NUCLEAR REGULATORY AUTHORITY, GHANA

DRAFT DESIGN OF NUCLEAR INSTALLATIONS REGULATIONS

NRA_DESIGN_DRAFT

Nuclear Regulatory Authority (NRA), Ghana

Houses 1 & 2, Neutron Avenue, P.O. Box AE 50, Atomic- Kwabenya, Accra

official.mail@gnra.org.gh

2024

Arrangement of Regulations

In exercise of the power conferred on the Minister responsible for the Nuclear Regulatory Authority, acting on the advice of the Board of the Authority by section 91 of the Nuclear Regulatory Authority Act, 2015 (Act 895), these Regulations are made this ,,, day …. of 2024.

Preliminary Provisions

Application

1. These regulations apply to

(a) the design requirements and design principles for nuclear installations, together with its systems, structures and components that are important to nuclear safety on the basis of a graded approach;

(b) the establishment of requirements for a comprehensive safety assessment, to enable the identification of the potential hazards that may arise from the operation of the plant, under various plant states including operational states and accident conditions;

(c) the expectations of the Authority regarding the safe design and safety of the nuclear installation taking into account all aspects of the design and promoting multiple levels of defence;

(d) the facilitation of high-quality design, and consistency with modern international codes and standards for nuclear installations;

(e) measures to address safety objectives, concepts and considerations, safety management in design, general considerations in design, design of specific plant system, safety analysis, and environmental protection and mitigation

Responsible Parties

2. (1) An organisation, including a design organisation that engages in an activity important to the safety of the design of a nuclear installation shall ensure that matters concerning safety, security and safeguards are given the highest priority.

(2) An authorised person is responsible for the design of the installation and shall ensure that the responsibility for protection, safety and security for an activity that gives rise to radiation risks is not delegated.

(3) The persons primarily responsible for the application of these regulations are

(a) the applicant;

(b) an employer of workers for a nuclear installation, in relation to occupational exposure; and

(c) a person or an organisation designated to deal with emergency exposure situations or existing exposure situations arising from nuclear activity or nuclear related activity.

(4) Other persons who shall have specified responsibilities for the application of these regulations, include,

(a) providers of nuclear related activity equipment and software;

(b) organisations that review the design of nuclear installations and nuclear related installations, machinery, activity, equipment and software

(c) designers and organisations that design nuclear installations and nuclear related installations, machinery, activity, equipment and software;

(d) qualified experts or other qualified persons assigned specific responsibilities by a person who has primary responsibility under Sub regulation (3); and

(e) workers assigned responsibilities by a person who has primary responsibility under Sub regulation (3).

Resolution of Conflicts in Respect to Application

3. Where in the application of these regulations there appears to be a conflict between the requirements of these regulations and any other law, the Authority shall be given notice in writing of the apparent conflict.

Safety Objectives, Concepts and Considerations

4. (1) An authorised person shall ensure that the nuclear installation of that authorised person is designed in a manner that protects the public and the environment from the harmful effects of ionising radiation.

(2) The authorised person shall, for the purpose of ensuring the achievement of the highest level of safety that can reasonably be achieved in the design of a nuclear installation, shall take measures to

(a) prevent the occurrence of accidents that have harmful consequences as a result of a loss of control over the reactor core or over other sources of radiation;

(b) mitigate the consequences of any accidents that do occur;

(c) ensure, taking into account the design of the installation, that the radiological consequences of any accident fall below the relevant limits and is kept as low as reasonably achievable;

(d) ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of an accident is mitigated to the fullest extent practicable;

(3) The authorised person shall ensure that the design of the nuclear installation

(a) provides for the control of exposure for all operational states at levels that are as low as reasonably achievable and which minimizes the likelihood of an accident that can lead to the loss of control over a source of radiation.

(b) makes provision for the mitigation of the radiological consequences of an accident;

(c) provides practical measures for the mitigation of the consequences of nuclear or radiation accidents on humans and the environment.

Safety of the Plant Design throughout the Lifetime of the Plant

5. (1) An authorised person shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear installation.

(2) The authorised person shall ensure that

(a) the formal system for the continuing safety of the plant design provides for the inclusion of a formally designated entity responsible for the safety of the plant design in the management system of the authorised person; and

(b) tasks that are assigned to external organisations for the design of specific parts of the plant are taken into account in the measures that are instituted.

(3) 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 and establish and implement a series of tasks and functions to ascertain whether

(a) 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) the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information, approval of key engineering documents, conduct of safety assessments and the maintenance of a safety culture are included in the formal system for ensuring the continuing safety of the plant design;

(c) the knowledge of the design that is needed for safe operation, maintenance, including adequate intervals for testing, and modification of the plant is available

and maintained up to date by the authorised person, and whether past operating experience and validated research findings are taken into account;

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

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

(f) the necessary engineering expertise and scientific and technical knowledge are maintained within the organisation of the authorised person;

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

(h) adequate documentation is maintained to facilitate future decommissioning of the nuclear installation.

Fundamental Safety Functions

6. (1) An authorised person shall, ensure the

(a) control of reactivity;

(b) removal of heat from the reactor and from the fuel store; and

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

(2) The authorised person shall

(a) adopt a systematic approach to

(i) identify the items important to safety that are necessary to fulfil the fundamental safety functions; and

(ii) identify the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states; and

(b) provide a means of monitoring the status of the plant to ensure that the required safety functions are fulfilled.

General Design Requirements

7. (1) An applicant for a certification of design of a nuclear installation shall ensure that the design submitted to the Authority meets all applicable safety requirements.

(2) An authorised person shall

(a) apply a management system that controls the complex design system and ensures the quality and consistency of the designs as well as the fulfilment of nuclear safety and security requirements;

(b) ensure that an organisation that is independent of the designer, reviews the compliance of the designs, including the means of design, the design data and the results with the requirements;

(c) ensure that the level of detail and elaboration of the designs correspond, at least, to the scope required for carrying out the regulatory licensing procedures associated with the given life cycle stage;

(d) ensure that the design basis for systems, structures and components important to nuclear safety are specified and documented systematically and that the technical requirements are laid down in the design specifications approved by the Authority;

(e) possess the design information required for maintaining the safe and secure operation of the nuclear installation;

(f) perform or provide for the performance of activities that ensure the safety of the nuclear installation;

(g) make decisions on matters that pertain to safety throughout the lifetime of the nuclear installation;

(h) in relation to the systems, structures and components of the nuclear installation, demonstrate that the fulfilment of the basic design requirements can be verified;

(i) in relation to programmable systems, ensure that the requirements for the systems, structures and components are related to the combination of the hardware and software participating in the performance of the function is fulfilled;

(j) ensure that the design enables the fundamental safety functions to be fulfilled in the case of normal operation, anticipated operational occurrences to design basis accident;

(k) after complex accidents, postulation of multiple failures, ensure that the fundamental safety functions are fulfilled to the extent required for bringing the nuclear installation into a controlled, safe shutdown condition;

(l) ensure that systems, structures and components are designed for the fulfilment of the fundamental safety functions;

(m) for the purpose of ensuring compliance with the fundamental safety functions, identify, by safety and any other analyses, the safety functions and the systems, structures and components required for performance for all operating conditions, including normal operation;

(n) ensure that the residual heat is transferred to the ultimate heat sink in a manner that ensures that the frequency of the loss of the heat removal function is lower than 10^{-7}/year; and

(o) ensure that the design provides reasonably practicable measures to prevent accidents and to mitigate the consequences of accidents if they do occur during the operation of a nuclear installation.

