

IAEA SAFETY STANDARDS SERIES

SPECIFIC SAFETY REQUIREMENTS No. SSR-2/1 [Rev.1](#)

SAFETY OF
NUCLEAR POWER PLANTS:
DESIGN

PREFACE

Revision through addenda of GSR Part 1, NS-R-3, SSR-2/1, SSR-2/2 and GSR Part 4

In the aftermath of the TEPCO's Fukushima Daiichi NPPs accident following the disastrous earthquake and tsunami of 11 March 2011, the IAEA Action Plan on Nuclear Safety approved by the IAEA Board of Governors and the General Conference in September 2011 (GOV/2011/59-GC(55)/14) includes an action to "Review and strengthen IAEA Safety Standards and improve their implementation".

It requires the Commission on Safety Standards and the IAEA Secretariat to review, and revise as necessary using the existing process in a more efficient manner, the relevant IAEA Safety Standards in a prioritised sequence.

The Secretariat started the review in 2011 of the IAEA Safety Requirements on the basis of the lessons from the information that was available, including the two reports from the Government of Japan, issued in June and September 2011, the report of the IAEA Fact Finding Mission conducted from 24 May to 2 June 2011 and the letter from INSAG dated 26 July 2011. The result of the work of the Secretariat and of its consideration by the four Safety Standards Committees early in 2012 was submitted to the Commission on Safety Standards at its meeting in March 2012¹. On that basis, the Commission on Safety Standards approved, at its meeting in October 2012, a document outline to initiate the revision process, through addenda and in a concomitant manner of GSR Part 1, NS-R-3, SSR-2/1, SSR-2/2 and GSR Part 4.

Additional inputs were considered in 2012 and 2013 when preparing the draft, including the findings of International Experts' Meetings

1 The report is available at the following address:

[http://www-](http://www-ns.iaea.org/committees/files/CSScomments/1188/Agendaltem5.3ProgressReportonthereviewofSafetyStandardsrev23february2012.doc)

[ns.iaea.org/committees/files/CSScomments/1188/Agendaltem5.3ProgressReportonthereviewofSafetyStandardsrev23february2012.doc](http://www-ns.iaea.org/committees/files/CSScomments/1188/Agendaltem5.3ProgressReportonthereviewofSafetyStandardsrev23february2012.doc)

and presentations made at the Second Extraordinary meeting of contracting parties to the Convention on Nuclear Safety. Several national and regional reports were also analysed.

The review consisted of a comprehensive analysis of the findings that were identified in these reports and meetings. In the light of the result of this analysis, the IAEA Safety Requirements were examined in a systematic manner in order to identify whether some modifications were desirable to reflect any of the findings. This comparative review was intended to provide a basis for the revisions to be made, if necessary, to ensure that the IAEA Safety Requirements are as useful as possible for Member States.

It was therefore decided to revise the following IAEA Safety Requirements: GSR Part-1 on Governmental, Legal and Regulatory Framework for Safety, NS-R-3 on Site Evaluation for Nuclear Installations, SSR-2/1 on Safety of Nuclear Power Plants: Design, SSR-2/2 on Safety of Nuclear Power Plants: Commissioning and Operation and GSR Part 4 on Safety Assessment for Facilities and Activities. After their revision, these publications will be re-issued to ensure that lessons that are to be learned from reports on and studies of the Fukushima accident are fully reflected in the relevant requirements.

For SSR-2/1, the approved revisions relate to the following main areas:

- Strengthening the prevention of unacceptable radiological consequences to the public and the environment
- Avoiding long term off site contamination through severe accident mitigation
- Preventing severe accident through strengthening the plant design basis

CONTENTS

1.	INTRODUCTION	1
	Background (1.1–1.3)	1
	Objective (1.4–1.5)	2
	Scope (1.6–1.8)	2
	Structure (1.9).....	2
2.	APPLYING THE SAFETY PRINCIPLES AND CONCEPTS (2.1–2.5)	32
	Radiation protection (2.6–2.7)	43
	Safety in design (2.8–2.11).....	54
	The concept of defence in depth (2.12–2.14)	65
	Maintaining the integrity of design of the plant throughout the lifetime of the plant (2.15–2.18)	87
3.	MANAGEMENT OF SAFETY IN DESIGN	98
	Requirement 1: Responsibilities in the management of safety in plant design (3.1)	98
	Requirement 2: Management system for plant design (3.2–3.4)	98
	Requirement 3: Safety of the plant design throughout the lifetime of the plant (3.5–3.6).....	109
4.	PRINCIPAL TECHNICAL REQUIREMENTS	110
	Requirement 4: Fundamental safety functions (4.1–4.2).....	110
	Requirement 5: Radiation protection (4.3–4.4)	11
	Requirement 6: Design for a nuclear power plant (4.5–4.8).....	121
	Requirement 7: Application of defence in depth (4.9–4.13)	132
	Requirement 8: Interfaces of safety with security and safeguards	143
	Requirement 9: Proven engineering practices (4.14–4.16).....	143
	Requirement 10: Safety assessment (4.17–4.18)	153
	Requirement 11: Provision for construction (4.19)	15
	Requirement 12: Features to facilitate radioactive waste management and decommissioning (4.20).....	165
5.	GENERAL PLANT DESIGN	165
	Design basis	165
	Requirement 13: Categories of plant states (5.1–5.2).....	165

