GIF/VHTR-SDC/2023/001

GEN IV International Forum

Expertise | Collaboration | Excellence

SAFETY DESIGN CRITERIA FOR GENERATION IV VERY HIGH TEMPERATURE REACTOR SYSTEM

June 2023

DISCLAIMER

This report focuses on Safety Design Criteria (SDC) for Generation IV Very High Temperature Reactor (VHTR) System. Neither GIF nor any of its members, nor any GIF member‘s national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member’s national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member’s national government.

Executive Summary

The Generation-IV International Forum (GIF) has been developing Safety Design Criteria (SDC) for specific Gen-IV systems. To date, the SDC are completed for SFR, LFR and GFR systems. This report focuses on SDC for VHTR system with the objective of establishing reference requirements for the safety design of VHTR structures, systems, and components consistent with the GIF safety goals and basis for safety approach.

Chapter 1 provides a background and introduces the objectives and SDC formulation principles. Chapter 2 outlines GIF safety goals and basic safety approach, introduces the fundamentals of VHTR safety approach, and discusses unique VHTR features that require specific revisions. In Chapter 3, eighty-five criteria for the overall safety design and specific structure, system and component design are described in the same structure of IAEA SSR 2/1, "Safety of Nuclear Power Plants: Design Specific Safety Requirements" on which the GIF SDCs for specific Gen-IV systems are based. The differences between the IAEA SSR 2/1 requirements and the VHTR-specific criteria are also captured in Appendix A with a side-by-side comparison of the original and revised requirements as well as the markups. The rationale for major revisions and deviations from the original IAEA SSR 2/1 requirements are captured in Chapter 2. A glossary covering specific terminology for the generation-IV systems in general, and VHTR system in particular, is also included. Several important terms, as defined in the IAEA safety glossary, are also incorporated in the glossary for convenience.

The potential users of this report are expected to be the VHTR concept developers as well as international and national regulatory organizations. Due to similarities of VHTR systems with the modular HTGR concepts currently being pursued world-wide, we envision its use by the modular HTGR designers as well.

Table of contents

1. INTRODUCTION

1.1 BACKGROUND AND OBJECTIVES

Nuclear power plants must ensure the highest level of safety that can reasonably be achieved to protect the workers, the public, and the environment from the harmful effects of ionizing radiation. The Generation-IV International Forum (GIF) was established in 2000 to coordinate the R&D of six specific nuclear systems to further their potential in meeting the demands for enhanced safety and reliability, economy, resource utilization, and security.[1] The high-level safety and reliability goals for the generation-IV nuclear energy systems were established in the original and updated versions of the "GIF Technology Roadmap".[2,3] It is recognized that the domestic codes and standards will be the reference for detailed design of structures, systems and components important to safety. However, there is a gap between the high-level GIF safety goals and the country-specific codes and standards, as illustrated in Figure 1.

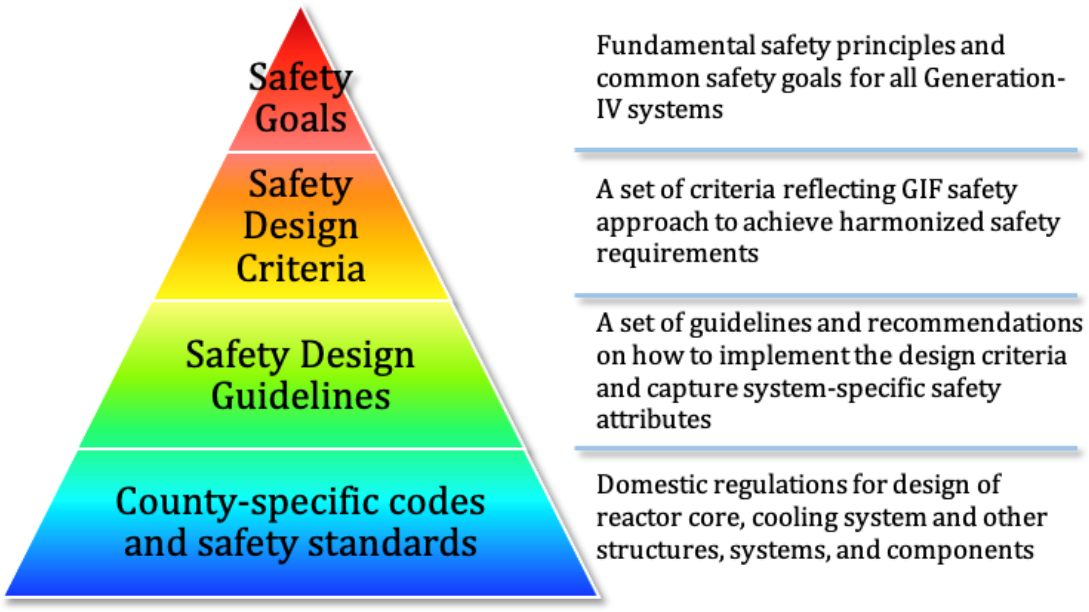

Figure 1. Hierarchy of Safety Standards.

Establishing Safety Design Criteria (SDC) and Safety Design Guidelines (SDG) to fill this gap for specific generation-IV reactor systems is an ongoing process in collaboration between the GIF System Steering Committees and Risk and Safety Working Group. The SDC development process involves revisions of IAEA SSR 2/1, "Safety of Nuclear Power Plants: Design Specific Safety Requirements"[4] for specific generation-IV design tracks. As most of the IAEA safety standards and fundamentals are originally established for the water-cooled reactor systems, the requirements in IAEA SSR 2/1 are being revised to reflect unique safety characteristics, attributes, and features of the generation-IV systems.

The effort also involves assuring the consistency of the system specific SDC with the following GIF safety and reliability goals:

- Generation-IV nuclear energy systems operations will excel in safety and reliability.
- Generation-IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.
- Generation-IV nuclear energy systems will eliminate the need for offsite emergency response.

Since its inception, the GIF focused on defining the attributes that are most likely to help meet these goals and identifying methodological advances needed to achieve them. In 2008, and later in 2021, the Risk and Safety Working Group established the "basis for safety approach" that identifies technology-neutral methods and tools to meet the GIF safety and reliability goals for all generation-IV reactor systems in support of their design and assessment processes.[5, 6] The SDC and SDG development efforts build on these previous work to reflect the fundamental GIF safety approaches and achieve the safety potential of the specific generation-IV systems.

The objective of this report is to establish design requirements for the structures, systems, and components of a VHTR plant to assure its safe operation and prevention of events, as well as for procedures and organizational processes that are required for mitigating the consequences of such events should they occur.

1.2 PRINCIPLES OF SDC FORMULATION

As a consensus document generated primarily by the GIF R&D community of designers and regulators, VHTR SDC are intended to provide minimum requirements for design, fabrication, construction, testing, and performance of structures, systems, and components that are important to safety. It is, however, recognized that the actual VHTR design is the choice of the developers, and it is not the intent of this SDC to enforce specific prescriptive design provisions.

The SDC serve as the fundamental requirements for design and review of SSCs that make up a nuclear plant particularly when assessing the performance of their intended safety functions during operational states and accident conditions. Attention is given to the consistency with GIF safety goals/approaches, and the requirements providing performance targets are described in greater depth. The bases of VHTR-specific revisions, additions, and deletions, including the rationale and background, are further clarified in Chapter 2.

The IAEA SSR 2/1 [4] requirements were established for third generation LWR systems with participation of nuclear regulatory authorities and support organizations. When establishing safety design criteria for the GIF VHTR systems, IAEA SSR 2/1 is considered as the reference document in terms of its structure and comprehensive formulation, basic approach towards safety, as well as terms and definitions. The VHTR SDC maintains the basic structure of IAEA SSR 2/1 and its original text is retained unless a revision is warranted. The safety-related terms for the SDC are basically the same as the ones defined in the IAEA Safety Glossary [7], and new definitions are added as needed for terms specific to the GIF VHTR systems.

2. GIF SAFETY APPROACH AND VHTR SAFETY ATTRIBUTES

2.1 GIF SAFETY APPROACH

The GIF "basis for safety approach" [6] outlines the main safety principles (such as Defense in Depth), summarizes the basic approaches for design and assessments (such as the risk-informed approach), and introduces the safety assessment methods and tools (Integrated Safety Assessment Methodology). The definitions of defense in depth and plant states follow those in IAEA SSR 2/1 with a major exception that the category for "Design Extension Conditions with Core Melting" does not apply to VHTR systems. Therefore, the plant states considered in design and their alignment with the levels of Defense in Depth for VHTR systems are simplified as shown in Table 1.

Table 1. Defense in Depth levels and Plant States for VHTR Systems.