Periodic Safety Review

8. (1) An authorised person shall,

(a) ensure that the management of the nuclear installation performs systematic safety assessments of the installation throughout the operational life span of the installation, taking into account, operating experience and significant new safety information from relevant sources;

(b) ensure that the strategy for review and the safety factors to be evaluated are approved by the Authority;

(c) by means of the periodic safety review, determine to what extent the existing Safety Analysis Report remains valid;

(d) ensure that the periodic safety review takes into consideration, at least,

(i) the plant design;

(ii) actual conditions of various systems;

(iii) systems, structures and components important to safety;

(iv) equipment qualification;

(v) ageing;

(vi) deterministic safety analysis;

(vii) probabilistic safety analysis;

(viii) hazard analysis;

(ix) safety performance;

(x) use of experience from other plants and research findings;

(xi) organizational establishment;

(xii) the management system and safety culture;

(xiii) work procedures;

(xiv) human factors;

(xv) emergency planning;

(xvi) radiological impact on the environment;

(xvii) information from global assessments; and

(xviii) any other relevant aspect;

(e) ensure that the scope of the periodic safety review includes every safety aspect of an operating plant, including both on-site and off-site emergency planning, accident management and radiation protection aspects;

(f) for the purpose of complementing the deterministic assessment, ensure that the periodic safety assessment is used as an input for the periodic safety review to provide insight into the relative contributions to safety of different aspects of the plant;

(g) ensure that the plant management reports to the Authority in a timely manner, the confirmed findings of the safety review that have implications for safety;

(h) ensure that on the basis of results of systematic safety assessment, the plant management implements the necessary corrective actions and reasonably practical modifications for compliance with the applicable standards with the aim of enhancing safety of the plant by further reducing the likelihood and potential consequences of accidents;

(i) submit progress report on the status of implementation of corrective actions generated as a result of periodic safety review, according to the frequency mutually agreed with the Authority;

(j) ensure that the report under paragraph (i), consists of at least the following:

(i) total number of actions with titles;

(ii) completed actions;

(iii) progress on implementation on actions in comparison with target dates;

(iv) reason for the delay in corrective actions, if any, and the measures taken to address the reason;

(v) implications of delayed actions on safe operation of the nuclear installation; and

(vi) alternative measures taken in connection with delayed corrective actions to ensure safety of the nuclear installation.

Defence-in-Depth and its Application

9. (1) An authorised person shall apply defence-in-depth

(a) to the organisational, behavioral, design-related activities in respect to the plant whether the plant is operating in full power or low power or is in various shutdown states. to ensure that the activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures; and

(b) throughout the design to provide for protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

(2) The authorised person shall

(a) implement defence-in-depth through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment;

(b) in implementing defence in depth for a nuclear installation, make provision in the design for a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations; and

(c) ensure that the design provides for each level of defence as contained in the First Schedule.

Operational Limits and Conditions for Safe Operation

10. (1) An authorised person shall ensure that

(a) the design establishes a set of operational limits and conditions for safe operation of the nuclear installation;

(b) the requirements and operational limits and conditions established in the design for the nuclear installations include

(i) safety limits;

(ii) limiting settings for safety systems;

(iii) limits and conditions for normal operation;

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

(v) 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;

(vi) specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems; and

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

Accident Mitigation and Management

11. An authorised person shall ensure that the design

(a) includes provisions to limit radiation exposure in normal operation, anticipated operational occurrence, design basis accident and design extension condition to as low as reasonably achievable levels, and to minimize the likelihood of an accident that could lead to the loss of normal control of the source of radiation;

(b) applies the principle that installation states that could result in high radiation doses or radioactive releases have very low frequency of occurrence, and installation states with significant frequency of occurrence have only minimal, if any, potential radiological consequences;

(c) the equipment to be used in severe accident management are designed to

(i) have sufficient capacity to cope with postulated design extension conditions;

(ii) have sufficient capacity with suitable margins, in accordance with the necessary equipment reliability, to cope with postulated design extension conditions;

(iii) function as required, with sufficient reliability under environmental and load conditions, during postulated design extension conditions; and

(iv) operates under the conditions of postulated design extension conditions;

(d) provides for

(i) permanent equipment for use in the preventive domain in severe accident management are designed in a manner that, as much as possible, takes into consideration diversity with respect to equipment for management of design basis accidents;

(ii) mobile equipment for use in the preventive domain in severe accident management are as diverse as possible with respect to equipment for the management of design basis accidents and permanent equipment for use in the preventive domain of severe accident management;

(iii) equipment for use in severe accident management are installed so as not to cause any detrimental impact to other equipment;

(iv) equipment and procedures are prepared so as to allow easy and reliable changeover from normal line configurations in the event that other equipment is to be used for severe accident management, different from their original use;

(v) measures are taken to standardize connecting methods so that mobile equipment and permanent equipment for severe accident management can be easily and reliably connected to enable the equipment to be used interchangeably between systems and units and multiple connections to

be prepared with appropriate spatial dispersion to avoid disconnection due to common mode failure;

(vi) appropriate measures for equipment use in the mitigatory domain in severe accident management, including piping, valves and electrical cables within the building, in addition to connections to mobile equipment for use in the mitigatory domain in severe accident management so as not to damage the necessary functions for withstanding standard ground motion; and

(vii) equipment for use in the preventive domain in severe accident management, including piping, valves and electrical cables within the building, in addition to connections to mobile equipment for use in the preventive domain in severe accident management, have equivalent seismic resistance to the corresponding equipment for the management of design basis accidents.

Radiation Protection and Dose Acceptance Criteria

12. (1) An authorised person shall ensure that the design

(a) enables the committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary as prescribed in the *Basic Ionising Radiation Control Regulations;* and

(b) during normal operation, including maintenance and decommissioning, doses are regulated by the limits prescribed in the *Basic Ionising Radiation Control Regulations*.

(2) The authorised person shall ensure that the design

(a) provides for the prevention and mitigation of radiation exposures resulting from design basis accidents and design extension conditions; and

(b) prevents potential radiation doses to the public from anticipated operational occurrence and design basis accident from exceeding the dose acceptance criteria provided in the *Basic Ionising Radiation Control Regulations*.

Exclusion Zone

13. An authorised person shall ensure that the design adequately provides for an appropriate exclusion zone as required in the *Emergency Preparedness and Response Regulations*.

Installation Layout

14. An authorised person shall ensure that the design

(a) takes into account the interfaces between the safety and security provisions of the nuclear installation and other aspects of the installation layout; and

(b) reflects an assessment of options, demonstrating that an optimized configuration has been sought for in the installation layout.

Safety Management in Design

Design Organisation

15. (1) An applicant shall ensure that a design organisation is appointed for each stage of the life of the nuclear installation.

(2) The applicant shall confirm that the design organisation has achieved the following objectives during the design phase:

(a) established a knowledge base of all relevant aspects of the installation design and kept it up-to-date, taking into account experience and research findings;
(b) ensured the availability of the design information that is needed for safe installation operation and maintenance;
(c) established the requisite security clearances and associated security measures to protect prescribed, designated, and classified material;
(d) maintained design configuration control;
(e) reviewed, verified, approved or rejected, and documented design changes;

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

(g) ensured that the necessary engineering and scientific skills and knowledge have been maintained; and

(h) ensured that, with respect to individual design changes or multiple changes that may have significant interdependencies, the associated impact on safety has been properly assessed and understood.

Integrated Management System for Design

16. (1) An authorised system shall, in the establishment of the management system for design, ensure that

(a) systems, structures and components important to safety meet their respective design requirements;

(b) due account is taken of the human capabilities and limitations of personnel;

(c) safety design information necessary for safe operation and maintenance of the installation and any subsequent installation modifications is preserved;

(d) Operational Limits and Conditions are provided for incorporation into the installations administrative and operational procedures;

(e) the installation design facilitates maintenance throughout the life of the installation;

(f) the results of the deterministic and probabilistic safety assessments are taken into account;

(g) due consideration is given to the prevention of accidents and mitigation of their consequences;

(h) generation of radioactive waste is limited to minimum practicable levels, in terms of both activity and volume;

(i) a change control process is established to track design changes to provide configuration management during construction, commissioning, and operation; and

(j) physical protection systems are provided to address design basis threats.

(2) The authorised person shall ensure that

(a) the design organisation establishes and implements a management system for ensuring that the safety, security and safeguards 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;

(b) the management system established by the design organisation guarantees the quality of the design of each system, structure and component, as well as of the overall design of the nuclear installation and includes the means for

(i) identifying and correcting design deficiencies;

(ii) for checking the adequacy of the design; and

(iii) for controlling design changes;

(c) the design of the plant, including subsequent changes, modifications or safety improvements, are in accordance with established procedures which

(i) are based on appropriate engineering codes and standards;

(ii) incorporate relevant requirements and design bases; and

(iii) identifies and controls interfaces.

(d) an adequate management system including quality assurance and quality control programmes are established to control the effectiveness of the design process;

(e) the quality assurance programme identifies the performance and assessment parameters for the design, as well as the detailed plans for each system, structure and component to ensure consistent quality of the design and the selected components;

(f) the quality assurance programme is carried out in accordance with established procedures which are based on appropriate standards and codes approved by the Authority, and that incorporate applicable requirements and design bases.

