulated initiating events such that all credible events with potential for serious**

consequences and all credible events with significant probability have been anticipated and addressed to achieve the safety objective.

5.7. [5.9] An analysis of the postulated initiating events has to be made to establish the preventive and/or protective measures necessary to ensure that the required safety functions will be achieved.

5.8. [4.8] The expected plant response to any postulated initiating event is such that the following can reasonably be achieved (in order of importance):

(1) a postulated initiating event 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 postulated initiating event, the plant is rendered safe by passive safety features or by the action of systems that are continuously operating in the state necessary to control the postulated initiating event; or

(3) following a postulated initiating event, the plant is rendered safe by the action of safety systems that need to be brought into service in response to the postulated initiating event; or

(4) following a postulated initiating event, the plant is rendered safe by the action of safety related items; or

(5) following a postulated initiating event, the plant is rendered safe by specified procedural actions.

5.9. The postulated initiating events include all credible failures of plant systems, structures and components; human errors during operation including during shutdown and refueling modes; human errors during testing, surveillance, maintenance, and modifications irrespective of the operating mode at which these activities take place; and possible failures resulting from internal and external initiated events.

5.10. [5.8] The postulated initiating events have to be selected on the basis of a combination of engineering analysis plus deterministic or probabilistic techniques or a combination of the two, and include a full range of events to ensure that all credible events with the potential both for serious consequences or of significant probability of occurrence have been anticipated and addressed to achieve the safety objective.

5.11. The postulated initiating event used in the development of the performance requirements for the items important to safety and in the overall safety assessment and detailed analysis of the plant are limited to a number of representative event sequences that identify bounding cases and provide the basis for the design and operational limits for systems, structures and components important to safety.

Requirement 13: Exclusion of rare events

A technically supported justification shall be provided for the exclusion of any rare initiating events, sequences or situations for which it is not reasonable to set up provisions for the management of their consequences.

Requirement 14: Design rules

[5.21] **The engineering design rules for structures, systems and components shall be specified and shall comply with the appropriate accepted national or international standard engineering practices, taking into account their relevance to a nuclear power plant and whose use is also accepted by the national regulatory body.**

5.12. [5.5] Conservative design measures have to be applied and sound engineering practices have to 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 as low as reasonably achievable.

Requirement 15: Operational limits and conditions

[5.26] **The design process shall establish a set of requirements and limitations for safe operation; these shall form the basis for the establishment of operational limits and conditions under which the operating organization will be authorized to operate the plant.**

5.13. [5.26]The requirements and limitations [8] include:

(1) safety limits;

(2) limiting safety system settings;

(3) limits and conditions for normal operation;

(4) control system and procedural constraints on process variables and other important parameters;

(5) requirements for surveillance, 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;

(6) clearly defined operational configurations, including operational restrictions in the event of safety system unavailability; and

(7) action statements including completion times for actions addressing deviations from the defined operating limits and conditions.

Requirement 16: Design basis accidents

[5.27**] A set of accident conditions (design basis accidents) shall be derived from postulated initiating events for the purpose of establishing the boundary conditions that the plant has to withstand without unacceptable consequences.**

5.14. The design basis accidents are used to define the design basis for the safety systems and for the design of all other structures, systems and components important to safety that are necessary to prevent those accidents, or control and mitigate their consequences

5.15. [5.28]Where prompt and reliable action is necessary in response to a postulated initiating event, provision has to be made to initiate the necessary actions of safety systems automatically, in order to prevent progression to a more severe condition.

5.16. [5.28] Where prompt action in response to a postulated initiating event is not necessary, manual initiation of systems or other operator actions is permitted, provided that the time interval between the detection of the abnormal event and the required action is sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures), are defined to ensure the fulfillment of such actions.

5.17. [5.29] The operator actions necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner have to be taken into account and facilitated by the provision of adequate instrumentation to monitor the plant status and controls for manual operation of equipment.

5.18 The design has to specify the accident management provisions, including procedures required to provide the means for regaining control over the plant in the event of a loss of control and for mitigating any harmful consequences.

5.19. [5.30] Any equipment necessary in manual response and recovery processes has to be placed at the most suitable location to ensure its availability at the time of need and to allow safe human access for the anticipated environmental conditions.

Requirement 17: Beyond design basis accidents

[5.31] **An analysis shall be undertaken using a combination of deterministic and probabilistic approaches to determine those event sequences that could lead to conditions beyond the design basis accident conditions, without significant core degradation, and with significant core degradation (severe accidents), from which event sequences can be selected to identify the provisions for their prevention and mitigation.**

5.20. [5.31] Proper justification has to be provided for the exclusion from the design basis of severe accident sequences for which it is not reasonably practicable to implement mitigatory measures.

5.21. [5.31] Acceptable measures to address the selected event sequences do not necessarily involve the application of the conservative engineering practices used in setting and evaluating design basis accidents, but have to be based at least upon realistic or best estimate assumptions, methods and analytical criteria, and on the basis of operational experience, relevant safety analysis and results from safety research.

5.22. [5.31] The design process identifies the equipment to be used for accident management. As part of accident management, consideration has to be given to the full design capabilities of the plant, including the possible use of some equipment (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 is shown that the systems are able to function at least in the environmental conditions to be expected. For multiunit plants, consideration has to 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.

5.23. Accident management procedures have to be established, taking into account representative and dominant severe accident scenarios.

