NS-R-1 Rev 26, 28 September 2010

IAEA SAFETY STANDARDS

for protecting people and the environment

Status:
Includes resolution of comments from Member States
Includes input from NUSSC WG 6-9 September 2010
To be discussed at the Safety Standards Committees on November-December 2010 for submission to CSS

Safety of Nuclear Power Plants: Design

DRAFT SAFETY REQUIREMENTS No. SSR 2/1 DS414

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

IAEA
International Atomic Energy Agency

CONTENTS

1. INTRODUCTION 1

BACKGROUND 1
OBJECTIVE 2
SCOPE 2
STRUCTURE 3

2. APPLYING THE SAFETY OBJECTIVE, SAFETY PRINCIPLES AND CONCEPTS 3

RADIATION PROTECTION 4
SAFETY IN DESIGN 5
THE CONCEPT OF DEFENCE IN DEPTH 6
THE CONCEPT OF MAINTAINING THE INTEGRITY OF DESIGN OF THE PLANT THROUGHOUT THE OPERATING LIFETIME 8

3. MANAGEMENT OF SAFETY IN DESIGN 9

Requirement 1: Responsibilities in the management of safety in design 9
Requirement 2: Management system for the plant design 9
Requirement 3: Safety of the design throughout the plant lifetime 10

4. PRINCIPAL TECHNICAL REQUIREMENTS 11

Requirement 4: Fundamental safety functions 11
Requirement 5: Radiation protection and acceptance criteria 12
Requirement 6: Design of the nuclear power plant 12
Requirement 7: Application of defence in depth 13
Requirement 8: Safety, safeguards and security interfaces 15
Requirement 9: Proven engineering practices 15
Requirement 10: Safety assessment 16
Requirement 11: Provision for construction 16
Requirement 12: Features to facilitate decommissioning 16

5. PLANT DESIGN 17

DESIGN BASIS 17
Requirement 13: Categories of plant states 17
Requirement 14: Design basis for items important to safety 18
Requirement 15: Design limits 18
Requirement 16: Postulated initiating events 18
Requirement 17: Hazards 20
Requirement 18: Engineering design rules 21
Requirement 19: Operational limits and conditions 22
Requirement 20: Design basis accidents 22
Requirement 21: Design extension conditions 23
Requirement 22: Separation and independence of safety systems 25
Requirement 23: Safety classification 25
Requirement 24: Reliability of items important to safety 26
Requirement 25: Common cause failures 26
Requirement 26: Single failure criterion 26
Requirement 27: Fail-safe design 27

Requirement 28: Support service systems 27
DESIGN FOR LIFETIME SAFE OPERATION 27
Requirement 29: Maintenance, testing, repair, replacement, inspection and monitoring 27
Requirement 30: Equipment qualification 28
Requirement 31: Ageing management 29
HUMAN FACTORS 30
Requirement 32: Design for optimal operator performance 30
OTHER DESIGN CONSIDERATIONS 31
Requirement 33: Sharing of safety systems between nuclear power plant units 31
Requirement 34: Systems containing fissile material or radioactive material 31
Requirement 35: Power plants used for cogeneration of heat and power, heat generation or desalination 32
Requirement 36: Escape routes 32
Requirement 37: Communication systems 32
Requirement 38: Control of access to the plant 33
Requirement 39: Prevention of interference with items important to safety 33
Requirement 40: Interactions of systems 33
Requirement 41: Interactions between the electrical power grid and the plant 34
SAFETY ANALYSIS 34
Requirement 42: Safety analysis of the plant design 34

6. DESIGN OF SPECIFIC PLANT SYSTEMS 36

REACTOR CORE AND ASSOCIATED FEATURES 36
Requirement 43: Performance of fuel elements and assemblies 36
Requirement 44: Structural capability of the reactor core 36
Requirement 45: Control of the reactor core 37
Requirement 46: Reactor shutdown 37
REACTOR COOLANT SYSTEM 38
Requirement 47: Design of the reactor coolant system 38
Requirement 48: Overpressure protection of the coolant pressure boundary 39
Requirement 49: Inventory of reactor coolant 39
Requirement 50: Cleanup of the reactor coolant 39
Requirement 51: Removal of residual heat from the core 39
Requirement 52: Emergency core cooling 39
Requirement 53: Heat transfer to an ultimate heat sink 40
CONTAINMENT STRUCTURES AND SYSTEMS 40
Requirement 54: Containment system 40
Requirement 55: Control of releases from the containment 41
Requirement 56: Containment isolation 41
Requirement 57: Containment access 42
Requirement 58: Control of containment conditions 42
INSTRUMENTATION AND CONTROL SYSTEMS 43
Requirement 59: Provision of instrumentation 43
Requirement 60: Control systems 44
Requirement 61: Protection system 44
Requirement 62: Reliability and testability of instrumentation and control of items important to safety 44
Requirement 63: Use of computer based equipment in systems important to safety 45
Requirement 64: Separation of protection systems and control systems 46
Requirement 65: Control room 46

Requirement 66: Supplementary control room 46
Requirement 67: Emergency control centre 47
EMERGENCY POWER SUPPLY 47
Requirement 68: Emergency power supply 47
SUPPORTING AND AUXILIARY SYSTEMS 48
Requirement 69: Performance of supporting and auxiliary systems. 48
Requirement 70: Auxiliary heat transport systems 48
Requirement 71: Process sampling systems and post-accident sampling systems 48
Requirement 72: Compressed air systems 49
Requirement 73: Air conditioning systems and ventilation systems 49
Requirement 74: Fire protection systems 49
Requirement 75: Lighting systems 50
Requirement 76: Overhead lifting equipment 50
OTHER POWER CONVERSION SYSTEMS 51
Requirement 77: Steam supply system, feedwater system and turbine generators 51
TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE 51
Requirement 78: Waste treatment and control systems 51
Requirement 79: Effluent treatment and control systems 52
FUEL HANDLING AND STORAGE SYSTEMS 52
Requirement 80: Fuel handling and storage systems 52
RADIATION PROTECTION 54
Requirement 81: Design for radiation protection 54
Requirement 82: Means of radiation monitoring 55

REFERENCES 57

DEFINITIONS 60

CONTRIBUTORS TO DRAFTING AND REVIEW 61

1. INTRODUCTION

BACKGROUND

1.1. The present publication supersedes the Safety Requirements publication on Safety of Nuclear Power Plants: Design (IAEA Safety Standards Series No. NS-R-1, issued in 2000). It takes account of the publication of the Fundamental Safety Principles in 2006 [1]. Requirements for nuclear safety are intended to ensure the highest level of safety that can reasonably be achieved for the protection of workers, the public and the environment from harmful effects of ionizing radiation arising from nuclear power plants. It is recognized that technology and scientific knowledge advance, and that nuclear safety and what is considered adequate protection need to be considered against the present state of knowledge. Safety requirements will change over time; this publication reflects the present consensus.

1.2. The designs of many existing nuclear power plants, as well as the designs for new plants, have been enhanced to include additional measures to mitigate the consequences of more complex accident sequences involving multiple failures, and of some severe accidents. Complementary systems and capabilities have been backfitted to many existing plants to aid in the prevention of severe accidents and mitigation of their consequences. Guidance on the mitigation of severe accidents has been provided in most existing nuclear power plants. The design of new nuclear power plants now explicitly includes consideration of severe accident scenarios and strategies for their management. Safeguards related requirements and security related requirements are also taken into account in the design of nuclear power plants. Integration of the safety and security features should ensure that neither compromises the other.

1.3. For nuclear power plants of the new generation, measures for use in severe accidents are now included in the plant design. However, it may not be practicable to apply all the requirements of this Safety Requirements publication for design to plants that are already in operation or under construction; in addition, it may not be feasible to modify designs that have already been approved by national regulatory bodies. For the safety analyses of such designs, it is expected that a comparison will be made against the current standards, for example as part of the periodic safety review of the plant, to determine whether the safe operation of the plant is still ensured, and whether any practicable safety improvements could be and should be implemented.

OBJECTIVE

1.4. This publication establishes design requirements for the structures, systems and components of a nuclear power plant as well as procedures and organizational processes important to safety that are required to be met for safe operation and for preventing or mitigating the consequences of events that could jeopardize safety.