Defence in Depth Levels				
Level 1	Level 2	Level 3	Level 4	Level 5
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions	Off-site emergency response
Plant states considered in design				

The plant states considered in the design are the operational states that include normal operation and anticipated operational occurrences, and the accident conditions that include design basis accidents and design extension conditions. The GIF goal for generation-IV systems to excel in safety and reliability is applicable to the defense in depth levels 1 and 2 (operational states). The GIF goal for Gen-IV systems to have a very low likelihood and degree of reactor core damage is applicable to levels 3 and 4 (accident conditions). This is achieved by reducing the frequency of initiating events, employing preventive design features for controlling the progression of an accident in response to initiating events, and mitigating the consequences to avoid a severe plant condition.

Focus is given to safety-by-design for accident prevention in the levels 1 and 2, prevention of severe plant conditions in level 3, and mitigation of potential severe plant conditions via reliable safety features along with accident management strategies to improve the safety in level 4. The GIF goal for Gen-IV systems to eliminate the need for off-site emergency response is applicable to level 5 of defense in depth, requiring not only effective accident management strategies to limit the consequences, but also consideration of measures for practical elimination of event sequences that could potentially lead to large releases.

2.2 VHTR SAFETY PRINCIPLES

The VHTR safety principles covering design, construction, commissioning, operation, and decommissioning are generally like those for other generation-IV systems. However, there are some notable differences in the safety philosophy between the VHTR and other systems. The VHTR concepts considered within GIF rely on the intrinsic safety characteristics such as low power density, a large heat capacity of ceramic core internals, strongly negative temperature coefficient of reactivity, large height-to-diameter ratio of the reactor core to promote passive heat removal, and coated fuel particles that act as the primary barrier to radionuclide release. This combination of attributes allows the VHTR systems to control the reactivity inherently and reject decay heat passively at a rate sufficient to avoid a severe core damage.

The events considered for the safety design include the external hazards and internal events resulting from human errors or plant component failures. For internal events, anticipated operational occurrences, design basis accidents and design extension conditions are to be identified and measures for each of event sequence are to be built into the design. For external hazards, design conditions are to be established in accordance with site conditions to protect safety functions with margins.

The VHTR SDC follows the defense in depth philosophy as the most fundamental safety approach by requiring design measures for every plant state, i.e., normal operation, anticipated operational occurrences, design basis accidents, and design extension conditions. Consideration is given to the independence and effective performance of balanced design measures at each defense in depth level so that a specific event sequence cannot pose the dominant risk. The design for operational states and design basis accidents are required to be conservative with due account of uncertainties of design conditions and transient phenomena. For design extension conditions, the safety design process to prevent large releases to the environment are allowed to be based on best-estimate analysis.

For normal operation, anticipated operational occurrences, and design basis accidents, the VHTR design should ensure that the fuel integrity is maintained, reactor can be reliably shutdown as needed, the decay heat can be removed to an ultimate heat sink, and the radioactive materials are confined. As for other reactor types, these goals are expected to be achieved with high system reliability via improvements based on operational experience, enhancement of safety margins through the introduction of new technologies, and effective inspection program capable of detecting conditions that could lead to, or cause propagation of, failures.

Safety for design extension conditions is attained by providing measures for preventing severe plant conditions and managing consequences to enhance the robustness of the system, with due consideration of the potential for common cause failures. Application of passive design measures is also desired for design extension conditions so that an unexpected event sequence progresses slow enough to allow time for systems to respond and the operators to take appropriate actions needed to mitigate the consequences. The IAEA SSR

2/1 Requirement 20 is revised to reflect the unique safety attributes of the VHTR systems for design extension conditions.

The appropriate management of radioactive materials and measures to accommodate abnormal events must be provided not just for the reactor core, but also for fuel handling, storage and radioactive waste management systems also considering their potential mutual interaction and interdependence as reflected in Requirement 80 in Chapter 3.

2.3 VHTR SAFETY DESIGN FEATURES THAT REQUIRE SDC REVISIONS

The target systems for establishing the SDC are the VHTR design tracks considered in the System Research Plan [8]. Like the earlier HTGRs, VHTR designs utilize graphite as moderator, helium as coolant, core structures that able to tolerate high temperatures under operational states and accident conditions, and the coated fuel particles as the primary barriers to fission product release. The coated fuel particles are typically dispersed in a graphite or some other carbide matrix and formed into spherical fuel elements for a pebble bed reactor, or cylindrical compacts for a prismatic block type reactor. The reactor is operated in a thermal neutron spectrum under the conditions of low power density but at high temperature.

Reactivity control

Since helium does not absorb neutrons, loss of helium does not introduce positive reactivity and the reactivity feedback at elevated temperatures is dominated by the Doppler feedback. Due to the resulting strongly negative temperature coefficient of reactivity, one of the protective actions considered in VHTR designs is to trip the helium circulator to make the reactor subcritical as the core temperature rises above normal. This brings the reactor to a safe and stable low power state even when all station power is lost, the primary coolant system is depressurized, and the control rods fail to insert.

Other independent reactivity control systems are also included to assure that increased core temperatures do not challenge the integrity of fuel, graphite core structures, or metallic alloys used in helium pressure boundary and other components (Requirements 4, 45 and 46 in Chapter 3). In pebble bed reactors, online refueling allows operation with minimal excess reactivity, and the control-rod or absorber-pebble systems are independently activated as needed. For prismatic reactors, burnable poison in the fuel reduces the excess reactivity, and separate control rod systems are used for short term reactivity control and safe shutdown. The shutdown system is designed with adequate reactivity margin and its reliability is assured by monitoring, testing, and maintenance throughout the lifetime of the plant.

The design of these reactivity control systems should address control rod ejection and inadvertent and uncontrolled rod withdrawal concerns. But the consequences of potential rapid control rod ejection or withdrawal are typically still evaluated to demonstrate that the negative temperature feedback is strong enough to prevent significant power excursions and the core safety limits are not challenged. Similarly, seismic disruption of the core must be assessed and shown not to result in excessive fuel temperatures due to core compaction in

pebble bed reactors. Mechanical design of the control rod channels should address the concern for the motion of the surrounding reflector blocks preventing rod insertion.

In case the control elements are not inserted, the core would eventually become re-critical as the core temperature and xenon concentration decrease. Therefore, the design should assure that:

- re-criticality may occur only after considerable time (measured in days) to facilitate operator actions,
- the resulting long-term oscillations in the core power (due to changes in fuel temperature and xenon concentration) are low in magnitude,
- the stable low-power end-state (when the rate of heat production equals to the rate of heat rejection) is a fraction of the nominal power, and
- the core temperature remains well below the limit at which significant quantities of radionuclides could be released from the fuel.

Air and Water Ingress

The helium coolant is not considered critical for plant safety; therefore, in a circulator trip or a severe fault condition that results in a loss of convective cooling, the design should demonstrate that the heat can be safely removed by conduction and radiation. In the event of an unplanned depressurization of the primary system, however, air can enter the core through breaks in pipes and other primary system components as can be expected at some point in the life of the plant.

Nuclear grade graphite does not burn but can oxidize at temperatures above 400°C if oxygen is available continuously and in sufficient concentration. In smaller quantities, the oxygen is consumed by the graphite closest to the location of a break. A continuous leak of oxygen into the primary loop may result in oxidation of graphite structures and generation of volatile combustible compounds such as carbon monoxide at high temperatures. Therefore, VHTRs should be designed to prevent rapid and large amounts of air and water from entering the primary loop, and the reactor building should be designed to take advantage of the density difference between air and helium to minimize the air concentration near the potential break locations (Requirements 47 and 54).

For plants driving a steam-based power conversion system, a rupture of a steam generator tube may result in water/steam entering the core. The additional moderating effect of the water in the core should be accounted for in the core design so that the corresponding increase reactivity is limited. Another risk associated with a steam generator tube rupture is that the water/steam can ‘wash off’ radiological species previously trapped near the surface of the graphite elements, adding to the circulating activity. Therefore, provisions to provide for timely isolation of the tube rupture and limit the water/steam ingress (via consideration of passive pressure relief valves and draining of the steam in the secondary side) are also required in the design (Requirement 53A).

Core heat removal

The reactor core is cooled by convective transport of heat via helium to the steam generator (or intermediate heat exchanger) during operational states (normal operation and anticipated operational occurrences). However, the high-pressure helium does not provide coolant function for decay heat removal. If forced cooling is lost, decay heat is transferred naturally via conduction and radiation from the core, through the outer reflector and reactor pressure vessel, and on to atmosphere as the ultimate heat sink. The Vessel Cooling System (VCS) is designed mainly for the protection of the vessel and the surrounding concrete. It absorbs heat from the pressure vessel outer surface and carry it via natural circulation of air or water to external cooling panels, preventing the vessel from exceeding its designed temperature limit. These characteristics of core heat removal are captured in Requirement 53. The helium injection systems are not needed and the VHTR designs are not required to accommodate a loss of helium event as reflected in removal of Requirement 52.

In the event of VCS failure (as assumed in some design extension conditions), the reactor building, surrounding structures and soil become the alternative ultimate heat sink. In such a case, the design should demonstrate that, even though it may sustain some damage, the pressure vessel and surrounding concrete structures will largely maintain their structural integrity, as reflected in Requirement 53.