Requirement 18: Hazards

All internal and external hazards that have the potential to directly or indirectly affect the safety of the plant shall be identified and used as events that could lead to postulated initiating events to be considered in the design basis of the affected structures, systems and components. The assessment of the consequences of such events shall also be included in the analysis. The capability for achieving the fundamental safety functions shall be maintained.

Internal hazards

5.24. [5.14] The potential for equipment failures or maloperation leading to internal hazards such as fire, explosions, flooding, missile generation, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site have to be taken into account in the design basis of structures, systems and components important to safety. Appropriate preventive and mitigatory measures are provided to ensure that safety is not compromised.

5.25. [5.15] If two fluid systems that are important to safety are operating at different pressures and are interconnected, either the systems have both to be designed to withstand the higher pressure, or provision has to 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 hazards[4]

5.26. [5.16, 5.18] The design basis has to include those natural and human induced events of origin external to the plant that have been identified in the site evaluation process. It also has to take into account various interactions between the plant and the environment, including such factors as population, meteorology, hydrology, geology and seismology. 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, also have to be taken into account.

5.27. [5.10] Structures, systems and components important to safety have to be designed and located so as to minimize, consistent with other safety requirements, the probabilities and effects of fires and explosions caused by external events.

5.28. The design has to ensure that the items important to safety required to maintain safety are appropriately qualified and capable of withstanding the effects of the external events, or other features such as passive barriers are provided to protect the plant and ensure that the required safety function will be achieved.

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

5.30 For multiple-unit plant sites, the potential simultaneous impact of specific hazards on several plants on the site has to be taken into account in the design.

[4] For further requirements, see Ref. [7]

5.31. [5.19]Nuclear power plants to be sited in tropical, polar, arid or volcanic areas have to be assessed with a view to identifying special design features which are necessary as a result of the characteristics of the site.

Requirement 19: Safety classification

[5.1] **All structures, systems and components, including hardware and software for instrumentation and control, that are items important to safety shall be first identified and then classified on the basis of their significance with regard to safety functions.**

5.32. [5.2] The method for classifying the safety significance of a structure, system or component is primarily based on the potential consequences associated with the failure to perform their safety function(s), estimated on a deterministic basis complemented where appropriate by probabilistic methods, 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 their function;

(3) the probability that the item will be called upon to perform a safety function; and

(4) the time following a postulated initiating event at which, or the period throughout which, it will be called upon to operate.

5.33. [5.3] The design has to ensure that any failure of structures, systems and components in a system classified in a lower class (less stringent requirements) will not propagate to a system classified in a higher class (more stringent requirements).

5.34. Equipment (including embedded software and electrical isolation devices) that performs multiple functions has to be classified consistent with the most important function performed. Similarly equipment, regardless of its safety function, has to be classified at the highest level of the functions, systems, and equipment from which it is not independent.

Requirement 20: Reliability of structures, systems and components

[5.32] **Structures, systems and components important to safety shall be designed, qualified, procured, installed, operated, modified and maintained to be capable of withstanding all conditions defined in their design basis such that their reliability is commensurate with their safety classification and expected performance.**

Requirement 21: Common cause failures

[5.33] **The potential for common cause failures of items important to safety shall be taken into account to determine where the principles of diversity, redundancy and independence shall be applied to achieve the required reliability.**

Requirement 22: Single failure criterion

[5.34] **The single failure criterion shall be applied to each safety functional group incorporated in the plant design to perform all actions necessary in response to a particular postulated initiating event.**

5.35. Consequential failures resulting from the assumed single failure have to be considered as part of the single failure.

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

5.37. [5.37]The worst permissible configuration, capacity level, and time demand of safety systems performing the necessary safety function has to be assumed, with account taken of maintenance, testing, inspection and repair, and allowable equipment outage times.

5.38. [5.38] Non-compliance with the single failure criterion has to be exceptional, and has to be clearly justified in the safety analysis.

5.39. [5.39]In the single failure analysis, it is necessary to assume that failure of a passive component may occur. However, when it is assumed that a passive component does not fail, such an analytical approach is 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.

Requirement 23: 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 by the operator.**

Requirement 24: 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**.

.

5.40. [5.41]The reliability, redundancy, diversity and independence and the provision of features for isolation and for testing of functional capability of such services have to commensurate with the importance to safety of the system that is supported.

DESIGN FOR LIFETIME SAFE OPERATION

Requirement 25: In-service testing, maintenance, repair, refurbishment, inspection and monitoring

[5.43] **Structures, systems and components important to safety shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability to meet the reliability target over the lifetime of the nuclear power plant.**

5.41. [5.43]The plant layout has to be such that the 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.

5.42. Where systems, structures or components need to be withdrawn from the reactor for calibration, test, maintenance or refurbishment, the facilities for doing such tasks have to have standards of quality assurance and quality control for components, practices and

environment commensurate with the importance of the safety function of the items requiring calibration, test, maintenance or refurbishment.

5.43. [5.44]If the structures, systems and components important to safety are not designed to be able to be tested, inspected or monitored to the extent desirable, then a robust technical justification has to be provided that incorporates the following approach:

(1) other proven alternative and/or indirect methods such as surveillance of reference items or use of verified and validated calculational methods have to be specified; and

(2) conservative safety margins are applied or other appropriate precautions have to be taken to compensate for possible unanticipated failures.

5.44. The design has to ensure that reasonable on-line maintenance and testing of systems important to safety can be conducted without the necessity to shut down the plant.