Requirement 14: Design basis for items important to safety (5.3)	176
Requirement 15: Design limits (5.4)	176
Requirement 16: Postulated initiating events (5.5–5.15).....	17
Requirement 17: Internal and external hazards (5.16–5.22).....	19
Requirement 18: Engineering design rules (5.23)	20
Requirement 19: Design basis accidents (5.24–5.26).....	210
Requirement 20: Design extension conditions (5.27–5.32).....	21
Requirement 21: Physical separation and independence of safety systems (5.33)	232
Requirement 22: Safety classification (5.34–5.36).....	23
Requirement 23: Reliability of items important to safety (5.37–5.38) .	243
Requirement 24: Common cause failures	24
Requirement 25: Single failure criterion (5.39–5.40).....	24
Requirement 26: Fail-safe design (5.41)	254
Requirement 27: Support service systems (5.42–5.43)	25
Requirement 28: Operational limits and conditions for safe operation (5.44)	25
Design for safe operation over the lifetime of the plant	26
Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety (5.45–5.47)	26
Requirement 30: Qualification of items important to safety (5.48–5.50).....	276
Requirement 31: Ageing management (5.51–5.52).....	287
Human factors	28
Requirement 32: Design for optimal operator performance (5.53–5.62).....	28
Other design considerations	29
Requirement 33: Sharing of safety systems between multiple units of a nuclear power plant (5.63).....	3029
Requirement 34: Systems containing fissile material or radioactive material	3029
Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination	30
Requirement 36: Escape routes from the plant (5.64–5.65)	30
Requirement 37: Communication systems at the plant (5.66–5.67)	310
Requirement 38: Control of access to the plant (5.68)	31
Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety	321
Requirement 40: Prevention of harmful interactions of systems important to safety (5.69–5.70)	321

Requirement 41: Interactions between the electrical power grid and the plant	331
Safety analysis	332
Requirement 42: Safety analysis of the plant design (5.71–5.76)	332
6. DESIGN OF SPECIFIC PLANT SYSTEMS	353
Reactor core and associated features	353
Requirement 43: Performance of fuel elements and assemblies (6.1–6.3).....	353
Requirement 44: Structural capability of the reactor core	354
Requirement 45: Control of the reactor core (6.4–6.6)	354
Requirement 46: Reactor shutdown (6.7–6.12).....	365
Reactor coolant systems	375
Requirement 47: Design of reactor coolant systems (6.13–6.16)	375
Requirement 48: Overpressure protection of the reactor coolant pressure boundary	386
Requirement 49: Inventory of reactor coolant	386
Requirement 50: Cleanup of reactor coolant (6.17)	386
Requirement 51: Removal of residual heat from the reactor core	397
Requirement 52: Emergency cooling of the reactor core (6.18–6.19).....	397
Requirement 53: Heat transfer to an ultimate heat sink	4038
Containment structure and containment system	4038
Requirement 54: Containment system for the reactor	4038
Requirement 55: Control of radioactive releases from the containment (6.20–6.21)	4038
Requirement 56: Isolation of the containment (6.22–6.24)	4138
Requirement 57: Access to the containment (6.25–6.26)	4138
Requirement 58: Control of containment conditions (6.27–6.30)	420
Instrumentation and control systems	431
Requirement 59: Provision of instrumentation (6.31)	431
Requirement 60: Control systems	431
Requirement 61: Protection system (6.32–6.33)	431
Requirement 62: Reliability and testability of instrumentation and control systems (6.34–6.36)	442
Requirement 63: Use of computer based equipment in systems important to safety (6.37).....	452
Requirement 64: Separation of protection systems and control systems (6.38).....	453

Requirement 65: Control room (6.39–6.40)	453
Requirement 66: Supplementary control room (6.41)	464
Requirement 67: Emergency control centre (6.42).....	464
Emergency power supply	475
Requirement 68: Emergency power supply (6.43–6.45)	475
Supporting systems and auxiliary systems	486
Requirement 69: Performance of supporting systems and auxiliary systems	486
Requirement 70: Heat transport systems (6.46).....	486
Requirement 71: Process sampling systems and post-accident sampling systems (6.47)	496
Requirement 72: Compressed air systems	497
Requirement 73: Air conditioning systems and ventilation systems (6.48–6.49)	497
Requirement 74: Fire protection systems (6.50–6.54).....	5047
Requirement 75: Lighting systems	5148
Requirement 76: Overhead lifting equipment (6.55).....	5148
Other power conversion systems	5149
Requirement 77: Steam supply system, feedwater system and turbine generators (6.56–6.58).....	5149
Treatment of radioactive effluents and radioactive waste	5249
Requirement 78: Systems for treatment and control of waste (6.59–6.60).....	5249
Requirement 79: Systems for treatment and control of effluents (6.61–6.63).....	5250
Fuel handling and storage systems	530
Requirement 80: Fuel handling and storage systems (6.64–6.68)	530
Radiation protection	542
Requirement 81: Design for radiation protection (6.69–6.76).....	542
Requirement 82: Means of radiation monitoring (6.77–6.84)	553
REFERENCES	585
DEFINITIONS	596
CONTRIBUTORS TO DRAFTING AND REVIEW	6158
BODIES FOR THE ENDORSEMENT OF	
—IAEA SAFETY STANDARDS.....	60

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. Account has been taken of the publication in 2006 of the Fundamental Safety Principles [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 and other nuclear facilities. It is recognized that technology and scientific knowledge advance, and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. Safety requirements will change over time; this Safety Requirements publication reflects the present consensus.

1.2. The designs of many existing nuclear power plants, as well as the designs for new nuclear power plants, have been enhanced to include additional measures to mitigate the consequences of complex accident sequences involving multiple failures and of severe accidents. Complementary systems and equipment with new capabilities have been backfitted to many existing nuclear power plants to aid in the prevention of severe accidents and the mitigation of their consequences. Guidance on the mitigation of the consequences of severe accidents has been provided at most existing nuclear power plants. The design of new nuclear power plants now explicitly includes the consideration of severe accident scenarios and strategies for their management. Requirements related to the State system of accounting for, and control of, nuclear material and security related requirements are also taken into account in the design of nuclear power plants. Integration of safety measures and security measures will help to ensure that neither compromise the other.

1.3. It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction; in addition, it might not be feasible to modify designs that have already been approved by regulatory bodies. For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements.

OBJECTIVE

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

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

SCOPE

1.6. 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). This publication may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design.

1.7. This publication does not address:

- (a) Requirements that are specifically covered in other IAEA Safety Requirements publications (e.g. Ref. [2]);
- (b) Matters relating to nuclear security or to the State system of accounting for, and control of, nuclear material;
- (c) Conventional industrial safety that under no circumstances could affect the safety of the nuclear power plant;
- (d) Non-radiological impacts arising from the operation of nuclear power plants.