1.5 This publication is intended for use by organizations in the design, manufacture, construction, modification, maintenance, operation and decommissioning of nuclear power plants, and in analysis, verification, review and the provision of technical support, as well as by regulatory bodies.

1.6. This publication does not set any quantitative acceptance criteria or safety goals. The setting of quantitative acceptance criteria or safety goals is the responsibility of the licensee and the regulatory body.

SCOPE

1.7. It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). For application to other reactor types, this publication may be used, with judgement, to determine the requirements that have to be considered in developing the design.

1.8. This publication does not address:

(1) requirements that are specifically covered by other publications in IAEA Safety Requirements publications (for example Ref. [2]) and matters relating to nuclear security and safeguards.

(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.

1.9. Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated (see under Definitions).

STRUCTURE

1.10. This Safety Requirements publication follows the relationship between safety objectives and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety principles, objectives, concepts that form the basis for deriving the safety function requirements that must be met by the plant as well as the safety design criteria. Sections 3, 4 and 5 establish numbered requirements in bold type, with additional paragraphs as appropriate. Section 3 establishes the general requirements to be satisfied by the design organization in the management of the design process. Section 4 establishes the main design criteria for safety and requirements for the fundamental safety functions, defence in depth, provisions for construction, for safety and security interfaces, and for ensuring that the radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 provides general plant design requirements that supplement the principal technical requirements to ensure that the safety objectives are met and the safety principles are applied. The general plant design requirements apply to all structures, systems and components important to safety. Section 6 establishes the overall design requirements applicable to specific plant systems, such as the reactor core, reactor coolant systems, containment systems and instrumentation and control systems.

2. APPLYING THE SAFETY OBJECTIVE, SAFETY PRINCIPLES AND CONCEPTS

2.1. The Fundamental Safety Principles publication [1] establishes one fundamental safety objective and ten safety principles that provide the basis for 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.

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

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

(2) To prevent events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at the nuclear power plant;

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

2.3. The fundamental safety objective applies for all stages over the lifetime of a nuclear power plant, 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. Safety Fundamentals [1], paragraph 2.3 states: "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."

2.5. This publication establishes requirements to apply those safety principles, which are particularly important in the design of nuclear power plants.

RADIATION PROTECTION

2.6. In order to satisfy the safety principles, it is required to ensure that in all operational states of a nuclear power plant and for any activities, exposure to radiation within the installation or due to any planned release of radioactive material from the installation is kept below authorized limits and kept as low as reasonably achievable. In addition, measures are implemented to mitigate the radiological consequences of any accidents, if they were to occur.

2.7. To apply the safety principles it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, this principle does not preclude limited doses to people or the release of authorized quantities of radioactive material to the environment from nuclear power plants in operational states. Such exposures and releases are required to be strictly controlled, however, and to be kept as low as reasonably achievable in compliance with national 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 required to take measures to do the following consistent with national acceptance criteria and safety goals:

(1) to prevent accidents with harmful consequences resulting from a loss of control over the reactor core and other sources of radiation, and to mitigate the consequences of accidents that do occur;

(2) to ensure with a high level of confidence that, for all accidents taken into account in the design of the installation any radiological consequences would be below the relevant limits and as low as reasonably achievable; and

(3) to ensure with a high level of confidence that the likelihood of an accident with serious radiological consequences occurring is extremely low, and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

2.9. To demonstrate that the fundamental safety objective [1] is achieved in the design of a nuclear power plant, a comprehensive safety assessment [2] of the design is required to be carried out to identify all sources of radiation and to evaluate the possible radiation doses that could be received by workers at the installation and by the public, as well as the possible effects on the environment as a result of the operation of the plant. The safety assessment is required in order to examine: (1) normal operation of the plant; (2) plant performance in anticipated operational occurrences; and (3) accident conditions. On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the plant equipment important to safety can be demonstrated, and the inputs (prerequisites) for emergency planning can be established.

2.10. Measures are required to be taken to control radiation exposure in all operational states to levels that are as low as reasonably achievable and to minimize the likelihood of an accident that could lead to the loss of control over a source of radiation. Nevertheless, there is a residual possibility that an accident could happen. Measures are therefore required to be taken to ensure that the radiological consequences of an accident are mitigated. Such measures include: engineered safety features; safety systems; accident management procedures established by the operating organization; and, possibly, off-site intervention

measures established by the appropriate authorities, supported as required by the operating organization, to mitigate radiation exposures if an accident has occurred. The design for safety of a nuclear power plant applies the principle that plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated[1] or of a very low frequency of occurrence, and that plant event sequences with a significant frequency of occurrence must have no or only minor potential radiological consequences. An essential objective is that the necessity for off-site intervention measures to mitigate radiological consequences is limited or is even eliminated in technical terms, although such measures may still be required by the responsible authorities.

THE CONCEPT OF DEFENCE IN DEPTH

2.11. The primary means of preventing accidents and mitigating the consequences of accidents is the application of the concept of defence in depth [4, 5]. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities 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 protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human actions within the plant, and from events that originate outside the plant.

2.12. Application of the concept of defence in depth in the design of a plant provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects on people or the environment, and ensuring adequate protection and mitigation in the event that prevention fails. The independent effectiveness of each of the different levels of defence is a necessary element of defence in depth and is achieved by incorporating features such as redundancy, independence and diversity.

(1) The aim of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to the requirements that the plant be soundly and conservatively sited, designed,

[1] The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise.

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 code and materials, and to the quality control of the fabrication of components and of plant construction, as well as to plant commissioning. Design options that reduce the potential for internal hazards contribute at this level of defence. Attention is also paid to the processes and procedures involved in 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 for operational and maintenance practices.

(2) The aim of the second level of defence is to detect and control 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 operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design; the confirmation of their effectiveness through analysis; and the establishment of operating procedures to prevent or minimize the damage from such postulated initiating events and to bring the plant to a safe state.

(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 controlled at a preceding level so that an accident may develop. In the design of the plant these accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be provided that are capable of preventing core damage or significant off site releases, and leading the plant first to a controlled state and subsequently to a safe shutdown state, and maintaining at least one barrier for the protection of the workers and public from radiological effects.

(4) The aim of the fourth level of defence is to mitigate the consequences of accidents that result from failure of safety features and accident management measures, with consequent potential radioactive releases. The most important objective for this

level is the protection of the confinement function, thus ensuring that radioactive releases are kept as low as reasonably achievable.

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

2.13. A relevant aspect of the implementation of defence in depth is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherently safe features contributing to their effectiveness in confining 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 possible internal and external hazards, and the potential consequences of failures.

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

2.14. The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks (i.e. the licensee) [1]. The design, construction and commissioning of a nuclear power plant may be shared between a number of organizations: the architect-engineer; the vendor of the reactor and its supporting systems; the suppliers of major components; the designer of electrical support systems; and the suppliers of other systems that are important to the safety of the plant.

2.15. The International Nuclear Safety Group [6] has suggested that the operating organization could set up a formal process to maintain the integrity of the plant design throughout its lifetime, i.e. during the operational phase and into decommissioning. A formally designated entity within the operating organization would take responsibility for this process.

2.16. In practice the design of a plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. Reference [6] emphasizes 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 this formally designated entity may assign responsibilities for parts of the plant. Prior to an application for authorization of a plant, the responsibilities for the design will rest with the design organization (e.g. the vendor). Once an application for authorization of a plant has been filed, the ultimate responsibility will lie with the applicant; however, the detailed knowledge of the design will rest with the responsible designers. This balance will change as the plant is put into operation, since much of this detailed knowledge, such as the safety analysis report, design manuals and other design documentation, will be transferred to the operating organization. To facilitate this transfer, the structure of such a formally designated entity is established at an early stage.

2.17. The management system requirements that are placed on the formally designated entity will also apply to the responsible designers. However, the overall responsibility for the integrity of design of the plant will rest with the formally designated entity, and hence ultimately with the operating organization.

3. MANAGEMENT OF SAFETY IN DESIGN

Requirement 1: Responsibilities in the management of safety in design

An applicant for a licence to construct and operate a nuclear power plant shall ensure that the design submitted to the regulatory body meets all applicable safety requirements.

3.1 All organizations, including the design organization, engaged in activities important to the safety of the design shall have a responsibility to ensure that safety matters are given the highest priority.