5.45. Equipment outages, including unavailability of systems or components due to failure, have to be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system has to be included in this consideration to ensure that the safety function can still be achieved with the necessary reliability

5.46. The time allowed for outages of equipment important to safety, and the actions to be taken, have to be analysed and defined for each case before the start of plant operation and have to be included in the plant operating instructions.

Requirement 26: Equipment qualification

[5.45] **A qualification programme shall be implemented to confirm that the structures, systems and components are capable of meeting, throughout their design life and taking into account maintenance and testing programmes, and the demands for performing their intended functions in the environmental conditions prevailing at the time of need.**

5.47. [5.45]The environmental conditions considered have to include the variations expected in the ambient conditions in normal operation, anticipated operational occurrences and design basis accidents, and where appropriate beyond design basis accidents including severe accidents. In the qualification programme, consideration has to be given to ageing effects caused by various environmental factors (such as vibration, irradiation, temperature, etc) 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 has to 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.

5.48. [5.46]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, have to be included in the qualification programme.

5.49. [5.46]Equipment that is credited to operate during beyond design basis accidents and during and after severe accidents has to be shown to be capable of performing its intended function under the expected environmental conditions. A qualification programme, or justifiable extrapolation of equipment behavior, based on design specifications, environmental

qualification testing, or other considerations has to be used to provide assurance on operability.

Requirement 27: 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, neutron embrittlement 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.**

5.50. [5.47]Ageing and wear-out effects in all normal operating conditions, testing, maintenance, maintenance outages, plant states in a postulated initiating event and post-postulated initiating event have to be taken into account.

5.51. [5.47]Provision has to 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

Requirement 28: Design for optimal operator performance

[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.**

5.52. The users (or user representatives) have to be actively involved in the design process in an iterative way in order to ensure that their needs are adequately considered.

5.53. [5.48]The design has to be aimed at supporting plant personnel (users) in the fulfillment of their tasks and responsibilities, and at limiting the effects of human errors that can impact upon safety. Attention has to be paid to plant layout and procedures (administrative, operational and accident management), including maintenance and inspection, in order to facilitate the interface between the operating personnel and the plant.

5.54 [5.51] The human–machine interface has to be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times.

5.55. [5.53]The operator has to be considered to have dual roles: that of a systems manager, including accident management, and that of an equipment operator.

5.56. [5.54]In the system manager role, the operator has to 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.

5.57. [5.55] As equipment operator, the operator has to be provided with sufficient information to operate the plant within the specified limits on parameters associated with individual plant systems and equipment to confirm that the necessary safety actions can be initiated safely.

5.58. [5.56] The design has to 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.

5.59. [5.56] The need for intervention by the operator on a short time-scale has to be kept to a minimum and it has to be demonstrated 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.

5.60. [5.49] The working areas and working environment of the site personnel have to be designed according to ergonomic principles.

5.61. [5.52] Verification and validation of aspects of human factors have to be included at appropriate stages to confirm that the design adequately specifies all necessary operator actions.

OTHER DESIGN CONSIDERATIONS

Requirement 29: Sharing of structures, systems and components between nuclear power plants

[5.57] **Structures, systems and components important to safety shall not be shared between two or more reactors in nuclear power plants unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and removal of residual heat from the remaining units.**

Requirement 30: 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:**

(1) prevent the occurrence of events that can lead to releases to the environment,

(2) prevent accidental criticality and overheating,

(3) ensure that the release of radioactive materials is below prescribed limits and as low as reasonably achievable in all operational states, and

(4) facilitate the mitigation of radiological consequences of design basis accidents.

Requirement 31: 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, and accident conditions.**

Requirement 32: Escape routes

[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.**

5.62. [5.61]The escape routes have to meet the relevant national/ international requirements for radiation zoning and fire protection and the relevant national requirements for industrial safety and plant security.

Requirement 33: Communication systems

[5.62]. **Effective means of communication shall be provided throughout the plant to facilitate safe operation in all modes of operation and following all postulated initiating events and accidents.**

5.63. [5.62]Suitable alarm systems and means of communication have to be provided so that all persons present in the plant and on the site can be warned and instructed, even under accident conditions.

5.64. [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, has to be ensured at all times and has to be taken into account in the design and the diversity of the methods of communication selected.

Requirement 34: Control of access to the plant

[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.**

5.65. [5.64]Provision has to be made in the design of the buildings and the layout of the site for the control of access of personnel and/or equipment to the plant, with particular reference to guarding against the unauthorized entry of persons and goods to the plant.

Requirement 35: Prevention of interference with items important to safety

[5.65] **Unauthorized access to, or interference for any reason with, structures, systems and components important to safety, including computer software and hardware, shall be prevented.**

5.66. [5.65]Where access is necessary for maintenance, testing or inspection purposes, it has to be ensured in the design that the necessary activities can be performed without significantly reducing the reliability of the associated safety related equipment.

Requirement 36: Interactions of systems

[5.66] **The potential interaction of systems important to safety that may be required to operate simultaneously shall be evaluated.**

5.67. [5.66]In the analysis, account has to be taken of physical interconnections, and 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.

Requirement 37: Interactions between the electrical power grid and the plant

[5.67] **Account shall be taken of power grid–plant interactions, including the independence of and number of power supply lines to the plant, potential variations in grid supply voltage and frequency, and system fault levels in relation to the necessary reliability of the power supply to plant systems important to safety.**

Requirement 38: Features to facilitate 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.**

5.68. [5.68]In particular, account has to 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 and means of handling that may be necessary; and

(3) the facilities necessary for storing radioactive waste generated in operation and the programmes to accommodate the waste generated in the decommissioning of the plant.