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

STRUCTURE

1.9. This Safety Requirements publication follows the relationship between the safety objective and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety

objective, safety principles and concepts that form the basis for deriving the safety function requirements that must be met for the nuclear power plant, as well as the safety design criteria. Sections 3–6 establish numbered overarching requirements (shown in bold type), with additional requirements as appropriate. Section 3 establishes the general requirements to be satisfied by the design organization in the management of safety in the design process. Section 4 establishes requirements for the principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction, and requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material, and for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 establishes requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. The requirements for general plant design apply to all items (i.e. structures, systems and components) important to safety. Section 6 establishes requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems.

2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS

2.1. The Fundamental Safety Principles [1] establish one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks.

2.2. This fundamental safety objective has to be achieved, and the ten safety principles have to be applied, without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that nuclear power plants are operated and activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following (see Ref. [1], para. 2.1):

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

(b) To restrict the likelihood of 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 a nuclear power plant;

(c) To mitigate the consequences of such events, were they to occur.

2.3. The fundamental safety objective applies for all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste (see Ref. [1], para. 2.2).

2.4. The Fundamental Safety Principles (Ref. [1], para. 2.3) state that:

“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 Safety Requirements publication establishes requirements that 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 for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the dose limits and kept as low as reasonably achievable. In addition, it is required to implement measures for mitigating the radiological consequences of any accidents, were they 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 exposures or the release of authorized amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept as low as reasonably achievable, in compliance with regulatory and operational limits as well as radiation protection requirements [94].

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, measures shall be taken to do the following, consistent with national acceptance criteria and safety objectives [1]:

- (a) To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or other sources of radiation, and to mitigate the consequences of any accidents that do occur;
- (b) To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;
- (c) To ensure that the likelihood of occurrence of an accident with serious radiological consequences 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 possible sources of radiation and to evaluate the possible doses that could be received by workers at the installation and by members of the public, as well as the possible effects on the environment, as a result of operation of the plant. The safety assessment is required in order to examine: (i) normal operation of the plant, (ii) the performance of the plant in anticipated operational occurrences, and (iii) 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 items important to safety can be demonstrated and the inputs (prerequisites) for emergency planning can be established.

2.10. Measures shall be taken to control exposure for all operational states at 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 will remain a possibility that an accident could happen. Measures shall be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site intervention measures by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident has occurred.

2.11. The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and the environment of nuclear or radiation incidents (Ref. [1]).

Principle 9): plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated² and 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 be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities.

THE CONCEPT OF DEFENCE IN DEPTH

2.12. The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. 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 induced events within the plant, and against consequences of events that originate outside the plant.

2.13. Application of the concept of defence in depth in the design of a nuclear power plant provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails. ~~The independent effectiveness of each of the different levels of defence is an essential element of defence in depth at the plant and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. There are five levels of defence:~~

(1) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and

² 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

to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

(2)The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that 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 safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return 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 might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such 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 damage to the reactor core or significant off-site releases and returning the plant to a safe state.

(4)The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This level is aimed at preventing the progression of fuel damage and mitigating consequences of severe accidents. In case of a severe accident, the most important objective for this level is to ensure the confinement function, thus ensuring that significant radioactive releases would be practically eliminatedare kept as low as reasonably achievable.

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

3 "significant radioactive releases": Those releases for which only limited protective measures in area and time are insufficient to protect the public and the environ-

2.13a The independent effectiveness of each of the different levels of defence is an essential element of defence in depth at the plant and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. The independence of levels three and four is of particular relevance because of the severity of potential consequences should simultaneous failures of these two levels occur.

2.14. A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

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

2.15. The design, construction and commissioning of a nuclear power plant might 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 systems, and the suppliers of other systems that are important to the safety of the plant.

2.16. 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 operating organization) [1]. The International Nuclear Safety Advisory Group [7] has suggested that the operating organization could set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e. during the operating lifetime and into the decommissioning stage). A formally designated entity within the operating organization would take responsibility for this process.

2.17. In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. Reference [7] emphasizes the need for a formally designated entity that has overall responsibility for the design process and is responsible for approving design changes and for ensuring that the requisite knowledge is maintained. Reference [7] also introduces the concept of ‘responsible designers’ to whom this formally designated entity could assign specific responsibilities for the design of parts of the plant. Prior to an application for authorization of a plant, the responsibility for the design will rest with the design organization (e.g.

the vendor). Once an application for authorization of a plant has been made, the prime responsibility for safety will lie with the applicant, although 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 knowledge embodied in the safety analysis report, design manuals and other design documentation, will be transferred to the operating organization. To facilitate this transfer of knowledge, the structure of the formally designated entity that has overall responsibility for the design process would be established at an early stage.

2.18. The management system requirements that are placed on this formally designated entity would also apply to the responsible designers. However, the overall responsibility for maintaining the integrity of design of the plant would 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 plant design

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

3.1. All organizations, including the design organization⁴, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.

⁴ The design organization is the organization responsible for preparation of the final

Requirement 2: Management system⁵ for plant design

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

3.2. The management system shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.

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

3.4. The adequacy of the plant 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 design work. Verification, validation and approval of the plant design shall be completed as soon as is practicable in the design and construction processes, and in any case before operation of the plant is commenced.

Requirement 3: Safety of the plant design throughout the lifetime of the plant

The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.

3.5. The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant 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 relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following:

- (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable;
- (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;
- (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings;
- (d) That management of design requirements and configuration control are maintained;
- (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled;
- (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;
- (g) That all design changes to the plant are reviewed, verified, documented and approved;
- (h) That adequate documentation is maintained to facilitate future decommissioning of the plant.

4. PRINCIPAL TECHNICAL REQUIREMENTS

Requirement 4: Fundamental safety functions

Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, 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 identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states.

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

Requirement 5: Radiation protection⁶

The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they 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 lead to high radiation doses or large radioactive releases are practically eliminated (see footnote 1) and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

4.4. Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.

Requirement 6: Design for a 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 necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

4.5. The design for a nuclear power plant shall be such as to ensure that the safety requirements of the operating organization, the requirements of the

⁶ Requirements on radiation protection and the safety of radiation sources for facilities

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 of 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 administrative and operational procedures for the plant (i.e. the 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 nuclear power plants, and of the results of relevant research programmes.

4.7. The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration has been given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur.

4.8. The design shall be such as to ensure that the generation of radioactive waste and 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 of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.