Requirement 2: Management system[2] for the plant design

The design organization[3] shall establish and implement a management system for ensuring that all safety requirements established for the plant design are considered and implemented in all phases of the design process and are met in the final design.

[2] Requirements on management systems are established in Ref. [8].

3.2. The management system shall include provisions to ensure the quality of design of each structure, system and component, as well as the overall plant design, at all times. This includes the means for the identification and correction of design deficiencies, checking the adequacy of the design, and the control of design changes.

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

3.4. The adequacy of the design, including design tools and design inputs and outputs, shall be verified and validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval of the design shall be completed as soon as practicable in the design and construction process, and in any case before operation of the plant is commenced.

Requirement 3: Safety of the design throughout the plant lifetime

The operating organization shall establish a formal system to maintain responsibility for the continuing safety of the plant design throughout its lifetime.

3.5. The prime responsibility for safety shall rest with the operating organization. The system for continuing safety of the plant shall be performed by establishing a formally designated entity (authority) for the safety of the plant design within the licensee's management system. Tasks that are assigned to external organizations for the design of specific parts of the plant (referred to as responsible designers) shall be taken into account in the arrangements.

3.6. The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with the relevant national and international codes and standards, laws, regulations and jurisdictional requirements. A series of tasks and functions shall be established and implemented to ensure the following:

(1) Consideration of the design to demonstrate that it is adequate, fit for purpose and meets the ALARA principle, design verification, definition of engineering

[3] The design organization is the organization responsible for the preparation of the final detailed design of the plant to be built.

standards and requirements, use of proven engineering practices, provision for feedback on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included;

(2) the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing), and modifications of the plant is available and is maintained up to date by the operating organization, with account taken of past operational experience and validated research findings;

(3) management of design requirements and configuration control are maintained;

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

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

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

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

4. PRINCIPAL TECHNICAL REQUIREMENTS

Requirement 4: Fundamental safety functions

Fulfilment of the following fundamental safety functions shall be ensured for all plant states:

(1) control of reactivity;

(2) removal of heat from the core;

(3) confinement of radioactive material, provision of shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

4.1. A systematic approach shall be taken to identify the items important to safety that are necessary to fulfil the fundamental safety functions, and to identify the inherent features that

are contributing to or affecting the fundamental safety functions, for all the levels of defence in depth.

4.2. Means of monitoring the plant status shall be provided for ensuring that the required safety functions are fulfilled.

Requirement 5: Radiation protection and acceptance criteria

The design shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed authorized limits and are kept as low as reasonably achievable in normal operation and anticipated operational occurrences for all plant life and remain below acceptable limits and as low as reasonably achievable in and following accident conditions.

4.3. The design shall be such as to ensure that plant states that could potentially lead to high radiation doses or large radioactive releases have a very low likelihood of occurrence, and that there are no or only minor potential radiological consequences of plant states with a significant likelihood of occurrence.

4.4. Acceptance criteria for radiation protection associated with the different categories of plant states shall be established, consistent with regulatory requirements.

Requirement 6: Design of the nuclear power plant

The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the required reliability, that the plant can be operated safely within authorized limits for the full duration of its design life, including decommissioning, and that impacts on the environment are minimized.

4.5. The design shall be such as to ensure that the safety requirements of the licensee and the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, as well as applicable national and international codes and standards, are all met, and that due account is taken of human capabilities and limitations and factors that could influence human performance. Adequate information on the design shall be provided for ensuring the safe operation and maintenance of the plant, and to allow subsequent plant

modifications to be made. Recommended practices shall be provided for incorporation into the plant administrative and operational procedures (i.e. operational limits and conditions).

4.6. The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other plants and of the results of relevant research programmes.

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

4.8. The design shall be such as 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 means of appropriate design measures and operational and decommissioning practices.

Requirement 7: Application of defence in depth

The design and the design process shall incorporate defence in depth into design activities. Independent levels of defence shall be provided so that if a failure or a deviation from normal operation or a deviation from procedures were to occur, it would be detected and compensated for, corrected or controlled.

4.9. The defence in depth concept shall be applied throughout the design process to provide several levels of defence that are aimed at preventing harmful effects on people or the environment and ensuring that appropriate measures are taken for protection and mitigation in the event that prevention fails.

4.10. Due account shall be taken in the design of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence shall be kept available at all times, and any permissible relaxations shall be specified for specific operational modes.

4.11. The design:

(1) shall provide for multiple physical barriers to the release of radioactive material to the environment;

(2) shall be conservative, and the construction shall be of high quality, to provide assurance that: plant failures and deviations from normal operation are minimized; that accidents are prevented as far as practicable; and that a small deviation in a plant parameter does not lead to a cliff edge effect[4];

(3) shall provide for the control of plant behaviour by means of inherent and engineered features; such that plant failures or deviations from normal operation requiring actuation of safety systems are minimized or excluded by design to the extent possible;

(4) shall provide for supplementing control of the plant, by the use of automatic actuation of safety systems such that failures or deviation from normal operation that exceed the protective capability of the plant control system are controlled with high confidence; automatic actuation of safety systems shall minimize the need for operator actions in the early phase of these failures or deviations from normal operation;

(5) shall provide for systems, structures and components and procedures to control the course and limit the consequences of failures and deviations from normal operation that exceed the protective capability of safety systems as far as practicable; and

(6) shall 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.

4.12. To ensure that the concept of defence in depth is maintained, the design shall prevent as far as practicable:

(1) challenges to the integrity of physical barriers;

(2) failure of one or more barriers;

(3) failure of a barrier as a consequence of the failure of another barrier;

[4] A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

(4) the possibility of harmful consequences of human errors during operation and maintenance.

4.13. The design shall be such as to ensure as far as practicable 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 operating lifetime of the nuclear power plant.

Requirement 8: Safety, safeguards and security interfaces

Safety measures, security measures and safeguards arrangements shall be designed and implemented in an integrated manner so that they do not compromise one another.

Requirement 9: Proven engineering practices

Items important to safety shall be designed in accordance with the relevant national and international codes and standards.

4.14. Items important to safety shall provide the highest level of safety that can reasonably be achieved [1]. Items important to safety shall preferably be of a design that has been previously proven in equivalent applications, or otherwise shall be items of high quality technology that has been qualified and carefully examined.

4.15. National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency, and shall be supplemented or modified as necessary to ensure that the final quality of the design is commensurate with the relevant safety function.

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

Requirement 10: Safety assessment[5]

Comprehensive deterministic safety assessments 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 lifetime, and to confirm that the design meets requirements as delivered for fabrication, for construction, as built, as operated and as modified.

4.17. The safety assessment shall commence at an early stage in the design process, with iteration between design activities and confirmatory analytical activities, and increasing in scope and level of detail as the design programme progresses.

4.18. The safety assessment shall be documented in a form that facilitates independent evaluation.

Requirement 11: Provision for construction

Items important to safety shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required safety performance.

4.19. The provision for construction and operation shall take due account of relevant experience that has been gained in the construction of other similar plants and the associated structures, systems and components. Where best practices from other relevant industries are adopted, it shall be shown that such practices are appropriate to the specific nuclear application.

Requirement 12: Features to facilitate decommissioning

Special consideration shall be given at the design stage to the incorporation of features that will facilitate the future decommissioning and dismantling of the plant.

4.20. In particular, account shall be taken in the design of:

[5] Requirements on safety assessment are established in Ref. [2].

(1) the choice of materials, so that quantities of future radioactive waste are minimized to the extent practicable and decontamination is facilitated;

(2) the access capabilities and means of handling that may be necessary;

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

5. PLANT DESIGN

DESIGN BASIS

Requirement 13: Categories of plant states

Plant states shall be identified and shall be grouped into a limited number of categories according to their frequency of occurrence.

5.1. The plant states shall typically cover:

(1) normal operation;

(2) anticipated operational occurrences, expected to occur over the lifetime of the plant;

(3) design basis accidents;

(4) design extension conditions including accidents with significant core degradation.

5.2. Criteria shall be assigned to each plant state such that frequently occurring plant states have no or only minor radiological consequences and plant states that may give rise to serious consequences have a very low frequency of occurrence.

Requirement 14: Design basis for items important to safety

The design of items important to safety shall specify the necessary capability, reliability and functionality for the required plant operational states, for accident conditions and for conditions generated by internal and external hazards, to meet the specified acceptance criteria over the lifetime of the plant.