SAFETY ANALYSIS[5]

Requirement 39: Safety analysis of the plant design

[5.69] **A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied to enable the challenges to safety under the various categories of plant states to be evaluated and assessed.**

5.69. [5.69]The safety analysis establishes and confirms the design basis for items important to safety. It also has to 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 the plant states within the design basis.

5.70. The safety analysis confirms that the instrumentation and control design is such that:

(1) assumed actuation points are consistent with instrument channel setpoints in consideration of setpoint uncertainty.

(2) assumed human response times are consistent with human machine interface and instrumentation and control design

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

(3) the safety analyses take account of all credible conditions that might be caused or augmented by any non-safety digital control system or the safety-related control and protection system, such as multiple spurious actuations; and
(4) Maloperation of the non-safety control system will not place the plant in a condition that is inconsistent with the safety analysis assumptions.

5.71. [5.69] The safety analysis provides assurance that, in design, defence in depth has been implemented.

5.72. [5.70] The computer programs, analytical methods and plant models used in the safety analysis have to be verified and validated, and adequate consideration has to be given to uncertainties.

Deterministic approach

5.73. [5.71] The deterministic safety analysis mainly provides:

(1) establishment and confirmation of the design bases for all structures, systems and components important to safety;

(2) characterization of the postulated initiating events that are appropriate for the design and site of the plant;

(3) analysis and evaluation of event sequences that result from postulated initiating events to confirm the qualification requirements;

(4) comparison of the results of the analysis with radiological acceptance criteria and design limits; and

(5) 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.

5.74. [5.72] The applicability of the analytical assumptions, methods and degree of conservatism used has to be verified. The safety analysis of the plant design has to be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and has to be consistent with the current or 'as built' state.

Probabilistic approach

5.75. [5.73] The design has to take account of the probabilistic safety analysis of the plant in all modes of operation and plant states, with particular reference:

(1) to establish that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety; and

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

6. ADDITIONAL REQUIREMENTS FOR DESIGN OF SPECIFIC PLANT SYSTEMS

REACTOR CORE AND ASSOCIATED FEATURES

Requirement 40: 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 and radiological acceptance criteria are not exceeded in all operational states, and in accident conditions, with account taken of the existing uncertainties.**

6.1. The reactor core and associated internal components located within the reactor vessel have to 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.

6.2. [6.3] The maximum degree of positive reactivity and its maximum rate of increase by insertion in operational states and design basis accidents have to be limited so that no resultant failure of the reactor coolant boundary will occur, cooling capability will be maintained and no significant damage will occur to the reactor core.

6.3. [6.4] The possibility of a recriticality or a reactivity excursion that results in exceeding fuel design limits following a postulated initiating event has to be precluded by design.

Requirement 41: Performance of fuel elements and assemblies

[6.6] **Fuel elements and assemblies shall be designed to maintain their structural integrity and 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.**

6.4. [6.7] The deterioration considered has to 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 has to be made for uncertainties in data, calculations and fabrication.

Requirement 42: Fuel element capability in design basis accidents

[6.9] **The fuel elements shall be designed to remain in position and not suffer distortion in design basis accidents 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.**

6.5. [6.8] Specified fuel design limits, including permissible leakage of fission products, have to encompass the plant operational states that may be imposed in anticipated operational occurrences such that the fuel remains fit for continued service.

Requirement 43: Control of the reactor core

[6.11]**The core shall remain stable in normal operation, and the demands made on the control system for maintaining flux shapes, levels and stability within specified limits in all operational states shall be minimized.**

6.6. [6.11] Adequate means of detecting the flux distributions have to be provided to ensure that there are no regions of the core in which the design limits could be exceeded without being detected.

Requirement 44: Reactor shutdown

[6.13] **Means shall be provided to ensure that there is a capability to shut down the reactor in operational states, design basis accidents and in external events within the design basis, and that the shutdown condition can be maintained even for the most reactive core conditions.**

6.7. [6.17] 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 have to be considered.

6.8. [6.14] The means for shutting down the reactor has to consist of at least two diverse systems.

6.9. [6.16] At least one of these two systems has to be capable of rendering the reactor subcritical from normal power 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.

6.10. [6.18]The means of shutdown has to be adequate to prevent or withstand any credible increase in reactivity by insertion during the shutdown, including refuelling or other routine operations in the shutdown state.

6.11. [6.19]Instrumentation has to be provided and tests specified to ensure that the shutdown means are always in the state stipulated for the given plant condition.

6.12. [6.20]In the design of reactivity control devices, account has to be taken of wear-out, and effects of irradiation, such as burnup, changes in physical properties and production of gas.

REACTOR COOLANT SYSTEM

Requirement 45: Design of the reactor coolant system

[6.21] **The reactor coolant system and its associated auxiliary systems shall be designed with sufficient margin to ensure that the design limits of the fuel and reactor coolant boundary are not exceeded in operational states.**

6.13. [6.21]Pipework connected to the reactor coolant boundary has to be equipped with adequate isolation devices to limit any loss of radioactive fluid.

6.14. [6.23]The components of the reactor coolant system have to be designed and constructed to be of the highest quality with respect to materials, design standards, capability of inspection and fabrication.

6.15. [6.24]The reactor coolant boundary has to 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).

6.16. [6.24]The design has to ensure that plant states in which components of the reactor coolant boundary could exhibit brittle behaviour are avoided.