Since a core melt accident cannot happen even for such extreme cases, the IAEA SSR 2/1 Requirements 7, 13, 20, 44, 45, and 68 are modified to exclude phenomena related to core melt scenarios, degradation of the reactor core, or severe accidents from the language without impacting the safety intent of these requirements. Although massive fuel failure is not expected in a VHTR even when the VCS malfunctions, the higher fuel temperatures in the core after a depressurized loss of forced cooling event may drive sufficient release of fission products from some parts of the core such that, if not captured by the filters, dose limits to workers and at the site boundary may be challenged. The emergency planning should consider this likelihood, taking advantage of the long grace period during which mitigating actions can take place.

Confinement of radioactive materials

The coated fuel particles and graphite matrix play an important role to fulfill the confinement function as the primary barriers to fission product release. The fuel coatings effectively retain the bulk of the radionuclide inventory under operational states and accident conditions. The GIF VHTR systems are expected to operate under more demanding conditions than the HTGR concepts with expected peak coolant outlet temperature higher than 1000°C. Therefore, maintaining the integrity of these unique fuel forms to retain fission products at burnup and temperatures that can be expected during operational states and accident conditions is an important requirement to assure that the coated fuel particles retain their structural integrity under such conditions as well as accidental mechanical loads and chemical attack (Requirements 43 and 44).

Other barriers preventing fission product release include the graphite matrix, the reactor coolant (helium) pressure boundary, and the vented low-pressure reactor building. Although the coated fuel particles are highly effective as the primary barriers, a slow rate of diffusion of certain species (e.g., cesium and silver) can be expected even at normal operating temperatures. Also considering the potential fabrication defects, it should be demonstrated that the small amounts of species released from fuel during operational states do not pose a radiological concern. Therefore, a dedicated helium purification system is required to keep the circulating activity at levels as low as reasonably achievable (Requirement 50).

A large break induced rapid depressurization, with or without failure of the decay heat removal system, is commonly considered as the bounding event that will likely lead to elevated release of fission product inventory. Blowdown of the primary loop releases the circulating inventory into the reactor building and most of it is released to the atmosphere by venting the building. If the circulating inventory is low enough, the site boundary release levels are expected to remain below actionable levels following a blowdown event.

Following the blowdown phase, the vents in the reactor building can be closed, and filtering of the building atmosphere can resume during the subsequent heat-up and cool-down phases. Due to the elevated temperatures attained in the heat-up phase, fission products are driven out of the fuel graphite at a greater rate. The diffusion of species increases as temperatures exceed a time-at-temperature limit; therefore, the design should demonstrate effectiveness of the fuel up to this limit. Duration of the transients is also an important factor due to the "time-at-temperature" aspect of fuel performance. If the core temperature exceeds the limit for extended periods of time, significant radionuclide release can be expected, especially for high burnup fuel.

Since multi-layer coated fuel particles, graphite matrix, reactor coolant pressure boundary and the reactor building all serve as multiple barriers against the release of fission products to collectively achieve the confinement function, a conventional leak-tight containment structure is not a requirement for VHTR systems. Consequently, the IAEA SSR 2/1 Requirement 54 is repurposed to capture the criteria for the reactor building, and Requirements 55-58 are considered 'not applicable'. The Requirements 20, 30, 47, 59 and 81 are also modified accordingly to capture the required collective 'confinement function'.

Other VHTR design features

Other unique VHTR design features that require attention include development and qualification of high temperature materials such as graphite and metallic alloys at high temperatures (Requirements 9, 23, 30, 44, 47 and 48), safety of multi-module plants (the new Requirements 33A and 83), and coupling of the reactor and the process heat applications including hydrogen production (Requirement 35).

3. VHTR SAFETY DESIGN CRITERIA

The structure of this chapter is consistent with the IAEA SSR 2/1, "Safety of Nuclear Power Plants: Design Specific Safety Requirements". [4] When some requirements and specific paragraphs are removed, or three new requirements are added, the original numbering system of Ref 4 is retained for easy tracking and comparison with Ref 4. The VHTR specific additions in revised requirements are italicized. Appendix A also provides a side-by-side comparison of the original IAEA SSR 2/1 and revised VHTR requirements with the specific differences captured in the last column as markups.

MANAGEMENT OF SAFETY IN DESIGN

No change

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 organization, 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.

No change

Requirement 2: Management system 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.

No change

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.

PRINCIPAL TECHNICAL REQUIREMENTS

No change

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.

No change

Requirement 5: Radiation protection in design

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 to a large radioactive release have been 'practically eliminated', and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.

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

No change

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 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 is 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 effect;

(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.

4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions shall as far as is practicable be independent of safety systems.

No change

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 power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

No change

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.

No change

Requirement 10: Safety assessment

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 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.

No change

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.

No change

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 management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) 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.

GENERAL PLANT DESIGN

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.

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.

No change

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.

No change

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.

No change

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.

No change

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 in designing the layout of the plant and in determining 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, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards.

5.15B. For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

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 hazards

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. Causation and likelihood shall be considered in postulating potential 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 firefighting 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. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A.

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. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A.

5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects.

5.21A. The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site.

5.22. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15B.

No change

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.

No change

Requirement 19: Design basis accidents

A set of accidents 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 consequences, on or off the site, and do not necessitate any off-site protective actions.

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.

5.27. An analysis of design extension conditions for the plant shall be performed. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as 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 mitigate the consequences of *severe plant conditions*, or to maintain the *confinement funct*ion. 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. The plant shall be designed so that it can be brought into a controlled state and the *confinement* function can be maintained, with the result that the possibility of plant states arising that could lead to a large radioactive release is 'practically eliminated'. The effectiveness of provisions to ensure the *confinement function* could be analysed on the basis of the best estimate approach.

5.28. The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing *severe plant conditions* from arising, or, if they do arise, 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 capable of 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, where appropriate;
(c) Shall have reliability commensurate with the function that they are required to fulfil.

5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release *requiring off-site protective actions* or a large radioactive release is 'practically eliminated'.

5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such 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.

No change

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.

No change

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.

No change

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.

No change

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.

No change

Requirement 25: Single failure criterion

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

5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion 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.

No change

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.

No change

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.

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:

(a) Safety limits;

(b) Limiting settings for safety systems;

(c) Limits and conditions for normal operation;

(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.

GENERAL PLANT DESIGN: Design for Safe Operation Over the Lifetime of the Plant

No change

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 external event, either by test or 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 shall be included in the qualification programme.

No change

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 to identify unanticipated behaviour of the plant or degradation that might occur in service.

GENERAL PLANT DESIGN: Human Factors

No change

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 likelihood and the effects of operating errors on safety. The design process shall give due consideration 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 all plant states.

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 decisions 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.

GENERAL PLANT DESIGN: Other Design Considerations

Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant

No change

Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.

5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.

Requirement 33A: Safety systems, and safety features for design extension conditions, of modules of a multi-module unit

Each module of a multi-module unit shall have its own safety systems and shall have its own safety features for design extension conditions, as far as practicable. Where a safety system or a safety feature for design extension conditions is shared between reactor modules of a multi-module unit, the shared safety system or safety feature shall be functionally capable of fulfilling the safety requirements of each of these modules, to protect against the consequences of events which have the potential to affect multiple modules.

5.63A. To further enhance safety, means allowing interconnections between modules of a multi-module unit shall be considered in the design.

No change

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 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 *process heat, hydrogen production*, district heating or water desalination) shall be designed to *limit the* transport *of* radionuclides from the nuclear plant to *heat utilization units to ensure that defined regulatory limits are not exceeded* under conditions of operational states and in accident conditions.

5.63B. The design of the nuclear power plant shall take account of the potential impact of abnormal events in coupled facilities on the safety of nuclear power plant by providing adequate physical separation.

No change

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. 34

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.

No change

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.

No change

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.

No change

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.

No change

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.

No change

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.

GENERAL PLANT DESIGN: 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. 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 and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases.

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 acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;
(e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by *inherent safety features and* 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 inherent safety features and* 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 situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;

(c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.

DESIGN OF SPECIFIC PLANT SYSTEMS: Reactor Core and Associated Features

Requirement 43: Performance of *particle based* fuel elements

The coated particles **for the nuclear power plant shall be designed to maintain their structural integrity,** ***maintain their confinement performance*****, 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** ***and accident conditions. The fuel elements that contain the fuel particles shall be designed to maintain their structural integrity in the operational states, and to prevent unacceptable loads to the coated fuel particles in accident conditions*****.**

6.1. The processes of deterioration to be considered shall include those arising from:

— *Thermal effect*;
— Internal pressure due to fission products and *other gasses* in *coated* fuel *particles*;
— *Kernel migration in coated fuel particle due to temperature gradient*;
— *Chemical attack of coating layers of coated fuel particle by metallic fission products*;
— Irradiation of fuel *particles* and other materials in the fuel *elements*;
— *Abrasion (for pebble bed design)*;
— *Coolant* chemical effects;
— Static and dynamic loading.

Allowance shall be made for uncertainties in data, in calculations and in manufacture.