(g) the adequacy of the design includes design tools and design inputs and outputs, verified or validated by individuals or groups that are independent from those who originally performed the work;

(h) the verifications, validations, and approvals are completed before the detailed design is implemented;

(i) the quality assurance programme facilitates the identification and control of design interfaces;

(j) the quality control programme covers document control, design control, procurement control, control of items, process control, inspection and test control, non-conformance control, corrective actions, records and audits and other control measures;

(l) the management system includes project management, project risk management, integrated quality management and data management;

(m) the management system is implemented for the activities that may influence safety, security and safeguards, or the derivation of parameters for the design; and

(n) records that permit independent review of the design are kept, and the processes leading to the design of the nuclear installation are made available to the Authority.

Proven Engineering Practices

17. (1) An authorised person shall ensure that the design organisation

(a) identifies the modern standards and codes that will be used for the plant design;

(b) evaluates the standards and codes for applicability, adequacy, and sufficiency to the design of the systems, structures and components important to safety; and

(c) where necessary, supplement or modify the codes and standards to ensure that the final quality of the design is commensurate with the necessary safety functions.

(2) An authorised person shall ensure that

(a) the systems, structures and components which are important, are of proven designs and would be designed according to the standards and codes identified for the nuclear installation; and

(b) where a new systems, structures and components design, feature, or engineering practice is introduced, adequate safety is proved by a combination of supporting research and development programmes, and by examination of relevant experience from similar applications;

(c) the design organisation establishes an adequate qualification programme to verify that the new design satisfies the applicable safety design requirements;

(d) new designs are

(i) tested before being brought into service; and

(ii) monitored in service to verify whether the design performs as required;

(e) in the selection of equipment, due attention is given to spurious operation and to unsafe failure modes which may fail to trip when necessary; and

(f) where the design has to accommodate systems, structures and components failure, preference is given to equipment that exhibits known and predictable modes of failure, and that facilitates repair or replacement.

Safety Assessment

18. An authorised person shall ensure that

(a) safety assessment is applied as a systematic process, throughout the design phase to ensure that the design satisfies the relevant safety requirements;

(b) the basis for the safety assessment is based on the derivation of data from the safety analysis, previous operational experience, results of supporting research, and proven engineering practices;

(c) the safety assessment is part of the design process, with iteration between the design and analyses, and increases in scope and level of detail as the design process progresses;

(d) before the design is submitted to the Authority, an independent peer review of the safety assessment is conducted by an expert separate from the one carrying out the design; and

(e) the safety assessment documentation

(i) identifies the aspects of the operation, maintenance, and management that are important to safety;

(ii) is maintained in a dynamic suite of documents to reflect changes in design as the plant evolves; and

(iii) is presented clearly and concisely, in a logical and understandable format, and is readily accessible to designers, operators, and the relevant organizations.

Design Documentation

19. An authorised person shall ensure that the design documentation includes,

(a) design description;

(b) design requirements;

(c) system classifications;

(d) description of installation states;

(e) security system design, including a description of physical security barriers;

(f) operational limits and conditions;

(g) identification and categorisation of initiating events;

(h) acceptance criteria and derived acceptance criteria;

(i) deterministic safety analysis;

(j) probabilistic safety assessment;

(k) hazards analysis;

(l) design manual; and

(m) Safety Analysis Report.

Classification of Systems, Structures and Components

20. An authorised person shall ensure that

(a) the design organisation classifies systems, structures and components in a consistent and clearly defined classification scheme on the basis of their function and safety significance;

(b) the systems, structures and components are designed, constructed and maintained to a standard that guarantees that their quality and reliability are commensurate with their classification;

(c) the systems, structures and components are identified as either important or not important to safety and the criteria for determining safety importance are based on

(i) the safety function to be performed;

(ii) consequence of failure;

(iii) probability that the systems, structures and components will be called upon to perform the safety function; and

(iv) the time at which the systems, structures and components will be called upon to operate, after a Postulated initiating event, and the expected duration of that operation;

(d) the design provides appropriate interfaces between systems, structures and components of different classes to minimize the risk of systems, structures and components of less important to safety from adversely affecting the function or reliability of systems, structures and components of greater importance;

(e) an equipment that performs multiple functions is classified in a safety class that is consistent with the most important function performed by the equipment; and

(f) the design has the capacity to prevent

(i) any interference between items important to safety and

(ii) in particular, the propagation of a failure of items important to safety in a system in a lower safety class, to a system in a higher safety class.

Installation Design Envelope

21. An authorised person shall ensure that

(a) the design organisation establishes the installation design envelope, which comprises the design basis and complementary design features;

(b) the design basis specifies the capabilities that are necessary for the installation in normal operation, anticipated operational occurrence and design basis accident;

(c) the conservative design measures and sound engineering practices are applied in the design basis for normal operation, anticipated operational occurrence and design basis accident;

(d) the complementary design features, addresses the performance of the installations in design extension condition, including selected severe accidents.

Installation States

22. (1) An authorised person shall ensure that for normal operations,

(a) the design facilitates safe operation of the plant within a defined range of parameters, with an assumed availability of a minimum set of specified support features for safety systems;

(b) the design minimizes the unavailability of safety systems and addresses the potential for occurrence of accidents where the availability of safety systems may be reduced, as a result of shutdown, start-up, low power operation, refuelling, and maintenance;

(c) the design establishes a set of requirements and limitations for safe normal operation, including,

(i) limits important to safety;

(ii) constraints on control systems and procedures;

(iii) plant maintenance, testing, and inspection requirements to ensure that systems, structures and components function as intended, taking the as low as reasonably achievable principle into consideration; and

(iv) clearly defined operating configurations, in the nature of start-up, power production, shutdown, maintenance, testing, surveillance, and refuelling, include relevant operational restrictions in the event of safety system and safety support system outages.

(2) The authorised person shall ensure that for an anticipated operational occurrence,

(a) the design includes provisions that restrict releases to the public following the anticipated operational occurrence, from exceeding the dose acceptance criteria;

(b) the design provides, to the extent practicable, for systems, structures and components not involved in the initiation of the anticipated operational occurrence to remain operable following the anticipated operational occurrence;

(c) the response of the plant to a wide range of anticipated operational occurrences allows safe operation or shutdown, where necessary; and

(d) the installation layout makes provision for equipment to be placed at the most suitable location to ensure its immediate availability when operator intervention is required, allowing for safe and timely access during an anticipated operational occurrence.

(3) The authorised person shall ensure that for design basis accidents,

(a) the set of accidents that are to be considered in the design are derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear installation to withstand, without the acceptable limits for radiation protection being exceeded;

(b) the design bases are defined by using the accidents and in that regard the bases include performance criteria,

(i) for safety systems and for other items important to safety; and

(ii) 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 accident;

(c) the design provides for key plant parameters which

(i) do not exceed the specified design limits; and

(ii) have the primary objective to manage the design basis accidents so that they do not have, or only have minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions;

(d) the analysis is done in a conservative manner which involves the postulating of certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis;

(e) the set of accidents set the boundary conditions according to which systems, structures and components important to safety are designed;

(f) the design prevents releases to the public following a design basis accident from exceeding the dose acceptance criteria;

(g) in order to prevent progression to a more severe condition that may threaten the next barrier, the design includes a provision the automatic initiation of the necessary safety systems where prompt and reliable action is required in response to a postulated initiating event;

(h) provision is made to support timely detection of, and manual response to, conditions where prompt action is not necessary, including responses in the nature of manual initiation of systems or other operator actions;

(i) the design takes into account operator actions that may be necessary to diagnose the state of the installation and to put the installation into a stable long-term shutdown condition in a timely manner;

(j) the design makes provision for adequate instrumentation to monitor installation status, and controls for manual operation of equipment; and

(k) equipment necessary for manual response and recovery processes are placed at the most suitable location to allow safe and timely worker access when needed.

(4) The authorised person shall ensure that for design extension condition,

(a) the set of extension conditions are derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of for the purpose of further improving the safety of the nuclear installation by enhancing the installation's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures;

(b) the extension conditions are used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of the accidents or mitigation of the consequences of the accidents;

(c) an analysis of the extension conditions for the plant are performed;

(d) additional safety features for the extension conditions, or extension of the capability of safety systems, are capable of 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.

(e) the installation is designed in a manner that enables the plant to be brought into a controlled state in which the containment function is 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 eliminated;

(f) the extension conditions are 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 the conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.