6.17. [6.26]The design of the components contained inside the reactor coolant boundary, such as pump impellers and valve parts, has to 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.

Requirement 46: Protection of the coolant boundary

[6.21] **Provision shall be made to ensure that the operation of pressure relief devices, even in design basis accidents, will protect the RCS pressure boundary from overpressure and will not lead to unacceptable releases of radioactive material from the plant.**

Requirement 47: Inventory of reactor coolant

[6.31] **Provision shall be made for controlling the inventory, temperature and pressure of the coolant to ensure that specified design limits are not exceeded in any operational state, with volumetric changes and leakage taken into account.**

Requirement 48: Cleanup of the reactor coolant

[6.32] **Adequate facilities shall be provided for removal of non-radioactive and radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel.**

6.18. [6.32]The capabilities of the necessary systems have to 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.

Requirement 49: Removal of residual heat from the core

[6.33] **Reliable means for removing residual heat from the reactor core shall be provided such that the design basis limits of the fuel, reactor coolant boundary and structures important to safety are not exceeded.**

Requirement 50: Emergency core cooling

[6.35] **Core cooling shall be provided to restore and maintain fuel cooling under accident conditions even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.**

6.19. [6.35]The cooling provided has to 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.

6.20. [6.36]Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable redundancy and diversity in components have to be provided in order to fulfil these requirements with sufficient reliability for each postulated initiating event, on the assumption of a single failure.

Requirement 51: 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.**

6.21. [6.39]All systems that contribute to the transport of heat (by conveying heat, by providing power or by supplying fluids to the heat transport systems) have to be designed in accordance with the importance of their contribution to the function of heat transfer.

CONTAINMENT STRUCTURE AND SYSTEM

Requirement 52: Design of the containment system

[6.43] **A containment system shall be provided to ensure or contribute to the achievement of the following safety functions:**

(1) Confinement of radioactive substances in operational states and in accident conditions,

(2) Protection of the reactor against external natural and human induced events, and

(3) **Radiation shielding in operational states and in accident conditions.**

6.22. [6.43]The containment system design has to ensure that any release of radioactive materials to the environment in a design basis accident is below prescribed limits. The system has to include, depending on design requirements: leaktight structures; associated systems for the control of pressures, temperatures and moisture levels; and features for the isolation, management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.

6.23. [6.45] The strength of the containment structure, including access openings and penetrations and isolation valves, has to be calculated with sufficient margins of safety on the basis of the potential internal overpressures, underpressures and temperatures, dynamic effects such as missile impacts caused by the event, reaction forces anticipated to arise as a result of design basis accidents, and end of life properties affected by ageing.

6.24. [6.46] The design has to include measures to avoid failure of the containment during severe accident sequences that can challenge the containment integrity.

6.25. [6.45 The effects of other potential energy sources, including, for example, possible chemical and radiolytic reactions, have to be also considered. In calculating the necessary strength of the containment structure, natural phenomena and human induced events have to be taken into consideration, and provision has to be made to monitor the condition of the containment and its associated features.

Requirement 53: Control of containment leakage

[6.48] **The containment system shall be designed so that the prescribed maximum leakage rate is not exceeded in design basis accidents, and as low as possible in beyond design basis accidents.**

6.26. [6.48] Provision has to be made for the collection and controlled release or storage of materials that may leak from the primary containment to the environment.

6.27. [6.49] The containment structure and equipment and components affecting the leaktightness of the containment system have to be designed and constructed so that the leak rate can be tested at the design pressure after all penetrations have been installed.

6.28. [6.49] Determination of the leakage rate of the containment system at periodic intervals over the service lifetime of the reactor has to be possible, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.

6.29. [6.51, 6.52] The number of penetrations through the containment has to be kept to a practical minimum, and all penetrations meet the same design requirements as the containment structure itself. They are protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles caused by the event, jet forces and pipe whip.

Requirement 54: Containment isolation

[6.55] **Each line that penetrates the containment as part of the reactor coolant boundary or that is connected directly to the containment atmosphere shall be designed to fail safe such that it will 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.**

6.30. [6.55] The lines have to 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), located as close to the

containment as is practicable and each valve is capable of being reliably and independently actuated and periodically tested.

631. [6.56] Each line that penetrates the primary reactor containment and is neither part of the reactor coolant boundary nor connected directly to the containment atmosphere has to have at least one adequate containment isolation valve. These valves have to be outside the containment and have to be located as close to the containment as practicable.

Requirement 55: Containment access

[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.**

6.32. [6.58] Where provision is made for entry of personnel for surveillance purposes, provisions for ensuring the safety of personnel have to be specified in the design. These requirements also apply to equipment air locks, where provided.

Requirement 56: Control of the containment atmosphere

Provision shall be made to control the pressure, temperature, and the buildup of fission products or other gaseous or solid substances that may occur within the containment.

6.33. [6.60] The design has to provide for ample flow routes between separate compartments inside the containment. The cross-sections of openings between compartments have to be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in damage to the pressure bearing structure or to other systems of importance in limiting the effects of accident conditions.

6.34. [6.62] The capability to remove heat from the reactor containment has to be ensured by the reduction of 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 has to have adequate reliability and redundancy to ensure that this can be fulfilled, on the assumption of a single failure.

6.35. [6.64] Systems to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment have to be provided as necessary to:

(1) reduce the amount of fission products that might be released to the environment in accident; conditions, and

(2) 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.