6.2. Fuel design limits shall *account for (i) key manufacturing parameters, coated fuel particles defect fraction, heavy metal contamination, and (ii) during operations irradiation time and temperature leading to a specified acceptable radionuclide release*.

6.2A Fuel shall be designed for acceptable radionuclide retention during accidents based on the spatial and time distribution of fuel temperature leading to a specified acceptable radionuclide release.

6.2B Fuel shall be designed to take chemical attack in all states into account.

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

Requirement 44: Structural capability of the reactor core

The *reactor core, including* fuel elements, *reflectors*, and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions, *unacceptable loads to the coated fuel particles are prevented, adequate core cooling can be achieved and maintained, and the core temperature remains within acceptable limits. The reactor core and supporting structures shall also be designed so that, in all plant states, a geometry to allow reactor shutdown (adequate for control of core heat generation) and sufficient heat removal (to the surrounding structures and environment, as necessary) can be maintained*.

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, 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 *and controlling* the neutron flux distributions in the reactor core and their changes shall be provided *as necessary* 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 shall be limited or compensated for 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 *design provisions* for shutting down the reactor shall consist of at least two diverse and independent *means*.

6.10. *At least one of* the two different shutdown *means* 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. *At least one of* 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.

DESIGN OF SPECIFIC PLANT SYSTEMS: 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 loss of *helium (coolant)* and to prevent the *rapid ingress of air or water*.

6.13A. The coolant pressure boundary shall form one of the layers of protection of the release of radionuclides from the fuel during operational states and accident conditions.

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 *circulator or turbine* 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 *an unacceptable* release of radioactive material from the nuclear power plant directly to the environment.

No change

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 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 *of the chemical impurities in the primary coolant, and shall ensure that the level of circuit activity* is as low as reasonably practicable.

No change

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 53: Heat transfer to an ultimate heat sink

The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

6.19A. *Means* for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. *Residual heat removal to the reactor pressure vessel is achieved by conduction, convection and radiation independent of the primary heat transfer system and helium pressurization. A highly reliable capability to transfer heat from the reactor pressure vessel wall to an ultimate heat sink shall be ensured and may be either completely passive or have both an active and a passive mode. For design extension conditions, residual heat removal* may require the use of a different ultimate heat sink *(such as buildings and surrounding structures)* or different access to the ultimate heat sink.

6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

Requirement 53A: Design of secondary coolant systems to limit water ingress

The secondary coolant systems using water and/or steam shall be designed with provision to limit the water ingress into the primary helium system, so as not to exceed specified design limits of the reactor core and coolant pressure boundary.

DESIGN OF SPECIFIC PLANT SYSTEMS: Containment Structure and Containment System

Requirement 54: *Reactor building*

A structure *(building, or part of a building)* shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) control and limit release of radioactive substances 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.

6.19C.The design of the structure shall provide for sufficient pathways for the release of reactor coolant from the structure in the event of depressurization or severe water ingress accidents. The cross-sections of openings 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 structure or systems that are important for the main safety functions in accident conditions.

6.19D. A structure (building or part of it) shall provide for controlled release of radioactive substances in operational states and in design basis accident conditions, and contribute to limit release in DECs (or BDBE covering Option B in requirement 13). Insofar, this structure combined with other supporting systems, e.g. ventilation systems, is a barrier for the retention of radioactive materials.

6.19E Design features to limit the availability of air for possible rapid ingress into the reactor core in the event of a break in the reactor coolant pressure boundary shall be provided as necessary.

Requirement 55: Control of radioactive releases from the *reactor building*

The design of the *reactor building* shall be such as to ensure that any radioactive release 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 structure*s and the supporting systems contributing to confinement function of the reactor building* shall be designed and constructed so that the *release* rate can be tested *at conditions representative of the credited confinement function during a postulated accident*.

DESIGN OF SPECIFIC PLANT SYSTEMS: 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 *reactor building* 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 releases and the amounts of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.

No change

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.

No change

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 shall 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.

No change

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 the 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.

No change

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.

No change

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.

No change

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, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases 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 of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

No change

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.

No change

Requirement 67: Emergency response facilities on the site

The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.

6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

DESIGN OF SPECIFIC PLANT SYSTEMS: Emergency Power Supply

Requirement 68: Design for withstanding the loss of off-site power

The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.

6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity.

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.

6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.

6.44B. Equipment that is necessary to mitigate the consequences of *design extension conditions* shall be capable of being supplied by any of the available power sources.

6.44C. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery.

6.44D. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources.

6.45. The design basis for any diesel engine or other prime mover 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.

6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.

DESIGN OF SPECIFIC PLANT SYSTEMS: Supporting Systems and Auxiliary Systems

No change

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.

No change

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.

No change

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.

No change

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.

No change

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 gaseous radioactive releases 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.

No change

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.

No change

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.

No change

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.

Requirement 77: Power Conversion Systems

The design of the power conversion systems 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. In a steam/water cycle, the design of the steam supply system *and the feedwater system* shall provide for appropriately rated and qualified steam*/water* isolation valves capable of closing under the specified conditions in operational states and in 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.

DESIGN OF SPECIFIC PLANT SYSTEMS: Treatment of Radioactive Effluents and Radioactive Waste

No change

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.

No change

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 liquid radioactive releases 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.

DESIGN OF SPECIFIC PLANT SYSTEMS: 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 *elements*, *as necessary*;
(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 avoid causing unacceptable handling stresses on fuel elements;
(d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel;
(e) To permit safe keeping of suspect or damaged fuel elements;
(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 shall be such as to prevent the uncovering of fuel *elements* in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design of the plant:

(a) Shall provide the necessary fuel cooling capabilities;

(b) Shall provide features to prevent the uncovering of fuel *elements* in the event of a leak or a pipe break;

(c) Shall provide a capability to restore the water inventory.

The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.

6.68bis. For reactors using an air-cooling system for fuel storage, the design of the plant:

(a) Shall provide the necessary fuel cooling capabilities;

(b) Shall provide features to ensure adequate cooling of fuel elements in the event of air-cooling system malfunctions.

The design shall also include features to provide shielding against radiation and necessary capability for confinement of radioactive material for dry cask.

6.68A. The design *for reactors using a water pool system for fuel storage* shall include the following:

(a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;

(b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;

(c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;

(d) Means for monitoring and controlling the water chemistry for operational states.

6.68B. For reactors using an air-cooling system for fuel storage, the design shall be such as to provide adequate cooling of fuel elements in all plant states of relevance for the spent fuel storage, so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design for reactors using an air cooling system for fuel storage shall include the following:

(a) Means for monitoring and controlling the air temperature for operational states and for accident conditions that are of relevance for the spent fuel storage;

(b) Means for monitoring and controlling the activity in air for operational states and means for monitoring the activity in air for accident conditions that are of relevance for the spent fuel storage.

DESIGN OF SPECIFIC PLANT SYSTEMS: 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, the integrity of the *coated* fuel *particles* 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.

No change

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 actions 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, and 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.

ADDITIONAL CONSIDERATIONS FOR MULTI-MODULE UNITS

Requirement 83: Multi-module units

For multi-module units, the design shall take due account of the potential for specific hazards impacting several modules simultaneously, and the potential for hazards initiating at one module impacting other reactor modules of the same unit. The potential for harmful interactions of systems important to safety that might be required to operate simultaneously in multi-module units shall be evaluated, and effects of any harmful interactions shall be prevented. The scope of the safety analysis shall consider events with impact on multiple reactor modules in a unit and multiple units on a site.

6.85. Interconnections among the reactor modules: For purposes such as operation and accident management, multi-module units might include interconnections between reactor modules. In this case, specific considerations are necessary to ensure that such interconnections will not be detrimental to the safety of each reactor module and of the overall plant.

6.86. Control and protection systems: The control and protection systems of each module and the entire plant must ensure that a clear actuation logic is reliably implemented so that an initiating event or accident occurring within one reactor module will not propagate to accident conditions in other reactor modules, and that the reactor modules will not have detrimental effects on each other under accident conditions.

6.87. Human factors engineering: The design of control room shall consider the interactions of different reactor modules providing that these modules share a common control room. This covers aspects relating to the main control room, supplementary control and other emergency response facilities and locations; maintenance of the multiple modules; potential remote control of the main control room; one operator managing several modules; more than one module supplying the same turbine.

6.88. Emergency preparedness and response: This includes aspects relating to the design of multi-module units to enable the emergency response under all relevant conditions.

6.89. Capacity for the addition of future modules, plant lay-out and construction: Some design schemes consider a plant layout which allows a consecutive and serialized construction of the reactor modules. This new practice should involve additional important safety considerations. Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in specifications or capability might result in the addition of new equipment which could, for example, increase the load on heating, ventilating and air conditioning systems. Therefore, consideration might need to be given to including margins in the design capability of relevant support systems to allow for the potential addition of new equipment later.

REFERENCES

[1] Generation-IV International Forum: https://www.gen-4.org/ .