(g) the analysis undertaken includes the 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;

(h) the features to be identified in paragraph (g) are required to

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

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

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

(i) the containment and its safety features shall be able to withstand extreme scenarios, selected by using engineering judgement and input from probabilistic safety assessments, which scenarios include, among other things, melting of the reactor core;

(j) the design is of a quality that eliminates the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release;

(k) the design is of a quality that makes protective actions that are limited in terms of lengths of time and areas of application, sufficient for the protection of the public, and provides sufficient time to take the required measures;

(l) where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events can lead to anticipated operational occurrences or to accident conditions, the combinations of events are considered to be design basis accidents or are included as part of design extension conditions, depending mainly on their likelihood of occurrence; and

(m) in the case where an event is a consequence of another event, the consequential effects are considered as part of the original postulated initiating event.

Postulated Initiating Events Considered in the Design

23. An authorised person shall ensure that

(a) the design for the nuclear installation applies a systematic approach to identifying a comprehensive set of postulated initiating events in a manner that permits foreseeable events

(i) with the potential for serious consequences, and

(ii) with a significant frequency of occurrence to be anticipated and to be considered in the design;

(b) 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 are 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;

(c) a technically supported justification is provided for the exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events;

(d) where prompt and reliable action are required in response to a postulated initiating event,

(i) provision is made in the design for automatic safety actions for the necessary actuation of the safety systems, to prevent progression to more severe plant conditions;

(ii) reliance can be placed on the manual initiation of systems or on other operator actions;

(e) paragraph (d) is applied only where

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

(ii) an assessment has been 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;

(f) the operator actions that are required to diagnose the state of the installation after postulated initiating event and to put the plant into a stable long term shutdown condition in a timely manner is facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment;

(g) the design specifies the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating harmful consequences of a loss of control; and

(h) an equipment that is necessary for actions to be taken in manual response and recovery processes is 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.

Internal and External Hazards

24. An authorised person shall ensure that

(a) foreseeable internal hazards and external hazards, including the potential for human induced events to directly or indirectly affect the safety of the nuclear installation, are identified and their effects evaluated;

(b) the hazards are taken into consideration in

(i) designing the layout of the installation;

(ii) determining the postulated initiating events and generated loadings for use; and

(iii) the design of relevant items important to safety for the installation;

(c) items important to safety are designed and located

(i) to withstand the effects of the hazards or with a provision for their protection;

(ii) in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards; and

(iii) taking due cognizance of other implications to safety;

(d) for multiple unit plant sites, the design takes due account of the potential for specific hazards to give rise to impacts on several or even all of the units on the site simultaneously;

(e) for internal hazards,

(i) the plant design takes into account the potential for hazards, including flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact, fire, smoke, and combustion by-products, or release of fluid from failed systems or from other installations on the site;

(ii) appropriate features for prevention and mitigation are provided to ensure that safety is not compromised; and

(iii) the design takes into consideration the possible interaction of external and internal events including external events that initiate internal fires or floods that may lead to the generation of missiles;

(f) for an internal hazard that involves the interconnection of two fluid systems operating at different pressures

(i) failure of the interconnection to operate as required will not affect the capability of the fluid systems to withstand the higher pressure; or

(ii) provision is made so that the pressure of the system operating at the lower pressure will not be exceeded, where the interconnection fails to operate as required;

(g) for external hazards,

(i) the design takes into consideration the natural and human-induced external events that may be linked with significant radiological risk;

(ii) the subset of external events that the installation is designed to withstand are selected and the design basis events are determined from this subset;

(iii) the design takes into consideration of natural and human induced external events that have been identified in the site evaluation process;

(iv) causation and likelihood are considered in postulating potential hazards;

(v) in the short term, the safety of the plant is not made dependent on the availability of off-site services including electricity supply and firefighting services;

(vi) the design takes due account of site-specific conditions to determine the maximum delay time by which off-site services need to be available;

(vii) features are 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;

(viii) the design of the installation, on the basis of the hazard evaluation of the site, provides for an adequate margin to protect items important to safety against levels of external hazards to be considered for design and for the avoidance of cliff edge effects;

(ix) the design of the installation on the basis of the hazard evaluation of the site provides 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; and

(x) the site evaluation and environmental assessment results are taken into account to determine the design basis for the installation; and

(h) for a combination of events,

(i) a combination of randomly occurring individual events that could credibly lead to anticipated operational occurrence, design basis accident, or design extension condition is considered in the design; and

(ii) an event that may result from other events including floods following an earthquake are considered to be part of the original postulated initiating event.

Engineering Design Rules

25. An authorised person shall ensure that

(a) the engineering design rules for items important to safety at a nuclear installation

(i) are specified and comply with the relevant national or international codes and standards and with proven engineering practices; and

(ii) take due account of the relevance of the rules for nuclear technology;

(b) methods that provide for a robust design are applied, and proven engineering practices are adhered to in the design of a nuclear installation to guarantee the achievement of the fundamental safety functions for each operational state and for every accident condition.

Fail-Safe Design

26. An authorised person shall ensure that

(a) fail-safe design is incorporated into the design of systems and components important to safety; and

(b) systems and components important to safety are designed for fail-safe capability so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.

Reliability of Design Safety

27. (1) An authorised person shall ensure that

(a) systems, structures and components important to safety are designed with sufficient quality and reliability to meet the design limits;

(b) a reliability analysis is performed for each of the systems, structures and components

(c) where possible, the design provides for testing to demonstrate the reliability of the design to meet the requirements during operation;

(d) the safety systems and their support systems are designed to guarantee that the probability of a safety system failure on demand from all causes is lower than 10^{-3};

(e) the reliability model for each system takes into account realistic failure criteria and best estimate failure rates, considering the anticipated demand on the system from the postulated initiating event;

(f) design for reliability includes consideration of mission times for systems, structures and components important to safety;

(g) the design stake into account the availability of off-site services upon which the safety of the installation and protection of the public may depend, the supply of electricity and external emergency response services.

(2) The authorised person shall, for common-cause failures, ensure that

(a) the potential for the failure of items important to safety are taken into consideration in determining where to apply the principles of diversity, separation, and independence to achieve the necessary reliability;

(b) the design provides sufficient physical separation between redundant divisions of the safety support systems and process systems;

(c) paragraph (b) is applied to equipment and to routing of

(i) electrical cables for power and control of equipment;

(ii) piping for service water for the cooling of fuel and process equipment; and

(iii) tubing and piping for compressed air or hydraulic drives for control equipment;

(d) space sharing arrangement is justified in the design documentation, where physical separation is not possible and where space sharing is necessary, services for safety and other important process systems are arranged in a manner that

(i) prevents a safety system which is designed to act as backup from being located in the same space as the primary safety system; and

(ii) ensures that where a safety system and a process system have to share space, the associated safety functions are also provided by another safety system to counter the possibility of failures in the process system;

(e) the design provides effective protection against common-cause events where sufficient physical separation among individual services or groups of services does not exist;

(f) the design organization assesses the effectiveness of specified physical separation or protective measures against common-cause events;

(g) diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components;

(h) the diversity is examined for any similarity in materials, components, and manufacturing processes, or subtle similarities in operating principles or common support features;

(i) there is a reasonable assurance that the addition of diverse components are of overall benefit, taking into account associated disadvantages including the extra complication in operational, maintenance, and test procedures, or the consequent use of equipment of lower reliability.

(3) The authorised person shall for single failure criteria ensure that:

(a) each safety group performs the required safety functions under the worst permissible systems configuration, taking into account considerations of maintenance, testing, inspection and repair, and equipment outage;

(b) an analysis is conducted of each possible single failure, and the associated consequential failures for each element of each safety group until every safety group has been considered;

(c) unintended actions and failure of passive components are considered as the two possible modes of failure of a safety group;

(d) passive components are exempted when single failure is assumed to occur prior to the postulated initiating event, or at any time during the mission time for which the safety group is required to function after the postulated initiating event;

(f) exemptions for passive components are applied only to the components that are designed and manufactured to high standards of quality, that are adequately inspected and maintained in service, and that remain unaffected by the postulated initiating event; and

(g) design documentation includes analytical justification of the exemptions, taking into account loads and environmental conditions, as well as the total period of time after the postulated initiating event for which the functioning of the component is necessary.