6.36. [6.67] The coverings and coatings for components and structures within the containment system have to be carefully selected, and the methods of application specified, to ensure fulfilment of their safety functions and to minimize interference with other safety functions in the event of the deterioration of the coverings and coatings.

INSTRUMENTATION AND CONTROL SYSTEMS

Requirement 57: Provision of instrumentation

[6.68] **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, for obtaining any information on the plant necessary for its reliable and safe operation, and for determining the status of the plant in a severe accident and for taking decisions in accident management.**

Requirement 58: Control systems

[6.70] **Appropriate and reliable control systems shall be provided to maintain the variables referred to in Requirement 57 within the specified operational ranges.**

6.37. [6.69]Instrumentation and recording equipment has to 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 the locations and quantities of radioactive materials that could escape from the locations intended in the design.

Requirement 59: Protection system

A protection system shall be provided that has the capability to sense unsafe conditions and automatically initiate the operation of the appropriate systems required for achieving and maintaining a safe condition.

6.38. [6.80]The protection system has to be designed:

(1) to be capable of overriding unsafe actions of the control system; and

(2) to achieve a safe condition in case of failure.

6.39. [6.84]The design has to be such as to:

(1) prevent operator action that could defeat the effectiveness of the protection system in normal operations and anticipated operational occurrences, but not to negate correct operator actions in design basis accidents; and

(2) minimize the need for operator action in response to any accident or postulated initiating event, and provides for timely action consistent with the safety analyses when operator action is needed.

Requirement 60: Reliability and testability of instrumentation and control safety systems

[6.81] **Instrumentation and control safety systems shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed, and shall meet the single failure criterion.**

6.40. [6.82]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 have to be used to the extent practicable to prevent loss of a protection safety function.

6.41. [6.83] The safety systems have to be designed to permit periodic testing of their 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 has to permit all aspects of functionality from the sensor to the input signal to the final actuator or display to be tested in operation.

6.42. [6.83] Where a safety system, or part of a safety system is required to be taken out of service for testing, adequate provision has to be made for the clear indication of any protection system bypasses that are necessary for the duration of the test or maintenance activity.

Requirement 61: Use of computer based equipment 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 computer based equipment, 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.**

6.43. [6.77] The level of reliability of the computer software has to be commensurate with the safety importance of the system. The necessary level of reliability is 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.

6.44. [6.85] Where computer based equipment is used in a safety system, the following requirements also apply:

(1) a very high quality of, and best practices for, hardware and software are used;

(2) the whole development process, including control, testing and commissioning of the design changes, are systematically documented and reviewable;

(3) in order to confirm confidence in the reliability of the computer based equipment, an assessment by expert personnel independent of the designers and suppliers is undertaken;

(4) where the necessary integrity of the equipment cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfillment of the protection functions is provided; and

(5) software based common-cause failures are taken into consideration.

Requirement 62: Separation of safety systems

[6.86] **Interference between the safety systems and systems of lower classification or between redundant elements of systems of the same class shall be prevented by means such as physical separation of safety systems, electrical isolation, functional independence and communications (data transferring) independence as appropriate**.

6.45. [6.86]If signals are used in common by both a safety system and any control system, appropriate separation (such as by adequate decoupling) has to be ensured and the signal source has to be classified as part of the higher-class system.

6.46. Safety system equipment (including cables and raceways) has to be readily identifiable in the plant for each redundant portion of a safety system.

Requirement 63: Control room

[6.71] **A control room shall be provided from which the plant can be safely operated in all its operational states either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after the onset of anticipated operational occurrences or accident conditions.**

6.47. [6.71]Appropriate measures have to be taken and adequate information is provided to safeguard the occupants of the control room against hazards, such as high radiation levels resulting from an accident condition or the release of radioactive material, or explosive or toxic gases.

6.48. [6.72]Special attention has to 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 has to provide for reasonably practicable measures to minimize the effects of such events.

Requirement 64: Supplementary control room

[6.75] **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, from which 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.**

6.49. The measures stated in para 6.47 for the protection of operating staff also have to be applied to the supplementary control room.

Requirement 65: Emergency control centre

[6.87] **An on-site emergency control centre, separated from the plant control room, shall be provided from which the emergency response can be directed.**

6.50. [6.87]Information about important plant parameters and radiological conditions in the plant and its immediate surroundings has to be provided. The centre provides 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 have to be taken to protect the occupants for a protracted time against hazards resulting from accident conditions.

Requirement 66: Emergency power supply

[6.88] **The emergency power supply shall be capable of supplying the necessary power in any operational state or in accident conditions, on the assumption of the coincidental loss of off-site power.**

6.51. [6.88]The design basis for the emergency power supply has to take account of the postulated initiating events to be addressed, and the associated safety duties to be performed to determine the required capability, availability, duration of the required demand, its capacity and requirement for continuity.

6.52. [6.89]The combined means to provide emergency power (such as by means of water, steam or gas turbine, diesel engines or batteries) have to have a reliability and form that are consistent with all the requirements of the safety systems to be supplied, and have to perform their functions on the assumption of a single failure.

6.53. The design basis for any safety related diesel or other prime mover powered system that provides a supply to a safety related system has to include:

(1) the capability of the associated fuel oil storage and transfer systems to satisfy the required demand;

(2) the capability of the starting system to operate successfully under all specified conditions and at the required time; and

(3) the auxiliary systems, such as cooling.

AUXILIARY SYSTEMS

Requirement 67: Reliability of auxiliary systems.