[2] A Technology Roadmap for Generation-IV Nuclear Energy Systems, https://www.gen-4.org/gif/jcms/c_40481/technology-roadmap, GIF-002-00 (2002)

[3] Technology Roadmap Update for Generation IV Nuclear Energy Systems, https://www.gen-4.org/gif/jcms/c_60729/technology-roadmap-update-2013, (2014).

[4] IAEA, 'Safety of Nuclear Power Plants: Design', SSR-2/1, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1715web-46541668.pdf, (2012).

[5] Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems (Revision 1), https://www.gen-4.org/gif/jcms/c_66624/basis-for-the-safety-approach-for-design-assessment-of-generation-iv-nuclear-systems-revision-1-2008, GIF/RSWG/2007/002 (2008).

[6] Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems (Revision 2), https://www.gen-4.org/gif/jcms/c_178828/bsa-update-v4-clean, (2021).

[7] IAEA Safety Glossary, http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf, (2018).

[8] GIF Very High Temperature Reactor (VHTR) System Safety Assessment, https://www.gen-4.org/gif/jcms/c_103659/gifvhtr-safety-assessment-finaldec2018, (2018).

GLOSSARY [7]

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

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

Confinement function: Prevention or control of releases of radioactive material to the environment in operation or in accidents.

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

Defence in depth: A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

Design basis accident: An accident causing 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.

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

Deterministic analysis: Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result.

Fuel: Fissionable nuclear material in the form of fabricated elements for loading into the reactor core of a civil nuclear power plant or research reactor.

Fuel element: Cylindrical compacts or pebble balls in which coated fuel particles are dispersed in a graphite or carbide matrix.

Grace period: The period of time during which a safety function is ensured in an event with no necessity for action by personnel.

Inherent safety: Fundamental property of a design concept that results from the basic choices in the materials used or in other aspects of the design which assures that a particular potential hazard cannot become a safety concern in any way.

Item (SSC) important to safety: An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. Items important to safety include:

- Those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- Those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions;
- Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.

Large release (of radioactive material): A release of radioactive material for which off-site protective actions that are limited in terms of times and areas of application are insufficient for protecting people and the environment.

Normal operation: Operation within specified operational limits and conditions.

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

Passive safety feature: A safety feature that does not depend on an external input such as actuation, mechanical movement or supply of power.

Passive safety system: A safety system that uses passive safety feature for its major parts.
A passive safety system for decay heat removal is operated by natural circulation of the coolant, or by conduction and radiation alone, and does not depend on safety system support features nor mechanical devices.

Plant states (considered in design): Operational states (normal operation and anticipated operational occurrences) as well as accident conditions (design basis accidents and design extension conditions).

Postulated initiating event: A postulated event identified in design as capable of leading to anticipated operational occurrences or accident conditions.

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

Probabilistic safety assessment: A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.

Reactor coolant pressure boundary: Helium pressure boundary.

Reactor coolant systems: The primary and secondary coolant systems.

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

Safety analysis: Evaluation of the potential hazards associated with the operation of a facility or the conduct of an activity. The formal safety analysis is part of the overall safety assessment; that is, it is part of the systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the activity) to ensure that all the relevant
safety requirements are met by the proposed (or actual) design.

Safety related item (SSC): An item important to safety that is not part of a safety system.

Safety system: A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states and non-safety functions in other operational states.

Safety feature for design extension conditions: Item designed to perform a safety function, or that has a safety function, for design extension conditions.

Safety system: A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states and non-safety functions in other operational states.

APPENDIX A: COMPARISON OF IAEA SSR 2/1 REQUIREMENTS WITH GIF REVISIONS FOR VHTRS

	IAEA SSR 2/1 (Rev 1)	GIF Revisions for VHTRs	Markups
MANAGEMENT OF SAFETY IN DESIGN			
1	**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 organization, 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.	*No change.*	*No change.*
2	**Requirement 2: Management system 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.	*No change.*	*No change.*

	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.		
3	**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	*No change.*	*No change.*

	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.		
PRINCIPAL TECHNICAL REQUIREMENTS			
4	**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.	*No change.*	*No change.*

5	**Requirement 5: Radiation protection in design** **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 to a large radioactive release have been 'practically eliminated', and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence. 4.4. Acceptable limits for purposes of radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.	*No change.*	*No change.*
6	**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 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	*No change.*	*No change.*

	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 is 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.		
7	**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	**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	**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 effect; (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;	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 effect; (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;	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 effect; (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. 4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.	(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. 4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions shall as far as is practicable be independent of safety systems.	(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. 4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions ~~(especially features for mitigating the consequences of accidents involving the melting of fuel)~~ shall as far as is practicable be independent of safety systems.
8	**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 power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.**	*No change.*	*No change.*
9	**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.	*No change.*	*No change.*

	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.		
10	**Requirement 10: Safety assessment** **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 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.	*No change.*	*No change.*
11	**Requirement 11: Provision for construction**	*No change.*	*No change.*

	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.		
12	**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 management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) 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.	*No change.*	*No change.*
GENERAL PLANT DESIGN: DESIGN BASIS			
13	**Requirement 13: Categories of plant states** **Plant states shall be identified and shall be grouped into a limited number of categories**	**Requirement 13: Categories of plant states** **Plant states shall be identified and shall be grouped into a limited number of categories**	**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 core melting. 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.	**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. 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.	**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 core melting~~. 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.
14	**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.	*No change.*	*No change.*
15	**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	*No change.*	*No change.*

	standards and codes, as well as with relevant regulatory requirements.		
16	**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	*No change.*	*No change.*

	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.		
17	**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 in designing the layout of the plant and in determining 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, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against	*No change.*	*No change.*

	common cause failure mechanisms generated by hazards. 5.15B. For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously. **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 hazards** 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. Causation and likelihood shall be considered in postulating potential 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 firefighting 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. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A. 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. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A. 5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. 5.21A. The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site. 5.22. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15B.		
18	**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.	*No change.*	*No change.*
19	**Requirement 19: Design basis accidents** **A set of accidents 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**	*No change.*	*No change.*

	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 consequences, on or off the site, and do not necessitate any off-site protective actions. 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.		
20	**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.**	**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.**	**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.**

	5.27. An analysis of design extension conditions for the plant shall be performed. 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 that are not considered design basis accident conditions, or 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 prevent, or to mitigate the consequences of, a severe accident, or 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 the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'. 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 specifications 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 capable of preventing or mitigating, events considered in the design extension conditions. These features:	5.27. An analysis of design extension conditions for the plant shall be performed. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as 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 mitigate the consequences of severe plant conditions, or to maintain the confinement function. 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. The plant shall be designed so that it can be brought into a controlled state and the confinement function can be maintained, with the result that the possibility of plant states arising that could lead to a large radioactive release is 'practically eliminated'. The effectiveness of provisions to ensure the confinement function could be analysed on the basis of the best estimate approach. 5.28. The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing severe plant conditions from arising, or, if they do arise, 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 capable of mitigating, events considered in the design extension conditions. These features:	5.27. An analysis of design extension conditions for the plant shall be performed. 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 that are not considered design basis accident conditions, or~~ 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 prevent, or~~ to mitigate the consequences of ~~a severe accident~~ severe plant conditions, or to maintain the ~~integrity of the containment~~ confinement function. 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~~ confinement function can be maintained, with the result that the possibility of plant states arising that could lead to ~~an early radioactive release or~~ a large radioactive release is 'practically eliminated'. The effectiveness of provisions to ensure the ~~functionality of the containment~~ confinement function could be analysed on the basis of the best estimate approach. 5.28. The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing ~~such~~ severe plant 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 capable 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 reliability commensurate with the function that they are required to fulfil. 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 by using engineering judgement and input from probabilistic safety assessments. 5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'. 5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such 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.	(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, where appropriate; (c) Shall have reliability commensurate with the function that they are required to fulfil. 5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release requiring off-site protective actions or a large radioactive release is 'practically eliminated'. 5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such 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	(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 reliability commensurate with the function that they are required to fulfil. ~~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 by using engineering judgement and input from probabilistic safety assessments.~~ 5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release requiring off-site protective actions or a large radioactive release is 'practically eliminated'. 5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such 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

		following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.	shall be considered to be part of the original postulated initiating event.
21	**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.	*No change.*	*No change.*
22	**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.	*No change.*	*No change.*

	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.		
23	**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.	*No change.*	*No change.*
24	**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.**	*No change.*	*No change.*
25	**Requirement 25: Single failure criterion** **The single failure criterion shall be applied to each safety group incorporated in the plant design.** 5.39. Spurious action shall be considered to be one mode of failure when applying the single failure criterion 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	*No change.*	*No change.*

	confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event.		
26	**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.	*No change.*	*No change.*
27	**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. 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.	*No change.*	*No change.*
28	**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 (Requirement 6 of IAEA	**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:	**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 ~~(Requirement 6 of IAEA~~

	Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation): (a) Safety limits; (b) Limiting settings for safety systems; (c) Limits and conditions for normal operation; (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.	(a) Safety limits; (b) Limiting settings for safety systems; (c) Limits and conditions for normal operation; (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.	~~Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation)~~: (a) Safety limits; (b) Limiting settings for safety systems; (c) Limits and conditions for normal operation; (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.
GENERAL PLANT DESIGN: DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT			
29	**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.	*No change.*	*No change.*

	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.		
30	**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.	**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.	**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 external event, either by test or 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.	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 external event, either by test or 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 shall be included in the qualification programme.	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 external event, either by test or 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.
31	**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 to identify unanticipated behaviour of the plant or degradation that might occur in service.	*No change.*	*No change.*

GENERAL PLANT DESIGN: HUMAN FACTORS			
32	**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 likelihood and the effects of operating errors on safety. The design process shall give due consideration 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 all plant states. 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 decisions to act shall be simply and unambiguously presented.	*No change.*	*No change.*

	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.		
GENERAL PLANT DESIGN: OTHER DESIGN CONSIDERATIONS			

33	**Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant** **Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.** 5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.	*No change.*	*No change.*
New		**Requirement 33A: Safety systems, and safety features for design extension conditions, of modules of a multi-module unit** **Each module of a multi-module unit shall have its own safety systems and shall have its own safety features for design extension conditions, as far as practicable. Where a safety system or a safety feature for design extension conditions is shared between reactor modules of a multi-module unit, the shared safety system or safety feature shall be functionally capable of fulfilling the safety requirements of each of these modules, to protect against the consequences of events which have the potential to affect multiple modules.** 5.63A. To further enhance safety, means allowing interconnections between modules of a multi-module unit shall be considered in the design.	**Requirement 33A: Safety systems, and safety features for design extension conditions, of modules of a multi-module unit** **Each module of a multi-module unit shall have its own safety systems and shall have its own safety features for design extension conditions, as far as practicable. Where a safety system or a safety feature for design extension conditions is shared between reactor modules of a multi-module unit, the shared safety system or safety feature shall be functionally capable of fulfilling the safety requirements of each of these modules, to protect against the consequences of events which have the potential to affect multiple modules.** 5.63A. To further enhance safety, means allowing interconnections between modules of a multi-module unit shall be considered in the design.
34	**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 are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and**	*No change.*	*No change.*

	are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.		
35	**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 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 process heat, hydrogen production, district heating or water desalination) shall be designed to limit the transport of radionuclides from the nuclear plant to heat utilization units to ensure that defined regulatory limits are not exceeded under conditions of operational states and in accident conditions.** 5.63B. The design of the nuclear power plant shall take account of the potential impact of abnormal events in coupled facilities on the safety of nuclear power plant by providing adequate physical separation.	**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 process heat, hydrogen production, district heating~~) and/~~or water desalination ~~units~~) shall be designed to ~~prevent processes that~~ limit the transport of radionuclides from the nuclear plant ~~to the desalination unit or the district heating unit~~ heat utilization units to ensure that defined regulatory limits are not exceeded under conditions of operational states and in accident conditions.** 5.63B. The design of the nuclear power plant shall take account of the potential impact of abnormal events in coupled facilities on the safety of nuclear power plant by providing adequate physical separation.
36	**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. 34 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.	*No change.*	*No change.*
37	**Requirement 37: Communication systems at the plant**	*No change.*	*No change.*

	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.		
38	**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.	*No change.*	*No change.*
39	**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.**	*No change.*	*No change.*
40	**Requirement 40: Prevention of harmful interactions of systems important to safety**	*No change.*	*No change.*

	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.		
41	**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.**	*No change.*	*No change.*
GENERAL PLANT DESIGN: SAFETY ANALYSIS			
42	**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	**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	**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. 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 and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. 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 acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation	initiating events and event sequences shall be confirmed. 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 and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. 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 acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by inherent safety features and safety actions	initiating events and event sequences shall be confirmed. 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 and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. 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 acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by inherent safety features and safety actions

	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 situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.	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 inherent safety features and 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 situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.	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 inherent safety features and 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 situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented; (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.
DESIGN OF SPECIFIC PLANT SYSTEMS: REACTOR CORE AND ASSOCIATED FEATURES			
43	**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.**	**Requirement 43: Performance of particle based fuel elements** **The coated particles for the nuclear power plant shall be designed to maintain their structural integrity, maintain their confinement performance, 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 and accident conditions. The fuel elements that contain the fuel particles shall be designed to maintain their structural integrity in the operational states, and to prevent**	**Requirement 43: Performance of particle based fuel elements ~~and assemblies~~** **~~Fuel elements and assemblies~~ The coated particles for the nuclear power plant shall be designed to maintain their structural integrity, maintain their confinement performance, 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 and accident conditions. The fuel elements that contain the fuel particles shall be designed to maintain their structural integrity in the operational states, and**

		unacceptable loads to the coated fuel particles in accident conditions.	**to prevent unacceptable loads to the coated fuel particles in accident conditions.**
	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; — Variations in performance in relation to heat transfer that could result from distortion or chemical effects. Allowance shall be made for uncertainties in data, in calculations and in manufacture.	6.1. The processes of deterioration to be considered shall include those arising from: — Thermal effect; — Internal pressure due to fission products and other gasses in coated fuel particles; — Kernel migration in coated fuel particle due to temperature gradient; — Chemical attack of coating layers of coated fuel particle by metallic fission products; — Irradiation of fuel particles and other materials in the fuel elements; — Abrasion (for pebble bed design); — Coolant chemical effects; — Static and dynamic loading. Allowance shall be made for uncertainties in data, in calculations and in manufacture.	6.1. The processes of deterioration to be considered shall include those arising from: — Thermal effect; ~~— Differential expansion and deformation;~~ ~~— External pressure of the coolant;~~ — ~~Additional~~ Internal pressure due to fission products and other gasses ~~the buildup of helium~~ in coated fuel ~~elements~~ particles; — Kernel migration in coated fuel particle due to temperature gradient; — Chemical attack of coating layers of coated fuel particle by metallic fission products; — Irradiation of fuel particles and other materials in the fuel ~~assembly~~ elements; ~~— Variations in pressure and temperature resulting from variations in power demand;~~ — Abrasion (for pebble bed design); — Coolant chemical effects; — Static and dynamic loading~~, including flow induced vibrations and mechanical vibrations;~~. ~~— Variations in performance in relation to heat transfer that could result from distortion 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.	6.2. Fuel design limits shall account for (i) key manufacturing parameters, coated fuel particles defect fraction, heavy metal contamination, and (ii) during operations irradiation time and temperature leading to a specified acceptable radionuclide release. 6.2A Fuel shall be designed for acceptable radionuclide retention during accidents based on the spatial and time distribution of fuel temperature leading to a specified acceptable radionuclide release. 6.2B Fuel shall be designed to take chemical attack in all states into account.	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~~ account for (i) key manufacturing parameters, coated fuel particles defect fraction, heavy metal contamination, and (ii) during operations irradiation time and temperature leading to a specified acceptable radionuclide release. 6.2A Fuel shall be designed for acceptable radionuclide retention during accidents based on the spatial and time distribution of fuel temperature leading to a specified acceptable radionuclide release.

	6.3. Fuel elements and fuel assemblies shall be capable of withstanding the loads and stresses associated with fuel handling.	6.3. Fuel particles and elements shall be capable of withstanding the loads and stresses associated with fuel handling.	6.2B Fuel shall be designed to take chemical attack in all states into account. 6.3. Fuel particles and elements ~~and fuel assemblies~~ shall be capable of withstanding the loads and stresses associated with fuel handling.
44	**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 44: Structural capability of the reactor core** **The reactor core, including fuel elements, reflectors, and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions, unacceptable loads to the coated fuel particles are prevented, adequate core cooling can be achieved and maintained, and the core temperature remains within acceptable limits. The reactor core and supporting structures shall also be designed so that, in all plant states, a geometry to allow reactor shutdown (adequate for control of core heat generation) and sufficient heat removal (to the surrounding structures and environment, as necessary) can be maintained.**	**Requirement 44: Structural capability of the reactor core** **The reactor core, including fuel elements ~~and fuel assemblies~~ , reflectors, 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~~, unacceptable loads to the coated fuel particles are prevented, adequate core cooling can be achieved and maintained, and the core temperature remains within acceptable limits. The reactor core and supporting structures shall also be designed so that, in all plant states, a geometry to allow reactor shutdown (adequate for control of core heat generation) and sufficient heat removal (to the surrounding structures and environment, as necessary) can be maintained.**
45	**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	**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, 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 and controlling the neutron flux distributions in the reactor core and their	**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 and controlling the neutron flux distributions in the reactor core and their

	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.	changes shall be provided as necessary 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 shall be limited or compensated for to maintain the capability for cooling and to prevent any significant damage to the reactor core.	changes shall be provided as necessary 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.
46	**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.	**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 design provisions for shutting down the reactor shall consist of at least two diverse and independent means.	**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~~ design provisions for shutting down the reactor shall consist of at least two diverse and independent ~~systems~~ means.