Instrumentation and Control

28. An authorised person shall ensure that

(a) design includes provision of instrumentation

(i) to monitor plant variables and systems over the respective ranges for normal operation, anticipated operational occurrence, design basis accident, and design extension condition; and

(ii) for measuring variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems, containment, as well as instrumentation for obtaining any 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;

(b) a protection system is provided at the nuclear installation 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;

(c) the design provides for the safety systems and the necessary support systems to be reliably and independently operated, either automatically or manually, when necessary;

(d) the design includes the capability to trend and automatically record measurement of any derived parameters that are important to safety;

(e) the instrumentation is adequate for measuring parameters for emergency response purposes and that the design includes reliable controls to maintain and limit variables within specified operational ranges;

(f) the design minimizes the likelihood of an operator action defeating the effectiveness of safety and control systems in normal operation and anticipated operational occurrence, without negating correct operator actions following a design basis accident;

(g) system control interlocks are designed to minimize the likelihood of inadvertent manual or automatic override, and to provide for situations where it is necessary to override interlocks to use equipment;

(h) instrumentation and recording equipment are provided to enable essential information to be available for

(i) monitoring the status of essential equipment and the course of accidents,

(ii) 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

(iii) post-accident analysis.

Support Service Systems

29. An authorised person shall ensure that

(a) the design of supporting systems and auxiliary systems make the systems capable to perform in a manner that is consistent with the safety significance of the system or component that they serve at the nuclear installation;

(b) auxiliary systems are provided as appropriate to remove heat from systems and components at the nuclear installation that are required to function in operational states and in accident conditions;

(c) process sampling systems and post-accident sampling systems are 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 every operational state and in accident conditions at the nuclear installation;

(d) the design basis for any compressed air system that serves an item important to safety at the nuclear installation specifies the quality, flow rate and cleanness of the air to be provided;

(e) systems for air conditioning, air heating, air cooling and ventilation are provided as appropriate in auxiliary rooms or other areas at the nuclear installation to maintain the required environmental conditions for systems and components important to safety in each plant state.

(f) non-combustible or fire retardant and heat resistant materials are used wherever practicable throughout the plant, in particular in locations including the containment and the control rooms;

(g) adequate lighting is provided in all operational areas of the nuclear installation in operational states and in accident conditions;

(h) overhead lifting equipment is provided for lifting and lowering items important to safety at the nuclear installation, and for lifting and lowering other items in the proximity of items important to safety;

(i) the overhead lifting equipment is designed in a manner that enables

(i) measures to be taken to prevent the lifting of excessive loads;

(ii) conservative design measures to be applied to prevent unintentional dropping of loads that could affect items important to safety;

(iii) the plant layout to permit safe movement of the overhead lifting equipment and of items being transported;

(iv) the equipment to be used only in specified plant states, by means of safety interlocks on the crane); and

(v) the equipment that are used in areas where items important to safety are located to be seismically qualified;

(j) the safety support systems designed in a manner that guarantees the availability of the fundamental safety functions in every installation state;

(k) where normal services are provided from external sources, backup safety support systems are also made available on the site;

(l) the design incorporates emergency safety support systems to cope with the possibility of loss of normal service and, where applicable, concurrent loss of backup systems;

(m) the systems that provide normal services, backup services and emergency services shall have

(i) sufficient capacity to meet the load requirements of the systems that perform the fundamental safety functions; and

(ii) availability and reliability that is commensurate with the systems to which they supply the service;

(n) the emergency support systems are

(i) independent of normal and backup systems;

(ii) provide continuity of the service until long term, normal or backup service is re-established;

(iii) have a capacity margin that allows for future increases in demand; and

(iv) testable under design load conditions.

Fire Safety

30. An authorised person shall ensure that

(a) fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, are provided throughout the nuclear installation, with due account taken of the results of the fire hazard analysis;

(b) the fire extinguishing systems are capable of automatic actuation where appropriate and are designed and located to ensure that their rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety;

(c) fire detection systems are designed to provide information promptly to operating personnel on the location and spread of fires that start;

(d) fire detection systems and fire extinguishing systems that are necessary to protect against a possible fire after a postulated initiating event are appropriately qualified to resist the effects of the postulated initiating event;

(e) the design of the installation, including that of external buildings and systems, structures and components integral to installation operation, make provisions for fire safety;

(f) for fire protection, systems, structures and components important to safety is designed and located to minimize the probability and effect of fires and explosions consistent with other safety requirements;

(g) non-combustible and heat resistant materials are used wherever practicable throughout the unit, particularly in locations including the containment and control room;

(h) fire detection and fighting systems of appropriate capacity and capability are provided and designed to minimize the adverse effects of fires on systems, structures and components important to safety; and

(i) firefighting systems are designed in a manner that guarantees that their rupture or inadvertent operation does not significantly impair the safety capability of the systems, structures and components

Seismic Qualification

31. An authorised person shall ensure that

(a) the seismic qualification of systems, structures and components are aligned with the requirements of Ghanaian national or equivalent-international standards; and

(b) the design includes instrumentation for monitoring seismic activity at the site for the life of the installation.

In-service Testing, Maintenance, Repair, Inspection and Monitoring

32. An authorised person shall ensure that

(a) items important to safety for a nuclear installation are 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 every condition specified in their design basis;

(b) the plant layout permits activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring to be facilitated and performed in accordance with relevant national and international codes and standards;

(c) the activities under paragraph (b) are commensurate with the importance of the safety functions to be performed, and are performed without undue exposure of workers;

(d) where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems are designed for performing the tasks with no significant reduction in the reliability of performance of the safety functions;

(e) the provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown are included in the design to enable the tasks to be performed with no significant reduction in the reliability of performance of the safety functions;

(f) an systems, structures and components that has a shorter service lifetime than the installation lifetime is identified and described in the design documentation;

(g) the design provides facilities for monitoring chemical conditions of fluids, and of metallic and non-metallic materials and specifies the means for adding or modifying the chemical constituents of fluid streams;

(h) where 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 is provided that

(i) specifies other proven alternative or indirect methods including surveillance testing of reference items or use of verified and validated calculational methods; and

(ii) applies conservative safety margins or takes other appropriate precautions to compensate for possible unanticipated failures.

Qualification of Items Important to Safety

33. An authorised person shall ensure that

(a) a qualification programme for items important to safety is implemented to verify that the items important to safety at a nuclear installation 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;

(b) the environmental conditions considered in the qualification programme for items important to safety at a nuclear installation include the variations in ambient environmental conditions that are anticipated in the design basis for the plant;

(c) the qualification programme for items important to safety includes the consideration of ageing effects caused by environmental factors and embraces

conditions of vibration, irradiation, humidity or temperature over the expected service life of the items important to safety;

(d) where the items important to safety are subject to a natural external event and are required to perform a safety function during or after the event, the qualification programme replicates 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; and

(e) an environmental condition that could reasonably be anticipated and that could arise in specific operational states, including periodic testing of the containment leak rate, is included in the qualification programme.

Ageing Management

34. An authorised person shall ensure that

(a) the design takes into consideration the effects of ageing and wear on systems, structures and components;

(b) for systems, structures and components important to safety, the matters to be taken into consideration paragraph (a), include

(i) an assessment of design margins, taking into account the known ageing and wear mechanisms and potential degradation in normal operation, including the effects of testing and maintenance processes; and

(ii) provisions for monitoring, testing, sampling, and inspecting systems, structures and components to assess ageing mechanisms, verify predictions, and identify unanticipated response or degradation that may occur during operation as a result of ageing and wear.

Control of Access to the Installation

35. An authorised person shall ensure that the design provides for exclusion and removal of all foreign material and corrosion products that may have an impact on safety.

Transport and Packaging for Fuel and Radioactive Waste

36. An authorised person shall ensure that the installation design

(a) incorporates appropriate features to facilitate transport and handling of new fuel, used fuel, and radioactive waste; and

(b) features include installation access, as well as lifting and packaging capabilities.

Escape Routes from the Installation

37. An authorised person shall ensure that

(a) the design provides a sufficient number of safe escape routes that will be available in every installation state, including a seismic event;

(b) the routes to be provided under paragraph (a), are identified with clear and durable signage, emergency lighting, ventilation and other building services essential to their safe use; and

(c) the escape routes are subject to the relevant national requirements for radiation zoning, fire protection, industrial safety, and installation security, which include assurance of the ability to escape from containment regardless of the pressure in containment.

Systems of Communication at the Installation

38. An authorised person shall ensure that

(a) suitable alarm systems and means of communication are installed and made available at all times to warn and instruct each person in the installation and on the site; and

(b) the design provides diverse and easily accessible facilities for communication within the installation, in the immediate vicinity, and to off-site agencies, in accordance with the emergency response plan;

Human Factors

39. An authorised person shall ensure that

(1) the design include a human factor engineering programme.

(2) human factors are taken into account in the design of the nuclear facility in the planning of its operations, maintenance, modification, and decommissioning in a manner that support the high-quality implementation of the work and ensures that human activities do not endanger plant safety.