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

4.10. The design shall take due account 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 in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.

4.11. The design:

(a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;

- (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect⁷;
- (c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;
- (d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;
- (e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems;
- (f) 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 is practicable:

- (a) Challenges to the integrity of physical barriers;
- (b) Failure of one or more barriers;
- (c) Failure of a barrier as a consequence of the failure of another barrier;
- (d) The possibility of harmful consequences of errors in operation and maintenance.

4.13. The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.

Requirement 8: Interfaces of safety with security and safeguards

Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear

⁷ 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

power plant 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 for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.

4.14. Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested.

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 quality of the design is commensurate with the associated safety function.

4.16. Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice 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 of the plant is as expected.

Requirement 10: Safety assessment⁸

Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified.

4.17. The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical

⁸ Requirements on safety assessment for facilities and activities are established in

activities, and shall increase in scope and level of detail as the design programme progresses.

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

Requirement 11: Provision for construction

Items important to safety for a nuclear power plant 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 level of safety.

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

Requirement 12: Features to facilitate radioactive waste management and decommissioning

Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant.

4.20. In particular, the design shall take due account of:

- (a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;
- (b) The access capabilities and the means of handling that might be necessary;
- (c) The facilities necessary for the treatment and storage of radioactive waste generated in operation and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

5. GENERAL 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 primarily on the basis of their frequency of occurrence at the nuclear power plant.

5.1. Plant states shall typically cover:

- (a) Normal operation;
- (b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;
- (c) Design basis accidents;
- (d) Design extension conditions, including accidents with significant degradation of the reactor core.

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

Requirement 14: Design basis for items important to safety

The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.

5.3. The design basis for each item important to safety shall be systematically justified and 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 for the nuclear power plant shall be specified for all operational states and for accident conditions.

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

Requirement 16: Postulated initiating events

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

5.5. The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided, to show that all foreseeable events have been considered.

5.6. The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating 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 for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed.

5.8. The expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:

(1) A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.

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

(3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event.

(4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures.

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

5.10. A technically supported justification shall be provided for 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 would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.

5.12. Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.

5.13. The operator actions that would be 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 status of the plant, and adequate controls for the manual operation of equipment.

5.14. The design shall specify the necessary provision of equipment and the procedures necessary 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 for actions to be taken in manual response and recovery processes shall be placed at the most suitable location to ensure its

availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

Requirement 17: Internal and external hazards

All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered when establishing plant layout, for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

5.15a Items important to safety shall be designed and located, considering other safety implications, to limit their exposure to hazards and possible harmful consequences of their failures.

Internal hazards

5.16. The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised.

External hazards⁹

5.17. The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, ~~including meteorological, hydrological, geological and seismic events~~. Human induced external events arising from nearby industries and transport routes shall be addressed. Causality and likelihood shall be considered in postulating potential concurrent hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

~~5.18. Items important to safety shall be designed and located to minimize, consistent with other safety requirements, the likelihood of external events and their possible harmful consequences.~~

Fo
Au
cm
Ko

5.19. Features shall be provided to minimize any interactions between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design.

5.20. The design shall be such as to ensure that those items that are necessary to fulfil the fundamental safety functions~~important to safety~~ are capable of withstanding the effects of external hazard events considered in the design basis, and if not, other features such as passive barriers shall be provided to protect those items~~the plant~~ and to ensure that the required safety function will be performed.

5.21. The design of items important to safety shall include sufficient provisions or margins to avoid cliff edge effects for external hazards of a severity or duration moderately exceeding those considered in their design basis.~~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 5).~~

5.22. For multiple unit plant sites, the design shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units on the site.

Requirement 18: Engineering design rules

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

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

Requirement 19: 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 nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.

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

5.25. The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures.

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

Requirement 20: Design extension conditions

A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur.

5.27. An analysis of design extension conditions for the plant shall be performed¹⁰. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or

¹⁰ This could be done with a best estimate approach (more stringent approaches may be

to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that significant radioactive releases would be practically eliminated (see footnote 1). The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

5.28. 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 for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.

5.29. The analysis undertaken shall include identification of the features that are designed for use in, or that are capable¹¹ of preventing or mitigating, events considered in the design extension conditions. These features:

(a) Shall be independent, to the extent practicable, of those used in more frequent accidents;

(b) Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate;

(c) Shall have a reliability commensurate with the function that they are required to fulfil.

(d) Shall include sufficient design margins to remain operational in conditions moderately more severe than those considered in their design basis to avoid cliff edge effects to occur.

5.30. In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments.

¹¹ For returning the plant to a safe state or for mitigating the consequences of an accident, consideration could be given to the full design capabilities of the plant and to the

5.31. The design shall be such that ~~design extension~~ conditions that could lead to significant radioactive releases are practically eliminated (see footnote 1). ~~If not, for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.~~

~~5.31a~~~~If not, f~~For design extension conditions ~~that cannot be practically eliminated~~, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.

Combinations of events and failures

5.32. Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might 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 21: Physical separation and independence of safety systems

Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

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

Requirement 22: Safety classification

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

5.34. The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented, where appropriate, by probabilistic methods, with due account taken of factors such as:

(a) The safety function(s) to be performed by the item;

- (b)The consequences of failure to perform a safety function;
- (c)The frequency with which the item will be called upon to perform a safety function;
- (d)The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

5.35. The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class.

5.36. Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.

Requirement 23: Reliability of items important to safety

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

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

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

Requirement 24: Common cause failures

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Requirement 25: Single failure criterion

The single failure criterion shall be applied to each safety group incorporated in the plant design.¹²

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

5.40. The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.

Requirement 26: Fail-safe design

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

5.41. Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.

Requirement 27: Support service systems

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

5.42. The reliability, redundancy, diversity and independence of support service systems 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 being supported.

¹² A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system

5.43. It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions and compromising the capability of these systems to fulfil their safety functions.

Requirement 28: Operational limits and conditions for safe operation

The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.

5.44. The requirements and operational limits and conditions established in the design for the nuclear power plant shall include (Req. 6, Ref. [4]):

- (a) Safety limits;
- (b) Limiting settings for safety systems;
- (c) Operational limits and conditions for operational states;
- (d) Control system constraints and procedural constraints on process variables and other important parameters;
- (e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;
- (f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;
- (g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions.

DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT

Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety

Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

5.45. The plant layout shall be such that activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be commensurate with the importance of the safety

functions to be performed, and shall be performed without undue exposure of workers.

5.46. Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions.

5.47. If an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable, a robust technical justification shall be provided that incorporates the following approach:

(a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified.

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

Requirement 30: Qualification of items important to safety

A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

5.48. The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant.

5.49. The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to

safety by the natural event, either by test or by analysis or by a combination of both.

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

Requirement 31: Ageing management

The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

5.51. The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event.

5.52. Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behaviour of the plant or degradation that might occur in service.

HUMAN FACTORS

Requirement 32: Design for optimal operator performance

Systematic consideration of human factors, including the human-machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.

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

5.54. Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is

given as early as possible in the process to the future operation and maintenance of equipment.

5.55. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall pay attention to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant in operational states and accident conditions.

5.56. The human-machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented.

5.57. The operator shall be provided with the necessary information:

- (a) To assess the general state of the plant in any condition;
- (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);
- (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;
- (d) To determine both the need for and the time for manual initiation of the specified safety actions.

5.58. The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator.

5.59. 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 sufficient time to act.

5.60. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel.

5.61. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts.

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

OTHER DESIGN CONSIDERATIONS

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

Safety systems shall not be shared between multiple units unless, in accident conditions, this contributes to enhanced safety for the units.

5.63. Safety system support features and safety related items shall be permitted to be shared between several units of a nuclear power plant if this contributes to safety. Such sharing shall not be permitted if it would increase either the likelihood or the consequences of an accident at any unit of the plant.

Requirement 34: Systems containing fissile material or radioactive material

All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: 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 radioactive releases of material are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.

Requirement 35: Nuclear 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 processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions.

Requirement 36: Escape routes from the plant

A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.

5.64. Escape routes from the nuclear power plant 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.

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

Requirement 37: Communication systems at the plant

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

5.66. Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions.

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

Requirement 38: Control of access to the plant

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

5.68. Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.

Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety

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

Requirement 40: Prevention of harmful interactions of systems important to safety

The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

5.69. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction

on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

5.70. 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 prevent 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 at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

SAFETY ANALYSIS

Requirement 42: Safety analysis of the plant design

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

5.71. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed (see footnote 6). It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.

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

5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant.

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

Deterministic approach

5.75. The deterministic safety analysis shall mainly provide:

- (a) Establishment and confirmation of the design bases for all items important to safety;
- (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
- (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;
- (d) Comparison of the results of the analysis with dose limits and acceptable limits, and with design limits;
- (e) Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;
- (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

Probabilistic approach

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

- (a) 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 risks, and that, to the extent practicable, the levels of defence in depth are independent;
- (b) Providing assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented (see footnote 5);
- (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

6. DESIGN OF SPECIFIC PLANT SYSTEMS

REACTOR CORE AND ASSOCIATED FEATURES

Requirement 43: Performance of fuel elements and assemblies

Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.

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

6.2. Fuel design limits shall include limits on the permissible leakage of fission products from the fuel in anticipated operational occurrences so that the fuel remains suitable for continued use.

6.3. Fuel elements and fuel assemblies shall be capable of withstanding the loads and stresses associated with fuel handling.

Requirement 44: Structural capability of the reactor core

The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and 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 reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational

occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

6.4. Adequate means of detecting the neutron flux distributions in the reactor 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, due account shall be taken of wear out and of the 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 states and accident conditions not involving degradation of the reactor core shall be limited or compensated for to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core.

Requirement 46: Reactor shutdown

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

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

6.8. In judging the adequacy of the means of shutdown of the reactor, 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 that 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 reactor core.

6.11. The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown, or during refuelling operations or other routine or non-routine operations in the shutdown state.

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

REACTOR COOLANT SYSTEMS

Requirement 47: Design of reactor coolant systems

The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.

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

6.14. The design of the reactor coolant pressure boundary shall be such 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 and to rapid crack propagation, thereby permitting the timely detection of flaws.

6.15. The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could exhibit embrittlement 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 consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service.

Requirement 48: Overpressure protection of the reactor 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 systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant 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 state of the nuclear power plant, with due account taken of volumetric changes and leakage.

Requirement 50: Cleanup of reactor coolant

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

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

Requirement 51: Removal of residual heat from the reactor core

Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.

Requirement 52: Emergency cooling of the reactor core

Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the pressure boundary of the primary coolant system is not maintained.

6.18. The means provided for cooling of the reactor core shall be such as to ensure that:

- (a) The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded;
- (b) Possible chemical reactions are kept to an acceptable level;
- (c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;
- (d) Cooling of the reactor core will be ensured for a sufficient time.

6.19. Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of para. 6.18 with adequate 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 at the nuclear power plant to an ultimate heat sink. This function shall be carried out with very high levels of reliability for all plant states.

6.19a If the availability of the ultimate heat sink cannot be demonstrated for all potential conditions generated by external hazards, an alternative ultimate heat sink that it is not impaired by the same hazards shall be provided.

CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

Requirement 54: Containment system for the reactor

A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) confinement of radioactive substances in operational states and in accident conditions, (ii) protection of the reactor against natural external events and human induced events and (iii) radiation shielding in operational states and in accident conditions.

Requirement 55: Control of radioactive releases from the containment

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

6.20. The containment structure and the 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 through the containment have been installed and, if necessary, during the operating lifetime of the plant, so that the leak rate can be tested at the containment design pressure.

6.21. 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 caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

Requirement 56: Isolation of the containment

Each line that penetrates the containment at a nuclear power plant 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.

6.22. Lines that penetrate the containment as part of the reactor coolant pressure boundary and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series¹³ and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.

6.23. Exceptions to the requirements for containment isolation stated in para. 6.22 shall be permissible for specific classes of lines such as instrumentation lines, or in cases in which application of the methods of containment isolation specified in para. 6.22 would reduce the reliability of a safety system that includes a penetration of the containment.

6.24. Each line that penetrates the 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. The containment isolation valves shall be located outside the containment and as close to the containment as is practicable.