	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.	6.10. At least one of the two different shutdown means 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. At least one of 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.	6.10. At least one of the two different shutdown ~~systems~~ means 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. At least one of 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.
DESIGN OF SPECIFIC PLANT SYSTEMS: REACTOR COOLANT SYSTEMS			
47	**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	**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 loss of helium (coolant) and to prevent the rapid ingress of air or water. 6.13A. The coolant pressure boundary shall form one of the layers of protection of the release of radionuclides from the fuel during operational states and accident conditions. 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	**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)~~ helium (coolant) and to prevent the ~~loss of coolant through interfacing systems~~ rapid ingress of air or water. 6.13A. The coolant pressure boundary shall form one of the layers of protection of the release of radionuclides from the fuel during operational states and accident conditions. 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.	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 circulator or turbine 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.	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~~ circulator or turbine 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.
48	**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 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 an unacceptable release of radioactive material from the nuclear power plant directly to the environment.**	**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~~ an unacceptable release of radioactive material from the nuclear power plant directly to the environment.**
49	**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.**	*No change.*	*No change.*
50	**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**	**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 products and fission products deriving from the fuel, and non-radioactive substances.**	**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.	6.17. The capabilities of the necessary plant systems shall be based on the specified design limit of the chemical impurities in the primary coolant, and shall ensure that the level of circuit activity is as low as reasonably practicable.	**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~~ of the chemical impurities in the primary coolant, and shall ensure that the level of circuit activity 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~~.
51	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.	*No change.*	*No change.*
52	**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;	*Not Applicable.*	*Not Applicable.*

	(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.		
53	**Requirement 53: Heat transfer to an ultimate heat sink** **The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.** 6.19A. Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink. 6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.	**Requirement 53: Heat transfer to an ultimate heat sink** **The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.** 6.19A. Means for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. Residual heat removal to the reactor pressure vessel is achieved by conduction, convection and radiation independent of the primary heat transfer system and helium pressurization. A highly reliable capability to transfer heat from the reactor pressure vessel wall to an ultimate heat sink shall be ensured and may be either completely passive or have both an active and a passive mode. For design extension conditions, residual heat removal may require the use of a different ultimate heat sink (such as buildings and surrounding structures) or different access to the ultimate heat sink. 6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.	**Requirement 53: Heat transfer to an ultimate heat sink** **The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states to achieve radionuclide retention within the fuel and maintain integrity of the reactor pressure vessel.** 6.19A. ~~Systems~~ Means for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. Residual heat removal to the reactor pressure vessel is achieved by conduction, convection and radiation independent of the primary heat transfer system and helium pressurization. A highly reliable capability to transfer heat from the reactor pressure vessel wall to an ultimate heat sink shall be ensured and may be either completely passive or have both an active and a passive mode. ~~This~~ For design extension conditions, residual heat removal may require the use of a different ultimate heat sink (such as buildings and surrounding structures) or different access to the ultimate heat sink. 6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.
New		**Requirement 53A: Design of secondary coolant systems to limit water ingress** **The secondary coolant systems using water and/or steam shall be designed with provision to limit the water ingress into the primary helium system, so**	**Requirement 53A: Design of secondary coolant systems to limit water ingress** **The secondary coolant systems using water and/or steam shall be designed with provision to limit the water ingress into the primary helium system, so**

		as not to exceed specified design limits of the reactor core and coolant pressure boundary.	**as not to exceed specified design limits of the reactor core and coolant pressure boundary.**
DESIGN OF SPECIFIC PLANT SYSTEMS: CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM			
54	**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 54: Reactor building** **A structure (building, or part of a building) shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) control and limit release of radioactive substances 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.** 6.19C.The design of the structure shall provide for sufficient pathways for the release of reactor coolant from the structure in the event of depressurization or severe water ingress accidents. The cross-sections of openings 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 structure or systems that are important for the main safety functions in accident conditions. 6.19D. A structure (building or part of it) shall provide for controlled release of radioactive substances in operational states and in design basis accident conditions, and contribute to limit release in DECs (or BDBE covering Option B in requirement 13). Insofar, this structure combined with other supporting systems, e.g. ventilation systems, is a barrier for the retention of radioactive materials. 6.19E Design features to limit the availability of air for possible rapid ingress into the reactor core in the event of a break in the reactor coolant pressure boundary shall be provided as necessary.	**Requirement 54: ~~Containment system for the r~~Reactor building** **A ~~containment system~~ structure (building, or part of a building) shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) ~~confinement~~ control and limit release 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.** 6.19C.The design of the structure shall provide for sufficient pathways for the release of reactor coolant from the structure in the event of depressurization or severe water ingress accidents. The cross-sections of openings 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 structure or systems that are important for the main safety functions in accident conditions. 6.19D. A structure (building or part of it) shall provide for controlled release of radioactive substances in operational states and in design basis accident conditions, and contribute to limit release in design extension conditions. Insofar, this structure combined with other supporting systems, e.g. ventilation systems, is a barrier for the retention of radioactive materials. 6.19E Design features to limit the availability of air for possible rapid ingress into the reactor core in the event of a break in the reactor coolant pressure boundary shall be provided as necessary.
55	**Requirement 55: Control of radioactive releases from the containment**	**Requirement 55: Control of radioactive releases from the reactor building**	**Requirement 55: Control of radioactive releases from the ~~containment~~ reactor building**

	The design of the containment shall be such as to ensure that any radioactive release 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.	**The design of the reactor building shall be such as to ensure that any radioactive release 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 structures and the supporting systems contributing to confinement function of the reactor building shall be designed and constructed so that the release rate can be tested at conditions representative of the credited confinement function during a postulated accident.	**The design of the ~~containment~~ reactor building shall be such as to ensure that any radioactive release 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~~ structures and the supporting systems ~~and components affecting the leaktightness of the containment system~~ contributing to confinement function of the reactor building shall be designed and constructed so that the ~~leak~~ release rate can be tested at conditions representative of the credited confinement function during a postulated accident ~~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.~~
56	**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	*Not Applicable.*	*Not Applicable.*

	are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series 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.		
57	**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, provision for ensuring protection and safety for operating personnel shall be specified in the design.	*Not Applicable.*	*Not Applicable.*

	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.		
58	**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. Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release. 6.28B. The design shall also include features to enable the safe use of non-permanent equipment for	*Not Applicable.*	*Not Applicable.*

	restoring the capability to remove heat from the containment. 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.		
DESIGN OF SPECIFIC PLANT SYSTEMS: INSTRUMENTATION AND CONTROL SYSTEMS			
59	**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 releases and the amounts of	**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 reactor building 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 releases and the amounts of	**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~~ reactor building 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

	radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.	radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.	the locations of releases and the amounts of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis.
60	**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.**	*No change.*	*No change.*
61	**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 shall 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.	*No change.*	*No change.*
62	**Requirement 62: Reliability and testability of instrumentation and control systems**	*No change.*	*No change.*

	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 the 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.		
63	**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:	*No change.*	*No change.*

	(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.		
64	**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.	*No change.*	*No change.*
65	**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**	*No change.*	*No change.*

	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, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases 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 of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.		
66	**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	*No change.*	*No change.*

	hazards also apply for the supplementary control room at the nuclear power plant.		
67	**Requirement 67: Emergency response facilities on the site** **The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.** 6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.	*No change.*	*No change.*
DESIGN OF SPECIFIC PLANT SYSTEMS: EMERGENCY POWER SUPPLY			
68	**Requirement 68: Design for withstanding the loss of off-site power** **The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.** 6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity. 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	**Requirement 68: Design for withstanding the loss of off-site power** **The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.** 6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity. 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	**Requirement 68: Design for withstanding the loss of off-site power** **The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.** 6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity. 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. 6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply. 6.44B. Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources. 6.44C. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery. 6.44D. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources. 6.45. The design basis for any diesel engine or other prime mover 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. 6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.	that are consistent with all the requirements of the safety systems to be supplied with power, and their functional capability shall be testable. 6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply. 6.44B. Equipment that is necessary to mitigate the consequences of design extension conditions shall be capable of being supplied by any of the available power sources. 6.44C. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery. 6.44D. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources. 6.45. The design basis for any diesel engine or other prime mover 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. 6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.	that are consistent with all the requirements of the safety systems to be supplied with power, and their functional capability shall be testable. 6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply. 6.44B. Equipment that is necessary to mitigate the consequences of ~~melting of the reactor core~~ design extension conditions shall be capable of being supplied by any of the available power sources. 6.44C. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery. 6.44D. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources. 6.45. The design basis for any diesel engine or other prime mover 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. 6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.