5.3. The design basis for each item important to safety shall be systematically documented. The documentation shall provide the necessary information for the operating organization to operate the plant safely.

Requirement 15: Design limits

A set of design limits consistent with the key physical parameters for each item important to safety shall be specified for all operational states and accident conditions.

5.4. The design limits shall be consistent with the relevant national and international standards and codes, as well as relevant regulatory requirements.

Requirement 16: Postulated initiating events

The design shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all credible events with the potential for serious consequences and all credible events with a significant frequency of occurrence have been anticipated and have been considered in the design.

5.5. The postulated initiating events shall be selected on the basis of engineering judgement and a combination of deterministic techniques and probabilistic techniques. A justification of the extent of usage of the deterministic analyses and the probabilistic analyses shall be provided to show that all credible events have been covered. Consideration shall be given to matters relating to nuclear security and to the system of accounting for and control of nuclear material.

5.6. The postulated initiating events shall include all credible failures of plant structures, systems and components, human errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

5.7. An analysis of the postulated initiating events shall be made to establish the preventive and/or protective measures that are necessary to ensure that the required safety functions will be performed.

5.8. The expected plant response to any postulated initiating event shall be such that the following can reasonably be achieved, in order of preference:

(1) a postulated initiating event produces no significant safety related effect or only produces a change in the plant towards safe conditions by means of its inherent characteristics;

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

(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 specified procedural actions.

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

5.10. A technically supported justification shall be provided for the exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events.

5.11. Where prompt and reliable action is necessary in response to a postulated initiating event, provision shall be made in the design to initiate the necessary actuation of safety systems automatically, to prevent progression to more severe conditions.

5.12. Where prompt action in response to a postulated initiating event is not necessary, the manual initiation of systems or other operator actions can be relied upon, provided that the

time interval between the detection of the abnormal event or accident and the required action is sufficiently long, and that adequate procedures (such as administrative, operational and emergency procedures) are specified to ensure the performance of such actions.

5.13. The operator actions that are 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 shall be facilitated by the provision of adequate instrumentation to monitor the plant status and controls for the manual operation of equipment.

5.14. The design shall specify the necessary provision of equipment, including the procedures required to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

5.15. Any equipment that is necessary in manual response and recovery processes shall be placed at the most suitable locations to ensure its availability at the time of need and to allow safe access to it for the anticipated environmental conditions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of such equipment or incorrect diagnosis of the required recovery process.

Requirement 17: Hazards

All credible internal and external hazards and human induced events that have the potential directly or indirectly to affect the safety of the plant shall be identified and their effects shall be evaluated. Hazards shall be considered for the determination of postulated initiating events and generated loadings for use in the design of relevant items important to safety.

Internal hazards

5.16. Possible system and equipment failures, human induced events or failures or maloperation that could lead to internal hazards such as fire, explosions, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site shall be taken into account in the design. Appropriate preventive and mitigatory measures shall be provided to ensure that safety is not compromised.

External hazards[6]

5.17. The design shall include due consideration of those natural and human induced events of origin external to the plant that have been identified in the site evaluation process. Natural events that shall be addressed include meteorological, hydrological, geological and seismic events. Human induced events that shall be addressed are those resulting from nearby industries and transport routes. The safety of the plant shall not be dependent on the availability of off-site services such as electricity supply and fire fighting services.

5.18. Items important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability of and the possible harmful effects of external events.

5.19. Measures shall be provided to minimize any interactions resulting from external events considered in the design between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure.

5.20. The design shall be such as to ensure that items important to safety are capable of withstanding the effects of external events considered in the design, or otherwise that other features such as passive barriers shall be provided to protect the plant and to ensure that the required safety function will be performed.

5.21. The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events and to avoid cliff edge effects (see footnote 3).

5.22. For multiple unit plant sites, the potential for simultaneous impacts of specific hazards on several units on the site shall be taken into account in the design.

Requirement 18: Engineering design rules

The engineering design rules for items important to safety shall be specified and shall comply with the relevant national or international codes and standards and with sound engineering practices, with account taken of their relevance to nuclear power technology.

[6] Requirements on site evaluation for nuclear installations are established in Ref. [7].

5.23. Methods that ensure a robust design shall be applied and sound engineering practices shall be adhered to in the design to ensure that the fundamental safety functions are achieved in all operational states and for all accident conditions.

Requirement 19: Operational limits and conditions

The design shall establish a set of requirements and limitations for safe operation; these requirements and limitations shall form the basis for the establishment of the operational limits and conditions under which the plant shall be operated.

5.24. The requirements and limitations [7] include:

(1) safety limits;

(2) limiting safety system settings;

(3) limits and conditions for normal operation and anticipated operational occurrences;

(4) control system constraints 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 principle of keeping radiation risks as low as reasonably achievable taken into consideration;

(6) clearly defined operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;

(7) action statements, including completion times for actions in response to deviations from the specified operational limits and conditions.

Requirement 20: Design basis accidents

A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the plant to withstand without exceeding acceptable limits for radiological protection.

5.25. Design basis accidents shall be used to define the design bases including performance criteria, for the safety systems and for other items important to safety that are necessary to control those accident conditions, with the objective of returning the plant to a safe state or mitigating the consequences of accidents.

5.26. The design shall be such that for the design basis accident conditions, key plant parameters do not exceed the specified limits. A primary objective shall be to manage all design basis accidents so that they have no or only minor radiological impacts, both on and off the site, and do not necessitate any off-site intervention measures. In order to meet this objective, the plant design and safety system design shall be such as to reduce, as far as reasonably achievable, the probability of a design basis accident resulting in the release of a significant amount of radioactive material or radiation.

5.27. The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specified design criteria, and the use of conservative assumptions, models and input parameters in the analysis.

Requirement 21: Design extension conditions

A set of design extension conditions shall be derived from engineering, deterministic and probabilistic considerations for the purpose of establishing further boundary conditions for the plant to withstand without acceptable limits for radiological consequences being exceeded. These conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention and mitigation of such accidents.

5.28. An analysis of design extension conditions shall be performed[7]. The main technical objective of considering the design extension conditions is to ensure that consequences in excess of acceptance criteria for design basis accidents are reduced so far as practicable. This may require additional safety features, or the extension of the capability of safety systems to ensure the management of accidents in which there is significant radiological material in the containment (including as a result of severe core degradation), to maintain the integrity of the containment. Furthermore, the plant shall be designed so that it can be brought into a controlled state and the containment function maintained, so that significant radioactive

[7] This shall be done with a best estimate approach (more stringent approaches may be used according to Member States' requirements).

releases would be practically eliminated. The effectiveness of measures to ensure the containment functionality shall be analysed on the basis of the best estimate approach.

5.29. The design extension conditions shall be used to define the design basis for safety features and for the design of all other items important to safety that are necessary to prevent these conditions from arising, or if they do arise to control them and to mitigate their consequences.

5.30. The analysis undertaken shall include identification of the equipment that is designed to prevent and/or to mitigate event sequences leading to accidents with melting of the reactor core. Consideration shall be given to the full design capabilities of the plant, and the temporary use of additional systems, to return the plant to a safe state or to mitigate the consequences of an accident, provided that it is shown that the systems are able to withstand and to function in the environmental conditions to be expected. These measures shall be demonstrated to be independent of measures used in less frequent accidents, to the extent practicable. The reliability of the measures shall be appropriate for the function they are required to fulfil. The additional systems shall be capable of operating in the environmental conditions pertaining to these design extension conditions. For multiple unit plants, consideration shall be given to the use of available means or to possible support from other units of the plant.

5.31. In particular, to determine the design bases for the containment and its safety features, it may be necessary to postulate extreme scenarios that involve, among other things, melting of the reactor core. These shall be selected using engineering judgement and input from probabilistic safety assessment. The design shall be such that design extension conditions that could lead to significant radioactive release are practically eliminated.

5.32. For design extension conditions that are not practically eliminated, design provisions shall be made such that only protective measures that are of limited scope in terms of area and time are necessary for the protection of the public, and sufficient time is available to implement these measures.

5.33. The design shall facilitate the development and application of emergency procedures and severe accident management procedures.