(3) human factors relating to safety be controlled with systematic procedures throughout the entire life cycle of the nuclear facility.

(4) the Human Factors Engineering (HFE) Programme are used to design the control, testing, review and maintenance of systems important to safety, with the following areas included:

(a) managing the HFE programme
(b) utilization of operating experience
(c) analysis and allocation of functions
(d) task analysis
(e) analysis of staff members and competences
(f) treatment of human task and actions significant to safety
(g) design of human-machine interface
(h) development of procedures
(i) development of training programmes
(j) verification and validation related to human factors.
(k) implementation of the design related to human factors.
(l) monitoring and assessment of human performance

(5) the relevant and proven systematic analysis techniques are used to address human factors issues within the design process.

(6) appropriate and clear distinction between the functions assigned to operating personnel and those assigned to automatic systems are facilitated by systematic consideration of human factors and the human-machine interface. This

consideration shall continue in an iterative way throughout the entire design process.

(7) the human–machine interface is designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times.

(8) the information necessary for the operator to make decisions to act is simply and unambiguously presented.

(9) verification and validation, including by the use of simulators, of features relating to human factors are included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.

(10) the need for operator intervention on a short time scale is kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act.

(11) the design for a nuclear installation shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.

(12) operating personnel who have gained operating experience in similar plants are, as far as is practicable, 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.

(13) the design,

(a) supports operating personnel in the fulfilment of their responsibilities and in the performance of their tasks;

(b) limits the likelihood and the effects of operating errors on safety; and

(c) gives 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.

(14) the operator is 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; and

(d) to determine both the need for and the time for manual initiation of the specified safety actions

(15) the design is 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.

(16) the design is 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.

(17) the design of workplaces and the working environment of the operating personnel is in accordance with ergonomic concepts.

(18) that for designing nuclear installation modifications, an HFE programme in accordance with Regulation 40 (3) above shall be prepared to the extent appropriate for the modification.

Decommissioning

40. An authorised person shall ensure that

(a) the design takes into account future installation decommissioning and dismantling activities;

(b) the materials for the construction and fabrication of installation components and structures are selected with the purpose of minimizing eventual quantities of radioactive waste and assisting decontamination;

(c) the installation layout is designed to facilitate access for decommissioning or dismantling activities; and

(d) the future potential requirements for storage of radioactive waste generated as a result of new facilities being built, or existing facilities being expanded are taken into account in the design.

Reactor Core Systems

41. (1) An authorised person shall ensure that for the reactor core,

(a) the design provides protection against deformations to reactor structures that have the potential to adversely affect the behaviour of the core or associated systems;

(b) the core and associated structures and cooling systems

(i) have the capability to withstand static and dynamic loading, including thermal expansion and contraction;

(ii) have the capability to withstand vibration including flow-induced and acoustic vibration;

(iii) maintain chemical compatibility;

(iv) meet the thermal material limits;

(v) meet the radiation damage limits; and

(vi) have the capability to withstand additional internal pressure due to fission products and the build-up of inert gases in fuel elements;

(c) the design facilitates the application of a guaranteed shutdown state;

(d) the design guarantees that

(i) the fission chain reaction is controlled during normal operation and anticipated operational occurrence; and

(ii) the maximum degree of positive reactivity and its maximum rate of increase by insertion in normal operation, Anticipated Operational Occurrence, and Design Basis Accident are limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained, and no significant damage will occur to the reactor core.

(2) The authorised person shall ensure that for fuel elements and assemblies,

(a) fuel assembly design includes the components in the assembly, and encompasses the fuel matrix, cladding, spacers, support plates, movable rods inside the assembly, among others;

(b) the fuel assembly design identifies the interfacing systems;

(c) a fuel assembly and the associated components are designed to maintain their structural integrity and to withstand the anticipated radiation levels and other conditions in the reactor core, in combination with each of the processes of deterioration that can occur in normal operation and anticipated operational occurrence;

(d) the long-term storage of irradiated fuel assemblies after discharge from the reactor are taken into account in the design;

(e) the fuel assembly design limits are established to include, as a minimum, limits on fuel power or temperature, limits on fuel burn-up, and limits on the permissible leakage of fission products in the reactor cooling system during operational states to ensure that the fuel is suitable for continued use;

(f) the design limits reflect the importance of preserving the cladding and fuel matrix;

(g) the design accounts for all known degradation mechanisms, with allowance being made for uncertainties in data, calculations, and fuel fabrication;

(h) fuel assemblies are designed in a manner that permits adequate inspection of their structures and component parts before and after irradiation;

(i) in design basis accident, the fuel assembly and its component parts remain in position with no distortion that would prevent effective post-accident core cooling or interfere with the actions of reactivity control devices or mechanisms;

(j) the fuel assembly design requirements in paragraph (a) to (i) are applied in the event of changes in fuel management strategy or in operating conditions over the lifetime of the installation;

(k) fuel assembly design and design limits reflect a verified and auditable knowledge base; and

(l) fuel assembly elements and fuel assemblies are designed in a manner that makes them capable of withstanding load and stresses associated with fuel handling.

(3) The authorised person shall ensure that for the control system

(a) the design provides the means for detecting levels and distributions of neutron flux in each region of the core during normal operation, including after shutdown and during and after refuelling states, and during anticipated operational occurrence;

(b) the reactor core control system has the capability to detect and intercept deviations from normal operation with the goal of preventing anticipated operational occurrence from escalating to accident conditions;

(c) the design provides adequate means to maintain both bulk and spatial power distributions within a predetermined range;

(d) the reactor control mechanisms limit the positive reactivity insertion rate to the level required to control reactivity changes and power manoeuvring;

(e) the control system, combined with the inherent characteristics of the reactor and the selected operating limits and conditions, minimize the need for shutdown action; and

(f) the control system and the inherent reactor characteristics keep the critical reactor parameters within the specified limits in the operational limits and conditions for a wide range of anticipated operational occurrence.

(4) The authorised person shall ensure that the processes of deterioration to be considered in design include those arising from

(a) differential expansion and deformation;

(b) external pressure of the coolant;

(c) additional internal pressure due to fission products and the build-up of helium in fuel elements;

(d) irradiation of fuel and other materials in the fuel assembly;

(e) variations in pressure and temperature resulting from variations in power demand;

(f) chemical effects;

(g) static and dynamic loading, including flow induced vibrations and mechanical vibrations; and

(h) variations in performance in relation to heat transfer that could result from distortion or chemical effects.

(5) The authorised person shall ensure that

(a) allowance is made for uncertainties in data, in calculations, and in manufacture.

(b) fuel design limits 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; and

(c) fuel elements and fuel assemblies are capable of withstanding the loads and stresses associated with fuel handling.

Reactor Coolant System

42. (1) An authorised person shall ensure that

(a) the design provides the reactor coolant system and its associated components and auxiliary systems with sufficient margin to ensure that the appropriate design limits of the reactor coolant pressure boundary in the operational limits and conditions are not exceeded in normal operation, anticipated operational occurrence, or design basis accident;

(b) the design prevents the operation of pressure relief devices from causing unacceptable releases of radioactive material from the plant, even in a design basis accident;

(c) the reactor coolant system is fitted with isolation devices to limit loss of radioactive coolant outside containment;

(d) the design reflects consideration of the conditions of the boundary material in normal operation, including maintenance and testing, anticipated operational occurrence, and design basis accident, as well as expected end-of-life properties affected by ageing mechanisms, the rate of deterioration, and the initial state of the components;

(e) the design of the moving components contained inside the reactor coolant pressure boundary, including pump impellers and valve parts, minimizes the likelihood of failure and associated consequential damage to other items of the reactor coolant system; and

(f) the design provides a system capable of detecting and monitoring leakage from the reactor coolant system.

(2) The authorised person shall ensure that

(a) for In-service Pressure Boundary Inspections

(i) the components of the reactor coolant pressure boundary are designed, manufactured, and arranged in a manner that permits adequate inspections and tests of the boundary throughout the lifetime of the plant; and

(ii) the design facilitates surveillance in order to determine the metallurgical conditions of materials for which metallurgical changes are anticipated;

(b) for Inventory,

(i) the design provides for control of coolant inventory and pressure; and

(ii) the inventory in the reactor coolant system and its associated systems are sufficient to support cool down from hot operating conditions to zero power cold conditions without the need for transfer from any other systems;

(c) the design provides for adequate removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel;

(d) for Removal of Residual Heat from Reactor Core,

(i) the design provides a means of removing residual heat from the reactor for all conditions of the Reactor Coolant System;

(ii) there is a backup for the removal of residual heat from the reactor and the backup is independent of the configuration in use;

(iii) the means of removing residual heat satisfies the reliability requirements on the assumptions of a single failure and the loss of off-site power, by incorporating suitable redundancy, diversity, and independence;

(iv) interconnections and isolation capabilities have a degree of reliability that is commensurate with system design requirements; and

(v) heat removal is at a rate that prevents the specified design limits of the fuel and the reactor coolant pressure boundary from being exceeded.