Requirement 57: Access to the containment

Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.

6.25. Where provision is made for entry of operating personnel for surveillance purposes, provision for ensuring protection and safety for operating personnel shall be specified in the design. Where equipment airlocks are provided,

¹³ In most cases, one containment isolation valve or check valve is outside the containment and the other is inside the containment. Other arrangements might be acceptable,

provision for ensuring protection and safety for operating personnel shall be specified in the design.

6.26. Containment openings for the movement of equipment or material through the containment shall be designed to be closed quickly and reliably in the event that 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 at a nuclear power plant and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.

6.27. 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 systems that are important in mitigating the effects of accident conditions.

6.28. The capability to remove heat from the containment shall be ensured, in order 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 systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

6.28a The design shall include features to facilitate the use of alternative/mobile equipment for removing heat from the containment for preserving its integrity in case of loss of all containment cooling systems.

6.28b The loss of containment integrity shall be practically eliminated. This shall be achieved without the use of means that could lead to significant radioactive releases.

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

(a) To reduce the amounts of fission products that could be released to the environment in accident conditions;

(b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment.

6.30. Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal 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 at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purposes of accident management.

6.31. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents, for predicting the locations of release and the amount of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

Requirement 60: Control systems

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

Requirement 61: Protection system

A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

6.32. The protection system shall be designed:

- (a) To be capable of overriding unsafe actions of the control system;
- (b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.

6.33. The design:

- (a) Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but not counteract correct operator actions in accident conditions;
- (b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;
- (c) Shall make relevant information available to the operator for monitoring the effects of automatic actions.

Requirement 62: Reliability and testability of instrumentation and control systems

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

6.34. Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent loss of a safety function.

6.35. Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display.

6.36. When a safety system, or part of a safety system, has 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 testing or maintenance activities.

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

If a system important to safety at the nuclear power plant 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 service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.

6.37. For computer based equipment in safety systems or safety related systems:

- (a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety;
- (b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable;
- (c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability;
- (d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided;
- (e) Common cause failures deriving from software shall be taken into consideration;
- (f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

Requirement 64: Separation of protection systems and control systems

Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.

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

Requirement 65: Control room

A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all 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 anticipated operational occurrences and accident conditions.

6.39. Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases.

6.40. Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events.

6.40a The design basis of the control room shall be such that it remains operable and habitable for a protracted period of time in situations generated by all accidents conditions and hazards with significant margins.

Requirement 66: Supplementary control room

Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

6.41. The requirements of para. 6.39 for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the supplementary control room at the nuclear power plant.

Requirement 67: ~~Emergency control~~Technical Support centre¹⁴

The design of the plant shall include an on-site emergency control~~technical support~~ centre, separate from both the plant control room and the supplementary control room, ~~shall be provided~~ from which technical support an emergency response can be ~~directed at the nuclear power plant~~provided to the operation staff during emergency conditions.

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

6.42a The design basis of the technical support centre shall be such that it remains operable and habitable for a protracted period of time in situations generated by all accident conditions and hazards with significant margins.

EMERGENCY POWER SUPPLY

Requirement 68: Emergency power supply

The emergency power supply at the nuclear power plant shall be capable of supplying the necessary power in anticipated operational occurrences and accident conditions, including in the event of prolonged~~the~~ loss of off-site power.

6.43. In the design basis for the emergency power supply at the nuclear power plant, due 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 power supply, capacity and continuity.

¹⁴ Other facilities for the management of emergencies such as the Emergency Centre are addressed in GSR Part 7: Emergency Preparedness and Response [insert

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

6.44aThe design of the emergency power supply shall be such that relevant safety features for design extension conditions can be supplied by dedicated back-up power system independent (including DC power) and physically separated from the one used in case of loss of off-site power to avoid significant core or spent fuel degradation. The same system shall be able to supply the power necessary to mitigate the consequences of a severe accident should it occurred. The dedicated back-up power system connection time shall be consistent with battery autonomy.

6.44bThe design of the emergency power supply shall be such that relevant safety features for design extension conditions could be powered by any of the available power sources.

6.45. The design basis for any diesel engine or other prime mover¹⁵ that provides an emergency power supply to items important to safety shall include:

- (a)The capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period;
- (b)The capability of the prime mover to start and to function successfully under all specified conditions and at the required time;
- (c)Auxiliary systems of the prime mover, such as coolant systems.

6.45aThe design shall include features for connection of alternative power sources (available at the site or mobile) to cope with prolonged total loss of AC power or DC sources.

¹⁵ A prime mover is a component (such as a motor, solenoid operator or pneumatic

SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

Requirement 69: Performance of supporting systems and auxiliary systems

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

Requirement 70: Heat transport systems

Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions.

6.46. The design of heat transport systems shall be such as to ensure that non-essential parts of the systems 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 specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

6.47. Appropriate means shall be provided at the nuclear power plant for the monitoring of activity in fluid systems that have the potential for significant contamination, and for the collection of process samples.

Requirement 72: Compressed air systems

The design basis for any compressed air system that serves an item important to safety at the nuclear power plant 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, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states.

6.48. Systems shall be provided for the ventilation of buildings at the nuclear power plant with appropriate capability for the cleaning of air:

- (a) To prevent unacceptable dispersion of airborne radioactive substances within the plant;
- (b) To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;
- (c) To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable;
- (d) To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents;
- (e) To control releases of gaseous radioactive material to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable.

6.49. Areas of higher contamination at the plant shall be maintained at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas.

Requirement 74: Fire protection systems

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

6.50. The fire protection systems installed at the nuclear power plant shall be capable of dealing safely with fire events of the various types that are postulated.

6.51. Fire extinguishing systems shall be capable of automatic actuation where appropriate. Fire extinguishing systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety.

6.52. Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start.

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

6.54. 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 in all operational areas of the nuclear power plant in operational states and in accident conditions.

Requirement 76: Overhead lifting equipment

Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.

6.55. The overhead lifting equipment shall be designed so that:

- (a) Measures are taken to prevent the lifting of excessive loads;
- (b) Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;
- (c) The plant layout permits safe movement of the overhead lifting equipment and of items being transported;
- (d) Such equipment can be used only in specified plant states (by means of safety interlocks on the crane);
- (e) Such equipment for use 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 for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.