Combinations of events/multiple failures

5.34. Where the results of engineering judgement and probabilistic methods indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered as design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Such events include common cause failures. Certain events may be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.

Requirement 22: Separation and independence of safety systems

Interference between 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 independence of communication (data transfer), as appropriate.

Requirement 23: Safety classification

All items important to safety shall be identified and the items identified shall be classified on the basis of their function and their safety significance.

5.35. The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methodologies 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 the safety function;

(3) the frequency at which the item will be called upon to perform a safety function;

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

5.36. The design shall be such as to ensure that any failure of items important to safety in a system classified in a lower class will not propagate to a system classified in a higher class.

5.37. Equipment that performs multiple functions shall be classified consistent with the most important function performed.

Requirement 24: Reliability of items important to safety

The level of reliability of items important to safety shall be commensurate with their safety significance.

5.38. The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated, modified and maintained to be capable of withstanding with sufficient reliability and effectiveness all conditions specified in their design basis.

5.39. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes. Preference shall be given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.

Requirement 25: Common cause failures

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

Requirement 26: Single failure criterion

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

5.40. Consequential failures resulting from the assumed single failure shall be considered to be part of the single failure.

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

5.42. Failure of a passive component shall be taken into account, unless it has been justified in the single failure analysis with high confidence that a failure of that component is very unlikely and its function remains unaffected by the postulated initiating event.

Requirement 27: Fail-safe design

The principle of fail-safe design shall be incorporated as appropriate for the plant into the design of systems and components important to safety.

Requirement 28: Support service systems

Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

5.43. The reliability, redundancy, diversity and independence of the support services and the provision of features for their isolation and for testing their functional capability shall be commensurate with the significance to safety of the system that is supported.

5.44. A failure of an auxiliary support service system shall not be capable of simultaneously affecting redundant parts of the safety systems or systems fulfilling diverse safety functions.

DESIGN FOR LIFETIME SAFE OPERATION

Requirement 29: Maintenance, testing, repair, replacement, inspection and monitoring

Items important to safety shall be designed to be qualified, installed, commissioned, operated, calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their tasks and maintaining their integrity in all conditions specified in their design basis.

5.45. The plant layout shall be such that activities for calibration, maintenance, testing, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and_standards commensurate with the importance of the safety functions to be performed, with no significant reduction in system availability and without undue radiation exposure of operating personnel.

5.46. Where items important to safety have to be withdrawn from service for calibration, testing, maintenance or replacement, the facilities for doing such tasks shall be in compliance with relevant national and international codes and_standards of quality management for

components, practices and the work environment, commensurate with the importance of the safety function of the items requiring calibration, testing, maintenance or replacement.

5.47. If an item important to safety cannot be designed to be able to be tested, inspected or monitored to the extent desirable, then a robust technical justification shall 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 shall be specified;

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

5.48. The design shall be such as to ensure to the extent practicable that:

(1) on-line maintenance and testing of items important to safety can be conducted safely without the necessity to shut down the plant;

(2) on-line and off-line maintenance of equipment and components can be performed safely and effectively.

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

5.50. Where access to items important to safety is necessary for purposes of maintenance, testing or inspection, it shall be ensured in the design that the necessary activities can be performed without significantly reducing the reliability of the associated safety related equipment.

Requirement 30: Equipment qualification

A qualification programme shall be implemented to confirm that items important to safety are capable of meeting the demands for performing their intended functions at the time of need, and in the prevailing environmental conditions throughout their design life, with account taken of conditions due to maintenance and testing.

5.51. The environmental conditions considered shall include the variations in ambient conditions that are expected in the design basis.

5.52. The qualification programme shall include the consideration of ageing effects caused by various environmental factors (such as conditions of vibration, irradiation or temperature) over the expected lifetime of the equipment. Where the equipment is subject to external natural events and is required to perform a safety function in or following such an event, the qualification programme shall replicate as far as practicable the conditions imposed on the equipment by the natural phenomenon, either by test or by analysis or by a combination of both.

5.53. Any environmental conditions that can reasonably be anticipated and that could arise from specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.

Requirement 31: Ageing management

Appropriate margins shall be provided in the design for all items important to safety so as to take into account relevant ageing, neutron embrittlement and wear-out mechanisms and the potential for age related degradation, in order to ensure the capability of the item important to safety to perform its necessary safety function throughout its design life.

5.54. Ageing and wear-out effects in all operational conditions for which a component is credited, including testing, maintenance, maintenance outages, and plant states in a postulated initiating event and following a postulated initiating event shall be taken into account.

5.55. Provision shall be made for monitoring, testing, sampling and inspection, to assess ageing mechanisms predicted at the design stage and which may be able to identify unanticipated behaviour or degradation that may occur in service.

Requirement 32: Design for optimal operator performance

Systematic consideration of human factors and the human–machine interface shall be included in the design process at an early stage and shall be continued throughout the entire process.

5.56 The design shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

5.57. Personnel who have experience of operating similar plants shall as far as practicable be actively involved in an interactive way in the design process conducted by the design organization to ensure that consideration is given as early as possible to the operation and maintenance of the equipment.

5.58. The design shall be aimed at supporting operating personnel in the fulfilment of their responsibilities and the performance of their tasks, and at limiting the effects of human errors that can affect safety. Attention shall be paid to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate the interface between the operating personnel and the plant.

5.59. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, compatible with the necessary decision and action times.

5.60. The operator shall be provided with information that permits the following:

(1) the ready assessment of the general state of the plant in whichever condition it is, and confirmation that the designed automatic safety actions are being carried out;

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

5.61. The operator shall be provided with sufficient information to operate the plant within the specified limits on parameters associated with individual plant systems and equipment and to confirm that the necessary safety actions can be initiated safely.

5.62. The design shall be aimed at promoting the success of operator actions with due regard for the time available for action, the physical environment to be expected and the psychological demands to be made on the operator.

5.63. The need for intervention by the operator on a short time-scale shall be kept to a minimum and it shall be demonstrated that the operator has sufficient time to make a decision and to act. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented.

5.64. 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 shall be such as to ensure the safety of the operational staff.

5.65. The working areas and working environment of the operating personnel shall be designed in accordance with ergonomic principles.

5.66. Verification and validation of aspects of human factors, including the use of simulators, shall be included at appropriate stages to confirm that all necessary operator actions have been identified and can be correctly performed.

OTHER DESIGN CONSIDERATIONS

Requirement 33: Sharing of safety systems between nuclear power plant units

Safety systems shall not be shared between multiple units.

5.67. Systems that are not safety systems may be shared between several units for the purpose of accident management provided that such sharing would not increase either the likelihood or the consequences of an accident.

Requirement 34: Systems containing fissile material or radioactive material

All systems in a nuclear power plant that may contain fissile material or radioactive material shall be designed to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; to ensure that releases of radioactive material are kept below authorized

limits in normal operation and below acceptable limits in accident conditions and as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.

Requirement 35: Power plants used for cogeneration of heat and power, heat generation or desalination

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 material from the nuclear plant to the desalination unit or district heating unit under any conditions of normal operation, in anticipated operational occurrences and in accident conditions.

Requirement 36: Escape routes

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.

5.68. The escape routes shall meet the relevant national and international requirements for radiation zoning and fire protection and the relevant national requirements for industrial safety and plant security.

5.69. At least one escape route shall be available from occupied areas following an internal event or an external event or other combinations of events considered in the design.

Requirement 37: Communication systems

Effective means of communication shall be provided throughout the plant to facilitate safe operation in all modes of operation and to be available for use following all postulated initiating events and in accident conditions.

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

5.71. Suitable and diverse means of communication necessary for safety, within the nuclear power plant, in the immediate vicinity and to relevant off-site agencies, shall be provided.

Requirement 38: Control of access to the plant

The plant shall be isolated from its surroundings with a suitable layout of the structural elements so that access to it can be controlled.

5.72. Provision shall be made in the design of the buildings and the layout of the site for the control of access of personnel and/or equipment, including emergency response personnel and vehicles, to the plant, with particular reference to guarding against the unauthorized entry of persons and goods to the plant.

Requirement 39: Prevention of interference with items important to safety

Unauthorized access to or unauthorized interference with items important to safety, including computer hardware and software, shall be prevented.