Steam Supply System

43. (1) An authorised person shall ensure that for Steam Lines,

(a) the steam piping up to and including the turbine generator governor valves and, where applicable, the steam generators, allow sufficient margin to ensure that the appropriate design limits of the pressure boundary are not exceeded in normal operation, an anticipated operational occurrence, or a design basis accident, taking into account the operation of control and safety systems;

(b) the main steam isolation valves are installed in each of the steam lines leading to the turbine, and located as close as practicable to the containment structure;

(c) where the main steam isolation valves have the function of preventing steam flow into containment, they are capable of closing under the conditions for which they are required to function;

(d) where the main steam isolation valves serve as a containment barrier, they satisfy the containment requirements that apply to those conditions for which they are required to function; and

(e) the main steam isolation valves are testable.

(2) The authorised person shall ensure that for

(a) Steam and Feed Water System Piping and Vessels,

(i) the piping and vessels are typically separated from electrical and control systems to the extent practicable; and

(ii) the auxiliary feed-water, boiler pressure control, and other auxiliary systems prevent the escalation of anticipated operational occurrence to accident conditions.

(b) Turbine Generators,

(i) the design provides over-speed protection systems for the turbine generators to minimize the probability of turbine disk failure leading to generation of missiles; and

(ii) the axes of the turbine generators are oriented in a manner that minimizes the potential of a missiles that results from a turbine break-up

to strike the containment, or strike other systems, structures and components important to safety.

Guaranteed Shutdown State and Means of Shutdown

44. (1) An authorised person shall ensure that

(a) the design organisation defines the guaranteed shutdown state that will support safe maintenance activities of the installation and measures for putting the reactor in a guaranteed shutdown state are incorporated into the design;

(b) the means to shut down the nuclear installation in operational states and in accident conditions is provided, and that the shutdown condition can be maintained even for the most reactive conditions of the installation;

(c) the design provides two independent means of preventing re-criticality from any pathway or mechanism during the guaranteed shutdown state;

(d) the shutdown margin for a guaranteed shutdown state allows the core, where possible without operator intervention, to remain subcritical for any credible changes in the core configuration and reactivity addition;

(e) where operator intervention is required to keep the reactor in a shutdown state, the feasibility, timeliness, and effectiveness of the intervention is demonstrated;

(f) the design provides for redundant shutdown systems;

(g) the design includes two separate, independent, and diverse means of shutting down the reactor;

(h) at least one means of shutdown is independently capable of quickly rendering the nuclear reactor sub-critical from normal operation, in anticipated operational occurrence and in design basis accident and maintaining the reactor sub-critical by an adequate margin, on the assumption of a single failure and with high reliability for even the most reactive conditions of the core.

(i) redundancy is provided in the fast-acting means of shutdown, if in the event of the failure of the established means for reactivity control during any anticipated operational occurrence or design basis accident, the inherent core characteristics are unable to maintain the reactor within specified limits;

(j) while resetting the means of shutdown, the maximum degree of positive reactivity and the maximum rate of increase are within the capacity of the reactor control system; and

(k) the effectiveness of the means of shutdown encompassing speed of action and shutdown margin, does not exceed the specified limits, and the possibility of re-criticality or reactivity excursion following a postulated initiating event is minimised.

(2) The authorised person shall ensure that

(a) for reactor trip parameters,

(i) the design organization specifies the derived acceptance criteria for effectiveness for anticipated operational occurrence and design basis accident;

(ii) the design organisation performs a safety analysis to demonstrate the effectiveness of the means of shutdown;

(b) for each credited means of shutdown, the design specifies a direct trip parameter to initiate reactor shutdown for anticipated operational occurrence and design basis accident in time to meet the respective derived acceptance criteria and where a direct trip parameter does not exist for an established means, there are two diverse trip parameters specified for the purpose;

(c) for anticipated operational occurrence and design basis accident., there are at least two diverse trip parameters unless it can be shown that failure to trip will not lead to unacceptable consequences;

(d) the design organisation provides additional trip parameters where necessary to close any gap in trip coverage for any operating condition, that encompasses power and temperature, among other similar elements, within the operational limits and conditions;

(e) the extent of trip coverage provided by the available parameters are documented for the entire spectrum of failures for each set of postulated initiating event;

(f) an assessment of the accuracy and the potential failure modes of the trip parameters are provided in the design documentation; and

(g) for the purpose of reliability,

(i) the design permits demonstration to be conducted to establish that each means of shutdown is being operated and maintained; and

(ii) the design organisation provides a schedule for periodic testing of the systems and their components.

(3) The authorised person shall ensure that for monitoring and operator action,

(a) the design permits automatic shutdown without operator capability to prevent its actuation;

(b) the design minimises the need for manual shutdown actuation; and

(c) the means for monitoring shutdown status and manual actuation are provided in the main control room.

Use of Computer-Based Equipment in Systems Important to Safety

45. An authorised person shall ensure that

(a) where a system important to safety at the nuclear installation is dependent upon computer-based equipment, appropriate standards and practices for the development and testing of the computer hardware and software are established and implemented in accordance with a quality management system, throughout the service life of the system, and in particular throughout the software development cycle;

(b) for a computer-based equipment in a safety system or safety related system,

(i) a high quality of, and best practices for, hardware and software are used, in accordance with the importance of the system to safety;

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

(iii) an assessment of the equipment is undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability;

(iv) 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 are provided;

(v) common cause failures deriving from software are taken into consideration; and

(vi) protection is provided against accidental disruption of, or deliberate interference with, system operation.

Emergency Core Cooling System

46. An authorised person shall ensure that

(a) the means of cooling the reactor core is provided to restore and maintain cooling of the fuel under accident conditions at the nuclear installation, even if the integrity of the pressure boundary of the primary coolant system is not maintained;

(b) the means provided for cooling of the reactor core

(i) prevent the limiting parameters for the cladding or for integrity of the fuel including the temperature from being exceeded;

(ii) enable possible chemical reactions to be kept to an acceptable level;

(iii) effectively compensates for possible changes in the fuel and in the internal geometry of the reactor core; and

(iv) guarantee a sufficient time for cooling;

(c) design features, including leak detection systems, appropriate interconnections and capabilities for isolation and suitable redundancy and diversity are provided to fulfil the requirements of paragraph (b), with adequate reliability for each postulated initiating event;

(d) water-cooled nuclear installations with thermal power above five megawatts-5MW- are equipped with an emergency core cooling system;

(e) the design provides for safety support systems for the emergency core cooling system;

(f) the design takes into account the effect on core reactivity of the mixing of emergency core cooling system water with reactor coolant water, including possible mixing due to in-leakage;

(g) the emergency core cooling system recovery flow path is devoid of debris or other material which can create an impediment to the recovery of coolant following a loss of coolant accident;

(h) maintenance and reliability testing of the emergency core cooling system is carried out without a reduction in the effectiveness of the system below the Operational limits and conditions;

(i) the emergency core cooling system components that may contain radioactive material are located inside containment or in an extension of containment; and

(j) the inadvertent operation of the emergency core cooling system or a part of the emergency core cooling system does not have any detrimental effect on plant safety.