The design measures provided for auxiliary systems shall ensure that the required reliability is consistent with the associated component or system.

Requirement 68: Process and post accident sampling systems

Process and post accident sampling systems shall be provided for determining in a timely manner the concentration of selected radionuclides in fluid process systems, and in gas and liquid samples taken from systems or the environment, in operational states and accident conditions.

6.54. Appropriate means have to be provided to allow monitoring of the activity in fluid systems that have a potential for significant contamination, and for the collection of process samples.

Requirement 69: Auxiliary heat transport systems

Auxiliary heat transport systems shall be provided as appropriate to remove heat from components and systems that are essential to the safe shutdown of the plant in normal operation and accident conditions.

6.55. The design has to ensure that non-essential portions of the system can be isolated.

Requirement 70: Compressed air systems

The design basis of any compressed air system that provides a service to an item important to safety shall specify the quality and cleanliness of the air to be provided.

Requirement 71: Air conditioning and ventilation systems

Air conditioning, heating, cooling and ventilation systems shall be provided as appropriate in auxiliary rooms or plant areas to maintain the required environmental conditions for components and systems important to safety in normal operation and accident conditions.

Requirement 72: Fire protection systems

[5.12] **Fire protection systems, including detection and extinguishing systems, fire containment barriers, and smoke control systems shall be installed throughout the plant as determined from the fire hazard analysis.**

6.56. The fire extinguishing systems have to be automatically initiated where appropriate. Systems have to 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.

6.57. The fire detection systems have to be designed to inform the operators promptly of the location and spread of any fires which start.

6.58. Fire detection and extinguishing systems that are required to protect against a potential fire following a postulated initiating event have to be appropriately qualified to resist the effects of the postulated initiating event.

6.59. [5.13]Non-combustible or fire retardant and heat resistant materials have to be used wherever practicable throughout the plant, particularly in locations such as the containment and the control room.

Requirement 73: Lighting systems

Adequate lighting shall be provided to facilitate safe operation in normal operation and accident conditions in all operational areas.

Requirement 74: Overhead lifting equipment

Equipment shall be provided for lifting and lowering items important to safety, or for lifting and lowering other items in the proximity of items important to safety.

6.60. The lifting equipment has to be designed such that:

(1) measures are provided to prevent the lifting of unacceptable, or excessive loads.

(2) conservative design measures are applied to minimize the likelihood of an uncontrolled load drop, and

(3) the plant layout facilitates the safe movement of the equipment being transported.

OTHER POWER CONVERSION SYSTEMS

Requirement 75: Steam supply system, feedwater, and turbine generators

The design of the steam supply system shall ensure that the appropriate design limits of the reactor coolant boundary are not exceeded in normal operation, anticipated operational occurrences, and design basis accident conditions.

6.61. The design of the steam supply system has to provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions.

6.62. Steam and feed water systems have to be of adequate capacity and have to be designed to prevent anticipated operational occurrences escalating into accident conditions

6.63. The turbine generators have to be provided with appropriate protection such as overspeed and vibration, and measures have to be taken to minimize the potential effects of turbine disintegration on items important to safety.

6.64. Measures have to be provided to minimize any interaction between buildings containing safety-related structures, systems and components (including power and control cabling) and any other plant structure resulting from external events such as earthquake and high winds (e.g., tornado, hurricane, etc.).

RADIOACTIVE WASTE MANAGEMENT

Requirement 76: Waste treatment and control systems

[6.90] **Systems shall be provided to treat radioactive solid, liquid and gaseous effluents in order to keep the quantities and concentrations of radioactive discharges within prescribed limits and as low as reasonably achievable.**

6.65. [6.91]Systems have to 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.

6.66. The generation of gaseous, liquid and solid waste has to be kept as low as reasonably achievable. Gaseous and liquid arisings have to be treated so that the exposure to radiation of members of the public due to any discharges to the environment is as low as reasonably achievable.

6.67. [6.92]The plant has to 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.

6.68. [6.93]Building ventilation systems, with appropriate levels of cleanup capability have to be provided to do the following:

(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;

(4) to ventilate rooms containing inert or noxious gases without impairing the capability to control radioactive releases; and

(5) control of releases of gaseous radioactive material to the environment within prescribed limits and as low as reasonably achievable.

6.69. [6.95] The offgas/extract stream cleanup equipment has to provide the necessary retention factor to meet the discharge limits and the filter systems are designed such that their efficiency can be tested.

FUEL HANDLING AND STORAGE SYSTEMS

Requirement 77: Fuel handling and storage systems

Fuel handling and storage systems shall be provided to ensure that the integrity and properties of the fuel are maintained at all times during handling and storage.

Transport and packaging for fuel and radioactive waste

6.70. [5.60] The design has to incorporate appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste. Consideration has to be given to access to facilities and lifting and packaging capabilities.

Handling and storage of non-irradiated fuel

6.71. [6.96] The handling and storage systems for non-irradiated fuel have to be designed to do the following:

(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 inspection of new fuel;

(3) to permit appropriate maintenance, periodic inspection and testing of components important to safety;

(4) to minimize the probability of loss of or damage to the fuel;

(5) to provide for identification of fuel bundles;

(6) to provide proper means for radiation protection; and

(7) to ensure that adequate operating and accounting procedures can be implemented to prevent any loss of fuel.