Requirement 40: Interactions of systems

The potential for interaction of systems important to safety that may be required to operate simultaneously shall be evaluated and harmful affects shall be prevented.

5.73. In the analysis of the potential for interaction of systems important to safety, account shall 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 physical environment do not affect the reliability of system components in functioning as intended.

5.74. If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded.

Requirement 41: Interactions between the electrical power grid and the plant

The functionality of items important to safety shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the grid supply voltage and frequency.

SAFETY ANALYSIS[8]

Requirement 42: Safety analysis of the plant design

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

5.75. On the basis of a safety analysis, the design basis for items important to safety and their link to initiating events and event sequences shall be confirmed. It shall also be demonstrated that the plant as designed is capable of meeting any authorized limits for radioactive releases and for doses for operational conditions, and is capable of meeting acceptable limits for accident conditions.

5.76. The safety analysis shall provide assurance that defence in depth has been implemented in the design.

5.77. The safety analysis shall provide assurance that adequate consideration has been given to uncertainties.

5.78. The applicability of the analytical assumptions, methods and degree of conservatism used shall be updated and verified for the current or 'as built' design.

Deterministic approach

5.79. The deterministic safety analysis shall mainly provide:

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

[8] Requirements on safety assessment for facilities and activities are established in Ref. [2].

(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 acceptance criteria for radiation protection and design limits;

(5) demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by the automatic response of safety systems in combination with prescribed actions of the operator.

Probabilistic approach

5.80. The design shall take into account the probabilistic safety analysis of the plant in all modes of operation and plant states including shutdown, with reference in particular to:

(1) establishing 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 to the extent practicable, there is independence between the levels of defence in depth;

(2) providing confidence that small deviations in plant parameters that could give rise to a large variation in plant conditions (‘cliff edge effects’) will be prevented (see footnote 3);

(3) comparing the results of the analysis with the acceptance criteria for risk where these have been defined.

6. DESIGN OF SPECIFIC PLANT SYSTEMS

REACTOR CORE AND ASSOCIATED FEATURES

Requirement 43: Performance of fuel elements and assemblies

Fuel elements and assemblies shall be designed to maintain their structural and dimensional integrity, and to withstand satisfactorily the anticipated radiation 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.

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

6.2. Fuel design limits shall include limits on the permissible leakage of fission products, to encompass the operational conditions for the plant that may be imposed in anticipated operational occurrences so that the fuel remains suitable for continued service.

6.3. Fuel elements and fuel assemblies shall be capable of withstanding fuel handling loads.

Requirement 44: Structural capability of the reactor core

The fuel elements and fuel assemblies and the supporting structures shall be designed so that in accident conditions other than severe accidents a geometry that allows for adequate cooling is maintained and that the insertion of control rods is not impeded.

Requirement 45: Control of the reactor core

Distributions of neutron flux that can arise in any state of the core, including states after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and design basis accident conditions, shall be inherently stable, and the demands made on the control system for maintaining shapes, levels and stability of the neutron flux within specified limits in all operational conditions shall be minimized.

6.4. Adequate means of detecting the neutron flux distributions in the core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.

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

6.6. The maximum degree of positive reactivity and its rate of increase by insertion in operational conditions and design basis accident conditions shall be limited or compensated for so that no resultant failure of the reactor coolant pressure boundary will occur, cooling capability will be maintained and no significant damage to the reactor core will occur.

Requirement 46: Reactor shutdown

Means shall be provided to ensure that there is a capability to shut down the reactor in operational states and accident conditions, and that the shutdown condition can be maintained even for the most reactive core conditions, with account taken of uncertainties.

6.7. The effectiveness, speed of action and shutdown margin of the means of shutdown shall be such that the specified limits for fuel are not exceeded.

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

6.9. The means for shutting down the reactor shall consist of at least two diverse and independent systems.

6.10. At least one of the two different shutdown systems shall be capable on its own of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the core.

6.11. The means of shutdown shall be adequate to prevent any credible increases in reactivity by insertion during the shutdown, including refuelling or other routine or non-routine operations in the shutdown state.

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

REACTOR COOLANT SYSTEM

Requirement 47: Design of the reactor coolant system

The components of the reactor coolant system shall be designed and constructed so that the risk of faults due to quality of materials, design standards, capability of inspection and quality of fabrication is minimized.

6.13. Pipework connected to the reactor coolant pressure boundary shall be equipped with adequate isolation devices to limit any loss of radioactive fluid (primary coolant) and to preclude the loss of coolant through interfacing systems

6.14. The reactor coolant pressure boundary shall be designed so that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture with fast crack propagation, to permit the timely detection of flaws.

6.15. The design shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could exhibit brittle behaviour are avoided.

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

Requirement 48: Overpressure protection of the coolant pressure boundary

Provision shall be made to ensure that the operation of pressure relief devices, will protect the pressure boundary of the reactor coolant system from overpressure and will not lead to the release of radioactive material directly to the environment.

Requirement 49: Inventory of reactor coolant

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

Requirement 50: Cleanup of the reactor coolant

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

6.17. The capabilities of the necessary systems shall be based on the specified fuel design limit on permissible leakage with a conservative margin to ensure that the plant can be operated with a level of circuit activity which is as low as reasonably practicable, and that radioactive releases meet the requirement of being as low as reasonably achievable and are within the authorized limits.

Requirement 51: Removal of residual heat from the core

Reliable means shall be provided for removing residual heat from the reactor core during the shutdown state such that the design basis limits for the fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.

Requirement 52: Emergency core cooling

Means of cooling the core shall be provided to restore and maintain fuel cooling under accident conditions even if the integrity of the pressure boundary for the primary coolant system is lost.

6.18. The means provided for cooling the core shall ensure that:

(1) the limiting parameters for the cladding or fuel integrity (such as temperature) will not be exceeded;

(2) possible chemical reactions are limited to an allowable level;

(3) the effectiveness of the means of core cooling compensates for possible alterations in the fuel and in the internal geometry of the core;

(4) the cooling of the core will be ensured for a sufficient time.

6.19. Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable redundancy and diversity shall be provided in order to fulfil these requirements with sufficient reliability for each postulated initiating event.

Requirement 53: Heat transfer to an ultimate heat sink

Systems shall be provided to transfer residual heat from items important to safety to an ultimate heat sink. This function shall be carried out at very high levels of reliability for all plant states.

CONTAINMENT STRUCTURES AND SYSTEMS

Requirement 54: Containment system

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

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

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

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

Requirement 55: Control of releases from the containment

The design of the containment shall be such as to ensure that any release of radioactive material to the environment is as low as reasonably achievable, and is below authorized limits in operational states and below acceptable limits in accident conditions.

6.20. Provision shall be made for the collection and controlled release or storage of materials that could leak from the containment to the environment.

6.21. The containment structure and systems and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations have been installed.

6.22. Determination of the leakage rate of the containment system at periodic intervals over the operating lifetime of the plant shall be possible at the containment design pressure.

6.23. The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be 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 56: Containment isolation

Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

6.24. Lines that penetrate the containment as part of the reactor coolant pressure boundary or that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series[9], with suitable leak detection provided. Isolation valves or check valves shall be located as close to the

[9] Normally one containment isolation valve or check valve is outside the containment and the other is inside the containment. However, other arrangements may be acceptable, depending on the design.

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

6.25. Exceptions shall only permitted for specific classes of lines such as instrumentation lines, or if the application of these isolation methods reduces the reliability of a safety system that penetrates the containment,.

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

Requirement 57: Containment access

Access by operating personnel to the containment shall be through airlocks equipped with doors that are interlocked to ensure that at all times at least one of the doors is closed when there is fuel inside the containment.

6.27. Where provision is made for entry of operating personnel for surveillance purposes, provisions for ensuring the safety of operating personnel shall be specified in the design. These requirements also apply to equipment air locks, where provided.

6.28 Containment openings for movement of equipment or material through the containment shall be designed to be closed quickly and reliably in case isolation of the containment is required.

Requirement 58: Control of containment conditions

Provision shall be made to control the pressure and temperature in the containment and to control any buildup of fission products and other gaseous or solid substances that may be released in the containment and that may affect the operation of systems important to safety.

6.29. The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure

bearing structure or to other systems of importance in limiting the effects of accident conditions.