6.56. 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 operational states and in accident conditions.

6.57. The steam supply system and the feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions.

6.58. 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: Systems for treatment and control of waste

Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.

6.59. Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site for a period of time consistent with the availability of the relevant disposal option.

6.60. The design of the plant shall incorporate appropriate features to facilitate the movement, transport 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: Systems for treatment and control of effluents

Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.

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

6.62. The design of the plant shall incorporate suitable means to keep the release of radioactive liquids to the environment as low as reasonably achievable and to ensure that radioactive releases remain below the authorized limits on discharges.

6.63. The cleanup equipment for the gaseous radioactive substances shall provide the necessary retention factor to keep radioactive releases below the authorized limits on discharges. 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 at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

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

6.65. The design of the plant 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.

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

- (a) To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation;
- (b) To permit inspection of the fuel;
- (c) To permit maintenance, periodic inspection and testing of components important to safety;
- (d) To prevent damage to the fuel;
- (e) To prevent the dropping of fuel in transit;
- (f) To provide for the identification of individual fuel assemblies;
- (g) To provide proper means for meeting the relevant requirements for radiation protection;
- (h) To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

6.67. In addition, the fuel handling and storage systems for irradiated fuel shall be designed:

- (a) To permit adequate removal of heat from the fuel in operational states and in accident conditions;
- (b) To prevent the dropping of spent fuel in transit;
- (c) To prevent causing unacceptable handling stresses on fuel elements or fuel assemblies;
- (d) To prevent the potentially damaging dropping on the fuel of heavy objects such as spent fuel casks, cranes or other objects;
- (e) To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;
- (f) To control levels of soluble absorber if this is used for criticality safety;
- (g) To facilitate maintenance and future decommissioning of fuel handling and storage facilities;
- (h) To facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- (i) To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;
- (j) To facilitate the removal of fuel from storage and its preparation for off-site transport.

6.68. For reactors using a water pool system for fuel storage, the design of the plant shall prevent the fuel uncover in operational and accident conditions and include the following:

- (a) Means for monitoring and controlling the water level and the temperature in all operational and accident conditions;

(b) Means for monitoring the activity in all operational and accident conditions;

(c) Means for monitoring chemistry in operational conditions;

(d) Means for preventing the uncovering of fuel assemblies in the pool in the event of a pipe break (i.e. anti-siphon measures);

(e) Means to facilitate the use of alternative/mobile equipment to ensure the long term cooling of the fuel in case of events not considered in the design.

RADIATION PROTECTION

Requirement 81: Design for radiation protection

Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.

6.69. Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable (see footnote 4), the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.

6.70. Materials used in the manufacture of structures, systems and components shall be selected to minimize activation of the material as far as is reasonably practicable.

6.71. For the purposes of radiation protection, provision shall be made for preventing the release or the dispersion of radioactive substances, radioactive waste and contamination at the plant.

6.72. 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 exposures and contamination are prevented or reduced by this means and by means of ventilation systems.

6.73. The plant shall be divided into zones that are related to their expected occupancy, and to radiation levels and contamination levels in operational states (including refuelling, maintenance and inspection) and to potential radiation

levels and contamination levels in accident conditions. Shielding shall be provided so that radiation exposure is prevented or reduced.

6.74. The plant layout shall be such that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection can be kept as low as reasonably achievable, and due account shall be taken of the necessity for any special equipment to be provided to meet these requirements.

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

6.76. Facilities shall be provided for the decontamination of operating personnel and plant equipment.

Requirement 82: Means of radiation monitoring

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

6.77. Stationary dose rate meters shall be provided for monitoring local radiation dose rates at plant locations that are routinely accessible by operating personnel and where the changes in radiation levels in operational states could be such that access is allowed only for certain specified periods of time.

6.78. Stationary dose rate meters shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. The stationary dose rate meters shall provide sufficient information in the control room or in the appropriate control position that operating personnel can initiate corrective action if necessary.

6.79. 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 substances might be such as to necessitate protective measures. These systems shall provide an indication in the control room or in other appropriate locations when a high activity 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.

6.80. Stationary equipment and laboratory facilities shall be provided for determining, in a timely manner, the concentrations of selected radionuclides in

fluid process systems, and in gas and liquid samples taken from plant systems or from the environment, in operational states and in accident conditions.

6.81. Stationary equipment shall be provided for monitoring radioactive effluents and effluents with possible contamination prior to or during discharges from the plant to the environment.

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

6.83. Facilities shall be provided for monitoring for exposure and contamination of operating personnel. Processes shall be put in place for assessing and for recording the cumulative doses to workers over time.

6.84. Arrangements shall be made to assess exposures and other radiological impacts, if any, in the vicinity of the plant by environmental monitoring of dose rates or activity concentrations, with particular reference to:

- (a) Exposure pathways to people, including the food chain;
- (b) Radiological impacts, if any, on the local environment;
- (c) The possible buildup, and accumulation in the environment, of radioactive substances;
- (d) The possibility of there being any unauthorized routes for radioactive releases.

REFERENCES

- [1]EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL 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 Rev.1, IAEA, Vienna (in preparation2009).
- [3]INTERNATIONAL ATOMIC ENERGY AGENCY, **IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection (2007 Edition)**, IAEA, Vienna (2007).
- [4]INTERNATIONAL ATOMIC ENERGY AGENCY, **Safety of Nuclear Power Plants: Commissioning and Operation**, IAEA Safety Standards Series No. SSR-2/2 Rev.1, IAEA, Vienna (in preparation2011).
- [5]INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, **Defence in Depth in Nuclear Safety**, INSAG-10, IAEA, Vienna (1996).
- [6]INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, **Basic Safety Principles for Nuclear Power Plants**, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).
- [7]INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, **Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life**, INSAG-19, IAEA, Vienna (2003).
- [8]INTERNATIONAL ATOMIC ENERGY AGENCY, **Leadership and Management for SafetyThe Management System for Facilities and Activities**, IAEA Safety Standards Series No. GSR Part 2GS-R-3, IAEA, Vienna (in preparation2006).
- [9]INTERNATIONAL ATOMIC ENERGY AGENCY, **Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards** ~~-(Interim Edition)~~, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (in preparation2011).
- [10]INTERNATIONAL ATOMIC ENERGY AGENCY, **Site Evaluation for Nuclear Installations**, IAEA Safety Standards Series No. NS-R-3 Rev.1, IAEA, Vienna (in preparation2003).
- [tbd] INTERNATIONAL ATOMIC ENERGY AGENCY. **Preparedness and Response for a Nuclear or Radiological Emergency**, IAEA Safety Standards Series No. GSR Part 7. IAEA, Vienna (in preparation).