Handling and storage of irradiated fuel

6.72. [6.97] The handling and storage systems for irradiated fuel have to be designed:

(1) to prevent criticality by physical means or processes, preferably by 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;

(14) to ensure that adequate operating and accounting procedures can be implemented to prevent any loss of fuel; and

(15) to accommodate all the fuel discharged from the reactor according to the foreseen core management strategy and the full core, with adequate margins.

6.73. [6.98]For reactors using a water pool system for fuel storage, the design has to includethe following:

(1) means for controlling the temperature, 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 (antisyphon measures).

RADIATION PROTECTION [10]

Requirement 78: Design for radiation protection

[6.101] **The design shall ensure that the exposure to radiation of plant personnel and members of the public remains below the prescribed limits and as low as reasonably achievable during normal operation, anticipated operational occurrences, following design basis accidents and during decommissioning.**

[10] For further requirements, see Ref. [10].

6.74. The sources of radioactivity throughout the plant have to be comprehensively identified and kept as low as reasonably achievable, the integrity of the fuel cladding is maintained, and the production and transport of corrosion and activation products is controlled.

6.75. The plant has to be divided into radiation zones which are related to their expected occupancy, and shielding has to be provided so that the exposure to radiation is kept as low as reasonably achievable.

6.76. The plant layout has to ensure that access of personnel to radiation areas and areas of potential contamination is adequately controlled, and that, together with the ventilation systems provided, any airborne activity is confined.

6.77. The plant layout has to ensure that the time spent by personnel in radiation areas during normal operation, refueling, maintenance and inspection is reduced as low as reasonably achievable, and the requirements of special equipment that is provided to achieve these objectives have to be taken into account.

6.78. [6.104] Facilities have to be provided for the decontamination of personnel, plant and equipment, and for handling radioactive waste arising from decontamination activities.

Requirement 79: 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, beyond design basis accidents including severe accidents**.

6.79. [6.105(1)] Stationary dose rate meters have to be provided for monitoring the local radiation dose rate at places routinely accessible by operating personnel and where the changes in radiation levels in normal operation or anticipated operational occurrences may be such that access is limited for certain specified periods of time.

6.80. [6.105(2)] Stationary dose rate meters have to 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 have to provide sufficient information in the control room or at the appropriate control position that plant personnel can initiate corrective action if necessary.

6.81. [6.105(3)] Stationary monitors have to be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by personnel and where the levels of airborne activity may on occasion be expected to be such as to necessitate protective measures. These systems have to provide an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected. Monitors also have to be located in areas possibly subject to contamination as a result of equipment failure or other unusual circumstances.

6.82. [6.105 (4)] Stationary equipment and laboratory facilities have to 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.

6.83. [6.105 (5)] Stationary equipment has to be provided for monitoring the effluents prior to or during discharge to the environment.

6.84. [6.105 (6)] Instruments have to be provided for measuring radioactive surface contamination.

6.85. [6.105 (7)] Facilities have to be provided for monitoring for individual doses to, and contamination of, personnel.

6.86. [6.106] Arrangements also have to be made to determine the radiological impact, if any, in the vicinity of the plant by surveillance of radioactivity concentrations and contaminations and dose and dose rates 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.

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, NTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life, INSAG-19, IAEA, Vienna (2003).

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

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, Safety Requirements NS-R-3, Vienna (2003).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna (200?)

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, IAEA, Vienna (2007).

[10] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996)

[11] Relevant Nuclear Security Series publications (to be finalized)

CONTRIBUTORS TO DRAFTING AND REVIEW

Antalik, R.	Nuclear Regulatory Authority of Slovak Republic, Slovak Republic
Aza, Z.M.	Atomic Energy Agency Organization of Iran (AEOI), Iran
Borysova, I.	World Nuclear Association (WNA), U.K.
Buttery, N.	British Energy Generation Ltd., U.K.
Carluec, B.	AREVA NP, France
Cowley, J.S.	Private Consultant, UK
Downing, D.J.	Pebble Bed Modular Reactor (PBMR), South Africa
El-Shanawany, M.	INTERNATIONAL ATOMIC ENERGY AGENCY
Englebert, B.	Suez-Tractebel, Belgium
Fiorini, G.L.	CEA/Cadarache/DEN/DER/SESI, France
Froehmel, T.	World Nuclear Association (WNA), U.K.
Gasparini, M.	INTERNATIONAL ATOMIC ENERGY AGENCY
Ghadge, S.G.	Nuclear Power Corporation of India Ltd. (NPCIL), India
Kurkowski, L.	EDF-SEPTEN, France
Matsumoto, T.	Japan Nuclear Energy Safety Organization (JNES), Japan
Mertins, M.	Gessellschaft für Anlagen und Reaktorsicherheit (GRS) GmbH, Germany
Pabarcius, R.	Lithuanian Energy Institute, Lithuania
Perez, J.-R.	ASN/Directorate of Nuclear Power Plants (Nuclear Safety Authority) France
Semanas, R.	State Nuclear Power Safety Inspectorate, Lithuania
Tronea, M.	National Commission for Nuclear Activities Control, Romania
Uhrik, P.	Nuclear Regulatory Authority of Slovak Republic, Slovak Republic
Valtonen, K.	STUK-Radiation and Nuclear Safety Authority, Finland

Yashimura, K.	Secretariat of the Nuclear Safety Commission, Japan
Zaiss , W.	ENISS/FORATOM, Belgium
Zemdegs, R.	Atomic Energy of Canada Ltd. (AECL), Canada
Ziakova, M.	Nuclear Regulatory Authority of Slovak Republic, Slovak Republic