6.30. The capability to remove heat from the reactor containment shall be ensured, to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels, after any accidental release of high energy fluids. The system performing the function of removing heat from the containment shall have adequate reliability and redundancy to ensure that this function can be fulfilled.

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

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

(2) to control the concentration of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions in order to prevent deflagration or detonation loads which could jeopardize the integrity of the containment.

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

INSTRUMENTATION AND CONTROL SYSTEMS

Requirement 59: Provision of instrumentation

Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment, for obtaining any information on the plant necessary for its reliable and safe operation, for determining the status of the plant in accident conditions, and for making decisions for the purposes of accident management.

6.33. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the course of accidents and the status of essential equipment; for predicting the locations and quantities of radioactive material that could escape from the locations intended in the design, and for post-accident analysis.

Requirement 60: Control systems

Appropriate and reliable control systems shall be provided to maintain and limit the relevant process variables within the specified operational ranges.

Requirement 61: Protection system

A protection system shall be provided that has the capability to detect unsafe conditions and automatically actuate the systems required for achieving and maintaining a safe condition.

6.34. The protection system shall be designed:

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

(2) to achieve a fail-safe condition in the event of its failure.

6.35. The design shall be such as:

(1) to prevent operator action that could defeat the effectiveness of the protection system in operational states and accident conditions, but not to negate correct operator actions in accident conditions;

(2) to automate various safety actions so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;

(3) to make appropriate information available to the operator for monitoring the effects of automatic actions.

Requirement 62: Reliability and testability of instrumentation and control of items important to safety

Instrumentation and control of items important to safety shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.

6.36. Design techniques such as testability, including a self-checking capability where necessary, fail-safe behaviour, functional diversity, and diversity in component design and

principles of operation shall be used to the extent practicable to prevent loss of a safety function.

6.37. Safety systems shall be designed to permit periodic testing of their functioning when the reactor is in service, including the possibility of testing channels independently to detect failures and losses of redundancy that may have occurred. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display.

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

Requirement 63: Use of computer based equipment in systems important to safety

If a system important to safety is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the lifetime of the system, and in particular the software development cycle. The entire development shall be subject to an appropriate quality management programme.

6.39. For computer based equipment in systems important to safety:

(1) a very high quality of and best practices for hardware and software shall be used, in accordance with the importance of the system to safety;

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

(3) an assessment of the computer based equipment shall be undertaken by experts independent of the designer team and supplier team to provide assurance of its high reliability;

(4) where safety functions are essential for achieving and maintaining a safe condition and the necessary integrity of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring their fulfilment shall be provided;

(5) common cause failures deriving from software shall be taken into consideration;

(6) protection from accidental or deliberate interference with system operation shall be provided.

Requirement 64: Separation of protection systems and control systems

Interference between the protection system and the control system shall be prevented by avoiding interconnections or by suitable functional isolation.

6.40. If signals are used in common by both a safety system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal source shall be classified as part of the safety system.

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

Requirement 65: Control room

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 and accident conditions.

6.42. Appropriate measures shall be taken, including provision of barriers between the control room and the external environment, and adequate information shall be provided to protect the occupants of the control room against hazards, such as high radiation levels resulting from an accident condition, the release of radioactive material, fire or explosive or toxic gases.

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

Requirement 66: Supplementary control room

Instrumentation and control equipment shall be available, preferably at a single location (supplementary control room) that is physically independent, electrically separated and functionally isolated 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 if there is a loss of ability to perform these essential safety functions in the control room.

6.44. The requirements of para. 6.43 for the protection of operating personnel also apply for the supplementary control room.

Requirement 67: Emergency control centre

An on-site emergency control centre, separated from the plant control room and supplementary control room, shall be provided from which the emergency response can be directed.

6.45. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings shall be provided in the on-site emergency control centre. The centre shall provide means of communication with the control room, the supplementary control room and other important points in the plant, and with the on-site and off-site emergency response organizations. Appropriate measures shall be taken to protect the occupants for a protracted time against hazards resulting from accident conditions. The emergency control centre shall include the necessary facilities to permit extended periods of occupation and operation by emergency response personnel.

EMERGENCY POWER SUPPLY

Requirement 68: Emergency power supply

The emergency power supply shall be capable of supplying the necessary power in anticipated operational occurrences and accident conditions, on the assumption of the coincidental loss of off-site power.

6.46. In the design basis for the emergency power supply, account shall be taken of the postulated initiating events and the associated safety functions to be performed, to determine the requirements for capability, availability, duration of the required supply, capacity and continuity.

6.47. The combined means to provide emergency power (such as by means of water, steam or gas turbine, diesel engines or batteries) shall have a reliability and form that are consistent with all the requirements of the safety systems to be supplied, and their functional capability shall be testable.

6.48. The design basis for any diesel engine or other prime mover[10] that provides a power supply to items important to safety shall include:

(1) the capability of the associated fuel oil storage and supply systems to satisfy the required demand within the defined time period;

(2) the capability of the prime mover to start and operate successfully under all specified conditions and at the required time;

(3) the auxiliary systems of the prime mover such as coolant systems.

SUPPORTING AND AUXILIARY SYSTEMS

Requirement 69: Performance of supporting and auxiliary systems.

The design of supporting and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the component or system that they serve.

Requirement 70: Auxiliary heat transport systems

Auxiliary heat transport systems shall be provided as appropriate to remove heat from components and systems that are required to function in operational states and accident conditions.

6.49. The design shall be such as to ensure that non-essential portions of the system can be isolated.

Requirement 71: Process sampling systems and post-accident sampling systems

Process sampling systems 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 from the environment, in all operational states and accident conditions.

6.50. Appropriate means shall be provided for the monitoring of the activity in fluid systems that have a potential for significant contamination and the collection of process samples.

[10] A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.

Requirement 72: Compressed air systems

The design basis of any compressed air system that serves an item important to safety shall specify the quality, flow rate and cleanness of the air to be provided.

Requirement 73: Air conditioning systems and ventilation systems

Systems for air conditioning, heating, cooling and ventilation 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 all plant states.

6.51. Systems shall be provided for building ventilation with appropriate capability for cleanup:

(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 levels of airborne radioactive substances in the plant below authorized limits, and as low as reasonably achievable;

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

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

6.52. Areas of higher contamination shall be maintained at a depression (partial vacuum) relative to areas of low contamination and other accessible areas.

Requirement 74: Fire protection systems

Fire protection systems, including fire detection and fire extinguishing systems, fire containment barriers and smoke control systems, shall be installed throughout the plant with account taken of the results of the fire hazard analysis.

6.53. The fire systems installed shall be capable of dealing safely with fire events of the various types that are postulated.

6.54. Fire extinguishing systems shall be automatically actuated where appropriate. Systems shall be designed and located so as to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety.

6.55. The fire detection systems shall be designed to inform the operating personnel promptly of the location and spread of any fires that start.

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

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

Requirement 75: Lighting systems

Adequate lighting shall be provided to facilitate safe operation in all operational areas of the plant in operational states and in accident conditions.

Requirement 76: Overhead lifting equipment

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

6.58. The lifting equipment shall be designed so that:

(1) measures are provided to prevent the lifting of excessive loads;

(2) conservative design measures are applied to prevent any uncontrolled load drop that may affect items important to safety;

(3) the plant layout permits the safe movement of the lifting equipment and the items being transported;

(4) the equipment can be used only in specified plant states (owing to safety interlocks on the crane);

(5) lifting equipment operating in areas where items important to safety are located is seismically qualified.

OTHER POWER CONVERSION SYSTEMS

Requirement 77: Steam supply system, feedwater system and turbine generators

The design of the steam supply system, feedwater system and turbine generators shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in normal operation, anticipated operational occurrences or accident conditions.

6.59. The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in normal operation, anticipated operational occurrences or accident conditions.

6.60. Steam supply systems and feedwater systems shall be of adequate capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions.

6.61. The turbine generators shall be provided with appropriate protection such as overspeed protection and vibration protection, and measures shall be taken to minimize the possible effects of turbine generated missiles on items important to safety.

TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

Requirement 78: Waste treatment and control systems

Systems shall be provided for treating solid and liquid radioactive waste to keep the quantities and concentrations of operational radioactive releases within authorized limits and as low as reasonably achievable.

6.62. Systems and facilities shall be provided for the management and safe storage of radioactive waste on the site for a period of time consistent with the availability of the disposal option.