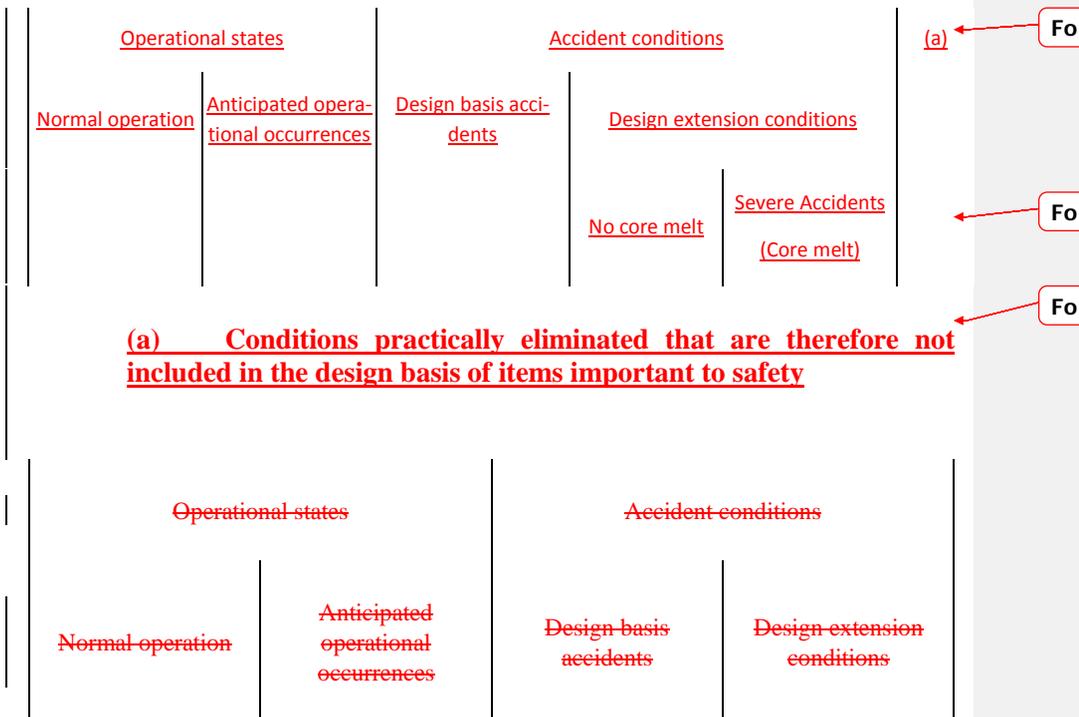
DEFINITIONS

The following definitions differ from those in the IAEA Safety Glossary (2007 Edition).

controlled state

Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.

plant states (considered in design)



accident conditions

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

design basis accident

An accident causing accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.

~~*{beyond design basis accident}*~~

~~This term is superseded by **design extension conditions**.~~

design extension conditions

Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

safe state

Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

safety feature for design extension conditions

Item designed to perform a safety function 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 the Slovak Republic, Slovakia
Aza, Z.M.	Atomic Energy Agency Organization of Iran, Islamic Republic of Iran
Borysova, I.	World Nuclear Association
Buttery, N.	British Energy Generation Ltd, United Kingdom
Carlucc, B.	AREVA, France
Cowley, J.S.	Consultant, United Kingdom
Downing, D.J.	Pebble Bed Modular Reactor, South Africa
El-Shanawany, M.	International Atomic Energy Agency
Englebert, B.	Suez-Tractebel, Belgium
Evrard, J.M.	Institut de radioprotection et de sûreté nucléaire, France
Fiorini, G.L.	Commissariat à l'énergie atomique, France
Froehmel, T.	World Nuclear Association
Gasparini, M.	International Atomic Energy Agency
Ghadge, S.G.	Nuclear Power Corporation of India Ltd, India
Harwood, C.	Canadian Nuclear Safety Commission, Canada
Järvinen, M.L.	Radiation and Nuclear Safety Authority, Finland
Kajimoto, M.	Japan Nuclear Energy Safety Organization, Japan
Kurkowski, L.	EDF-SEPTEN, France

Le Cann, G.	Federal Authority for Nuclear Regulation, United Arab Emirates
Matsumoto, T.	Japan Nuclear Energy Safety Organization, Japan
Mertins, M.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Germany
Ohshima, T.	Nuclear and Industrial Safety Agency, Japan
Pabarcus, R.	Lithuanian Energy Institute, Lithuania
Perez, J.R.	Autorité de sûreté nucléaire, France
Semenas, R.	State Nuclear Power Safety Inspectorate, Lithuania
Thadani, A.	Nuclear Regulatory Commission, United States of America
Toth, C.	International Atomic Energy Agency
Tronea, M.	National Commission for Nuclear Activities Control, Romania
Uhrik, P.	Nuclear Regulatory Authority of the Slovak Republic, Slovakia
Valtonen, K.	Radiation and Nuclear Safety Authority, Finland
Vaughan, G.J.	Nuclear Installations Inspectorate, United Kingdom
Wassilew, C.	Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, Germany
Yashimura, K.	Secretariat of the Nuclear Safety Commission, Japan
Zaiss, W.	FORATOM, Belgium
Zemdegs, R.	Atomic Energy of Canada Ltd, Canada
Ziakova, M.	Nuclear Regulatory Authority of the Slovak Republic, Slovakia

D. Delattre International Atomic Energy Agency

P. Hughes International Atomic Energy Agency

B. Poulat International Atomic Energy Agency

M. Gasparini International Atomic Energy Agency

Participants at the NUSSC Working Group meeting held from 5 to 8 March 2013