DESIGN OF SPECIFIC PLANT SYSTEMS: SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS			
69	**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.**	*No change.*	*No change.*
70	**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.	*No change.*	*No change.*
71	**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.	*No change.*	*No change.*
72	**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.**	*No change.*	*No change.*

73	**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 gaseous radioactive releases 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.	*No change.*	*No change.*
74	**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.**	*No change.*	*No change.*

	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.		
75	**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.**	*No change.*	*No change.*
76	**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.	*No change.*	*No change.*
DESIGN OF SPECIFIC PLANT SYSTEMS: OTHER POWER CONVERSION SYSTEMS			

77	**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.	**Requirement 77: Power conversion systems** **The design of the power conversion systems 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. In a water/steam cycle, the design of the steam supply system and the feedwater system shall provide for appropriately rated and qualified steam/water isolation valves capable of closing under the specified conditions in operational states and in 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.	**Requirement 77: ~~Steam supply system, feedwater system and turbine generators~~ Power conversion systems** **The design of the ~~steam supply system, feedwater system and turbine generators~~ power conversion systems 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~~ In a water/steam cycle, the design of the steam supply system and the feedwater system shall provide for appropriately rated and qualified steam/water 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.
DESIGN OF SPECIFIC PLANT SYSTEMS: TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE			
78	**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	*No change.*	*No change.*

	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.		
79	**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 liquid radioactive releases 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.	*No change.*	*No change.*
DESIGN OF SPECIFIC PLANT SYSTEMS: FUEL HANDLING AND STORAGE SYSTEMS			
80	**Requirement 80: Fuel handling and storage systems** **Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that**	**Requirement 80: Fuel handling and storage systems** **Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that**	**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 avoid causing unacceptable handling stresses on fuel elements or fuel assemblies;	**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 elements, as necessary; (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 avoid causing unacceptable handling stresses on fuel elements;	**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~~ elements, as necessary; (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 avoid causing unacceptable handling stresses on fuel elements ~~or fuel assemblies~~;

	(d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel; (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 shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design of the plant: (a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break; (c) Shall provide a capability to restore the water inventory. The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.	(d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel; (e) To permit safe keeping of suspect or damaged fuel elements; (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 shall be such as to prevent the uncovering of fuel elements in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design of the plant: (a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to prevent the uncovering of fuel elements in the event of a leak or a pipe break; (c) Shall provide a capability to restore the water inventory. The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation. 6.68bis. For reactors using an air-cooling system for fuel storage, the design of the plant:	(d) To prevent the potentially damaging dropping of heavy objects such as spent fuel casks, cranes or other objects onto the fuel; (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 shall be such as to prevent the uncovering of fuel ~~assemblies~~ elements in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated' and so as to avoid high radiation fields on the site. The design of the plant: (a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to prevent the uncovering of fuel ~~assemblies~~ elements in the event of a leak or a pipe break; (c) Shall provide a capability to restore the water inventory. The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation. 6.68bis. For reactors using an air-cooling system for fuel storage, the design of the plant:

		(a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to ensure adequate cooling of fuel elements in the event of air-cooling system malfunctions. The design shall also include features to provide shielding against radiation and necessary capability for confinement of radioactive material for dry cask.	(a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to ensure adequate cooling of fuel elements in the event of air-cooling system malfunctions. The design shall also include features to provide shielding against radiation and necessary capability for confinement of radioactive material for dry cask.
	6.68A. The design shall include the following: (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool; (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool; (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool; (d) Means for monitoring and controlling the water chemistry for operational states.	6.68A. The design for reactors using a water pool system for fuel storage shall include the following: (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool; (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool; (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool; (d) Means for monitoring and controlling the water chemistry for operational states.	6.68A. The design for reactors using a water pool system for fuel storage shall include the following: (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool; (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool; (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool; (d) Means for monitoring and controlling the water chemistry for operational states.
		6.68B. For reactors using an air-cooling system for fuel storage, the design shall be such as to provide adequate cooling of fuel elements in all plant states of relevance for the spent fuel storage, so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’ and so as to avoid high radiation fields on the site. The design for reactors using an air cooling system for fuel storage shall include the following: (a) Means for monitoring and controlling the air temperature for operational states and for accident conditions that are of relevance for the spent fuel storage; (b) Means for monitoring and controlling the activity in air for operational states and means for monitoring	6.68B. For reactors using an air-cooling system for fuel storage, the design shall be such as to provide adequate cooling of fuel elements in all plant states of relevance for the spent fuel storage, so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’ and so as to avoid high radiation fields on the site. The design for reactors using an air cooling system for fuel storage shall include the following: (a) Means for monitoring and controlling the air temperature for operational states and for accident conditions that are of relevance for the spent fuel storage; (b) Means for monitoring and controlling the activity in air for operational states and means for monitoring

		the activity in air for accident conditions that are of relevance for the spent fuel storage.	the activity in air for accident conditions that are of relevance for the spent fuel storage.
DESIGN OF SPECIFIC PLANT SYSTEMS: RADIATION PROTECTION			
81	**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, 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	**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, the integrity of the coated fuel particles 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	**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, the integrity of the coated fuel particles ~~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.	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.	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.
82	**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 actions if necessary. 6.79. Stationary monitors shall be provided for measuring the activity of radioactive substances in the	*No change.*	*No change.*

	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, and 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.		
ADDITIONAL CONSIDERATIONS FOR MULTI-MODULE UNITS			
New		**Requirement 83: Multi-module units** **For multi-module units, the design shall take due account of the potential for specific hazards impacting several modules simultaneously, and the potential for hazards initiating at one module impacting other reactor modules of the same unit. The potential for harmful interactions of systems important to safety that might be required to operate simultaneously in multi-module units shall be evaluated, and effects of any harmful interactions shall be prevented. The scope of the safety analysis shall consider events with impact on multiple reactor modules in a unit and multiple units on a site.** 6.85. Interconnections among the reactor modules: For purposes such as operation and accident management, multi-module units might include interconnections between reactor modules. In this case, specific considerations are necessary to ensure that such interconnections will not be detrimental to the safety of each reactor module and of the overall plant. 6.86. Control and protection systems: The control and protection systems of each module and the entire plant must ensure that a clear actuation logic is reliably implemented so that an initiating event or accident occurring within one reactor module will not propagate to accident conditions in other reactor modules, and that the reactor modules will not have detrimental effects on each other under accident conditions.	**Requirement 83: Multi-module units** **For multi-module units, the design shall take due account of the potential for specific hazards impacting several modules simultaneously, and the potential for hazards initiating at one module impacting other reactor modules of the same unit. The potential for harmful interactions of systems important to safety that might be required to operate simultaneously in multi-module units shall be evaluated, and effects of any harmful interactions shall be prevented. The scope of the safety analysis shall consider events with impact on multiple reactor modules in a unit and multiple units on a site.** 6.85. Interconnections among the reactor modules: For purposes such as operation and accident management, multi-module units might include interconnections between reactor modules. In this case, specific considerations are necessary to ensure that such interconnections will not be detrimental to the safety of each reactor module and of the overall plant. 6.86. Control and protection systems: The control and protection systems of each module and the entire plant must ensure that a clear actuation logic is reliably implemented so that an initiating event or accident occurring within one reactor module will not propagate to accident conditions in other reactor modules, and that the reactor modules will not have detrimental effects on each other under accident conditions.

		6.87. Human factors engineering: The design of control room shall consider the interactions of different reactor modules providing that these modules share a common control room. This covers aspects relating to the main control room, supplementary control and other emergency response facilities and locations; maintenance of the multiple modules; potential remote control of the main control room; one operator managing several modules; more than one module supplying the same turbine. 6.88. Emergency preparedness and response: This includes aspects relating to the design of multi-module units to enable the emergency response under all relevant conditions. 6.89. Capacity for the addition of future modules, plant lay-out and construction: Some design schemes consider a plant layout which allows a consecutive and serialized construction of the reactor modules. This new practice should involve additional important safety considerations. Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in specifications or capability might result in the addition of new equipment which could, for example, increase the load on heating, ventilating and air conditioning systems. Therefore, consideration might need to be given to including margins in the design capability of relevant support systems to allow for the potential addition of new equipment later.	6.87. Human factors engineering: The design of control room shall consider the interactions of different reactor modules providing that these modules share a common control room. This covers aspects relating to the main control room, supplementary control and other emergency response facilities and locations; maintenance of the multiple modules; potential remote control of the main control room; one operator managing several modules; more than one module supplying the same turbine. 6.88. Emergency preparedness and response: This includes aspects relating to the design of multi-module units to enable the emergency response under all relevant conditions. 6.89. Capacity for the addition of future modules, plant lay-out and construction: Some design schemes consider a plant layout which allows a consecutive and serialized construction of the reactor modules. This new practice should involve additional important safety considerations. Some SMR designs adopt extension of power capacity during plant lifetime through additional module installation. Changes in specifications or capability might result in the addition of new equipment which could, for example, increase the load on heating, ventilating and air conditioning systems. Therefore, consideration might need to be given to including margins in the design capability of relevant support systems to allow for the potential addition of new equipment later.

A report produced by

GEN IV International Forum

Expertise | Collaboration | Excellence

www.gen-4.org

VHTR-SDC

Very High Temperature Reactor — Safety Design Criteria