6.63 The design shall incorporate appropriate features to facilitate the movement and handling of radioactive waste. Consideration shall be given to the provision of access to facilities and to capabilities for lifting and for packaging .

Requirement 79: Effluent treatment and control systems

Systems shall be provided for treating liquid and gaseous radioactive effluents to keep their quantities within authorized limits and as low as reasonably achievable.

6.64. Liquid and gaseous radioactive effluents shall be treated so that exposure of members of the public due to discharges to the environment is as low as reasonably achievable.

6.65. The plant shall include suitable means to control the release of radioactive liquids to the environment to be as low as reasonably achievable and to ensure that emissions and concentrations remain within authorized limits.

6.66. The cleanup equipment for the off gas or extract stream shall provide the necessary retention factor to meet the authorized limits for discharges and the filter systems shall be designed so that their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air.

FUEL HANDLING AND STORAGE SYSTEMS

Requirement 80: 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.

6.67. The design shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel.

6.68. The design shall be such as to prevent any significant damage to items important to safety during the transfer of fuel or casks, or in the event of fuel or casks being dropped.

6.69. The storage system and handling system for irradiated and non-irradiated fuel shall be designed:

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

(2) to permit inspection of the fuel;

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

(4) to prevent possible damage to the fuel;

(5) to prevent the dropping of fuel in transit;

(6) to provide for the identification of individual fuel assemblies;

(7) to provide proper means for radiation protection;

(8) to ensure that adequate operating procedures and a system of accounting for and control of fuel can be implemented to prevent any loss of fuel.

6.70. In addition, the storage system and handling system for irradiated fuel shall be designed:

(1) to permit adequate heat removal in operational states and in accident conditions;

(2) to prevent the dropping of spent fuel in transit;

(3) to prevent unacceptable handling stresses on fuel elements or fuel assemblies;

(4) to prevent the dropping of heavy objects such as spent fuel casks, cranes or other potentially damaging objects on the fuel;

(5) to permit safe storage of suspect or damaged fuel elements or fuel assemblies;

(6) to control levels of soluble absorber if this is used for criticality safety;

(7) to facilitate maintenance and eventual decommissioning of fuel storage and handling facilities;

(8) to facilitate decontamination of fuel storage and handling areas and equipment when necessary;

(9) to accommodate all the fuel removed from the reactor in accordance with the core management strategy foreseen and the amount of fuel in the full core, with adequate margins.

6.71. For reactors using a water pool system for fuel storage, the design shall include the 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;

(3) means to prevent the uncovering of fuel assemblies in the pool in the event of a pipe break (i.e. antisyphon measures).

RADIATION PROTECTION

Requirement 81: Design for radiation protection

Provision shall be made for ensuring that the radiation dose to site personnel will be maintained below the dose limits and the dose constraints and will be kept as low as reasonably achievable.

6.72. Radiation sources throughout the plant shall be comprehensively identified and exposures associated with them shall be kept as low as reasonably achievable[11], the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

6.73. Materials used in the fabrication of structures, systems and components shall be selected so as to minimize as far as reasonably practicable activation of the material.

6.74. For the purposes of radiation protection, provision shall be made for preventing the release or the spread of radionuclides, radioactive waste and contamination.

6.75. The plant layout shall be such as to ensure that access of operating personnel to areas with radiation hazards and areas of possible contamination is adequately controlled, and that

[11] Requirements on radiation protection for facilities and activities are established in Ref. [11].

by this means and by means of ventilation systems, exposure and contamination are prevented or reduced.

6.76. The plant shall be divided into zones that are related to their expected occupancy, and to radiation and contamination levels in operational states (including refuelling, maintenance and inspection) and potential levels in accident conditions. Shielding shall be provided so that radiation exposure is kept as low as reasonably achievable.

6.77. The plant layout shall be such as to ensure that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection are as low as reasonably achievable, and the requirements for special equipment to be provided to achieve these objectives shall be taken into account.

6.78. Plant equipment requiring frequent maintenance or manual operation shall be located in areas of low dose rate to reduce the exposure of workers.

6.79. Facilities shall be provided for decontamination of operating personnel, plant and equipment.

Requirement 82: Means of radiation monitoring

Equipment shall be provided to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as practicable, in design extension conditions.

6.80. Stationary dose rate meters shall be provided for monitoring local radiation dose rates 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.

6.81. Stationary dose rate meters shall be installed to indicate the general radiation level at appropriate locations in the event of accident conditions. These instruments shall provide sufficient information in the control room or at the appropriate control position that operating personnel can initiate corrective action if necessary.

6.82. Stationary monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by operating personnel and where the levels of activity of airborne radioactive material may on occasion be expected to

be such as to necessitate protective measures. These systems shall provide an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected. Monitors shall also be provided in areas subject to possible contamination as a result of equipment failure or other unusual circumstances.

6.83. Stationary equipment and laboratory facilities shall be provided for determining in a timely manner the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or from the environment, in operational states and in accident conditions.

6.84. Stationary equipment shall be provided for monitoring, prior to or during discharge to the environment, radioactive effluents and effluents that may have become contaminated.

6.85. Instruments shall be provided for measuring radioactive surface contamination. Stationary monitors (e.g. portal radiation monitors, hand and foot monitors) shall be provided at the main exit points from the controlled areas and supervised areas, to facilitate the control of operating personnel and equipment.

6.86. Facilities shall be provided for monitoring of individual doses to and contamination of operating personnel. Processes shall also be in place to measure and record the cumulative doses to workers over time.

6.87. Arrangements shall be made to determine the radiological impacts, if any, in the vicinity of the plant by the surveillance of activity concentrations and contamination and doses and dose rates with particular reference to:

(1) pathways to the human population, including the food-chain;

(2) the radiological impacts, if any, on local ecosystems;

(3) the possible accumulation of radioactive material in the physical environment;

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

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2.2, IAEA, Vienna (2010).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).[[References from [8] still to be cited in text.]

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2003).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2.2, IAEA, Vienna (2010).

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

[12] The Agency's Safeguards System, INFCIRC/66/Rev.2, IAEA, Vienna (1968).

[13] Model Protocol Additional to the Agreement(s) Between State(s) and the International Atomic Energy Agency for the Application of Safeguards, INFCIRC/540(Corrected), IAEA, Vienna (1997).

[14] The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, INFCIRC/153(Corrected), IAEA, Vienna (1972).

[15] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999); Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities, IAEA-TECDOC-967 Rev.1, IAEA, Vienna (2000); Amendment to the Convention on the Physical Protection of Nuclear Material, IAEA International Law Series No. 2, IAEA, Vienna (2006). (The final act of the new Convention on the Physical Protection of Nuclear Material and Nuclear Facilities was approved on 8 July 2005. See http://www.iaea.org/NewsCenter/Features/PhysicalProtection/index.html).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[18] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE CO-ORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material (2009 Edition), IAEA Safety Standards Series No. TS-R-1, IAEA, Vienna (2009).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Governmental, Legal and Regulatory Framework for Safety, IAEA Safety Standards Series No. GSR Part 1, IAEA, Vienna (2010).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2003).

DEFINITIONS

The following definitions, which differ from those in the IAEA Safety Glossary (2007 Edition), will be reflected in the next edition of that Glossary.

plant states (considered in design)

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions

accident conditions

Deviations from *normal operation less frequent and* more severe than *anticipated operational occurrences, which include design basis accidents and design extension conditions*.

design basis accidents

Accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which the release of radioactive material is kept within acceptable limits.

beyond design basis accidents

This term used in earlier IAEA publications is superseded by **design extension conditions**

design extension conditions

Accident conditions of lower frequency than design basis accidents in which doses or radioactive releases could exceed acceptable limits for design basis accidents. These include conditions with or without significant core degradation.

s**afety feature**

Equipment designed to perform or which has a safety function in design extension conditions.

safety system settings

The levels at which safety systems are automatically actuated in the event of *anticipated operational occurrences* or *design basis accidents*, to prevent *safety limits* from being exceeded.

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), United Kingdom
Buttery, N.	British Energy Generation Ltd., United Kingdom
Carluec, B.	AREVA NP, France
Cowley, J.S.	Private Consultant, United Kingdom
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), United Kingdom
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
Semenas, 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