Containment and Confinement

47. (1) An authorised person shall ensure that

(a) each nuclear installation for which that authorised person is responsible is installed within a containment or confinement structure;

(b) the containment system is designed for anticipated operational occurrence, design basis accident and design extension conditions;

(c) the containment includes complementary design features, which are subject to the design expectations as approved by the Authority;

(d) the containment structure is designed to fulfil the following safety functions at the nuclear installation:

(i) confine radioactive substances in operational states and in accident conditions;

(ii) protect the reactor against natural external events and human induced events; and

(iii) provide radiation shielding in operational states and accident conditions;

(e) the containment is designed in a manner that restricts any radioactive release from the nuclear installation to the environment to

(i) as low as reasonably achievable;

(ii) below the authorised limits on discharges in operational states; and

(iii) below acceptable limits in accident conditions;

(f) the containment structure and the systems and components that affect the leak-tightness of the containment system are designed and constructed to enable the leak rate to be tested

(i) after every penetration through the containment have been installed;

(ii) during the operating lifetime of the plant; and

(iii) at the containment design pressure;

(g) the design includes a clearly defined continuous leak-tight containment envelope;

(h) the boundaries in 44(2) are defined for all conditions that could exist in the operation or maintenance of the reactor, or after an accident;

(i) each piping that is part of the main or backup reactor coolant systems are entirely within the main containment structure, or in a containment extension;

(j) the containment design incorporates systems to assist in controlling internal pressure and the release of radioactive material to the environment after an accident;

(k) the independence of the compressed air system is demonstrated when the containment design includes the use of compressed air or non-condensable gas systems in response to a design basis accident;

(l) the design organisation identifies where and when the containment boundary is required to provide shielding for people and equipment;

(2) The authorised person shall ensure that for the strength of the containment structure,

(a) sufficient margins of safety are provided, based on potential internal over-pressures, under pressures, temperatures, dynamic effects including missile generation, and reaction-forces anticipated to result in the event of design basis accident;

(b) the strength margins are applied to access openings, penetrations, and isolation valves, and to the containment heat removal system;

(c) the positive and negative design pressures within each part of the containment boundary include the highest and lowest pressures that could be generated in the respective parts as a result of any Design basis accident;

(d) the containment structure protects the systems and equipment important to safety;

(e) the design supports the maintenance of full functionality after a design basis earthquake of all parts of the containment system identified in the safety analysis; and

(f) the containment structure is subjected to pressure testing at a specified pressure to demonstrate structural integrity before plant operation commences and throughout the lifetime of the plant.

(3) The authorised person shall ensure that

(a) for Leakage Rate Limits,

(i) the design leakage rate limit is below the safety leakage rate limit;

(ii) the design leakage rate limit is as low as is practicably attainable;

(iii) the design leakage rate limit is consistent with state-of-the-art design practices approved by the Authority;

(b) for Containment Penetrations,

(i) the number of penetrations through the containment are kept to a minimum and the penetrations satisfy the same design requirements as the containment structure itself

(ii) the penetrations are protected against reaction forces caused by pipe movement or accidental loads including those due to missiles caused by external or internal events, jet forces and pipe whip;

(iii) the penetrations are designed to allow for periodic inspection; and

(iv) resilient seals used with penetrations, allow for leak testing at the containment design pressure;

(c) for Containment Isolation,

(i) each line that penetrates the containment at the nuclear installation as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere is automatically and reliably sealable in the event of an accident in which the leak-tightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits;

(ii) each line that penetrates the containment as part of the reactor coolant pressure boundary and each line that is connected directly to the containment atmosphere is fitted with at least two adequate containment isolation valves or check valves arranged in series and provided with a suitable leak detection system;

(iii) each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere has at least one adequate containment isolation valve;

(iv) a containment isolation valve is located outside the containment and as close to the containment as is practicable;

(v) each automatic isolation valve is positioned to provide the greatest safety upon loss of actuating power;

(vi) a piping system that penetrates the containment system shall have isolation devices with redundancy, reliability, and independent actuation and with the capability of being periodically tested; and

(vii) manual isolation valves possess locking or continuous monitoring capability;

(d) for Reactor Coolant System Auxiliaries that Penetrate Containment,

(i) each auxiliary line that is connected to the reactor coolant pressure boundary, and that penetrates the containment structure, includes two isolation valves in series;

(ii) to the extent practicable, penetrations are designed to allow individual testing of each penetration;

(iii) the design provides for ready and reliable detection of any significant breach of the containment envelope;

(iv) where the valves provide isolation of the heat transport system during normal operation, both valves are kept in the closed position;

(v) a system directly connected to the reactor coolant system that may be open during normal operation is subject to the same isolation

expectations as the normally closed system, with the exception that manual isolating valves inside the containment structure will not be used; and

(vi) at least one of the two isolation valves is either automatic or powered, and operable from the main and secondary control rooms.

(4) The authorised person shall ensure that for any piping outside of containment that could contain radioactivity from the reactor core,

(a) the design parameters are the same as those for a piping extension to containment, and are subject to the requirements for metal penetrations of containment;

(b) each piping and each piping component that is open to the containment atmosphere is designed for a pressure greater than the containment design pressure;

(c) each piping and piping component is housed in a confinement structure that prevents leakage of radioactivity to the environment and to adjacent structures; and

(d) the housing includes detection capability for leakage of radioactivity and the capability to return the radioactivity to the flow path.

(5) The authorised person shall ensure that

(a) for systems that are connected to a containment atmosphere, each line that connects directly to the containment atmosphere and penetrates the containment structure but is not part of a closed system is provided with two isolation barriers

(i) that have two automatic isolation valves in series for lines that may be open to the containment atmosphere;

(ii) that have two closed isolation valves in series for lines that are normally closed to the containment atmosphere; and

(iii) to which the line up, including the second valve is part of the containment envelope;

(b) for Closed Systems,

(i) the closed piping service systems have at least one single isolation valve on each line penetrating the containment, with the valve being located outside of, but as close as practicable to, the containment structure;

(ii) where failure of a closed loop is assumed to be a Postulated initiating event or the result of a postulated initiating event, the isolations for reactor coolant system auxiliaries in 44(2) are applied;

(iii) closed piping service systems inside or outside the containment structure that form part of the containment envelope are not further isolated if they meet the applicable service piping standards and codes; and can be continuously monitored for leaks;

(c) for Containment Air Locks,

(i) personnel access to the containment is through airlocks that are equipped with doors that are interlocked to ensure that at least one of the doors is closed during normal operation, anticipated operational occurrence, and design basis accident;

(ii) where provision is made for entry of personnel for surveillance or maintenance purposes during normal operation, the design specifies provisions for personnel safety, including emergency egress and equipment air locks;

(iii) containment openings for the movement of equipment or material through the containment is designed to be closed quickly and reliably in the event that isolation of the containment is required;

(iv) the design provides for ample flow routes between separate compartments inside the containment;

(v) the openings between compartments are large enough to prevent significant pressure differentials that may cause damage to load bearing and safety systems during anticipated operational occurrence and design basis event;

(d) for the Internal Structures of the Containment,

(i) the design provides for ample flow routes between separate compartments inside the containment;

(ii) the openings between compartments are large enough to prevent significant pressure differentials that may cause damage to load bearing and safety systems during Anticipated operational occurrence and Design basis accident;

(iii) the design of internal structures takes into consideration any hydrogen control strategy, and assist in the effectiveness of that strategy;

(e) for control of containment conditions,

(i) provision is made to control the pressure and temperature in the containment at the nuclear installation 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;

(ii) the design provides for sufficient flow routes between separate compartments inside the containment;

(iii) the cross-sections of openings between compartments are of dimensions that prevents the pressure differentials that occur during pressure equalization in accident conditions from resulting in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions;

(iv) the capability to remove heat from the containment is provided for, 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;

(v) the systems that perform the function of removal of heat from the containment are sufficiently reliable and redundant to guarantee the performance of this function;

(vi) the design makes provision to prevent the loss of the structural integrity of the containment in each plant state, without the possibility of an early radioactive release or a large radioactive release;

(vii) the design includes features that enable the safe use of non-permanent equipment for restoring the capability to remove heat from the containment;

(viii) design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment are provided as necessary to reduce the amounts of fission products that could be released to the environment in accident conditions and 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; and

(ix) coverings, thermal insulations and coatings for components and structures within the containment system are carefully selected and methods for their application are 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.

Prevention of Harmful Interactions of Systems Important to Safety

48. An authorised person shall ensure that

(a) the potential for harmful interactions of systems important to safety at the nuclear installation that might be required to operate simultaneously are evaluated, and effects of any harmful interactions are prevented;

(b) in the analysis of the potential for harmful interactions of systems important to safety, due account is taken of physical interconnections and of the possible effects of the operation, mal-operation or malfunction 0f one system on the local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of a system or a component in functioning as intended; and

(c) where two fluid systems important to safety are interconnected and are operating at different pressures, either the systems are both designed to withstand the higher pressure, or provision is made to prevent the design pressure of the system operating at the lower pressure from being exceeded.

Control and Clean-up of the Containment Atmosphere

49. An authorised person shall ensure that

(a) the design provides systems to control the release of fission products, hydrogen, oxygen, and other substances into the reactor containment as is necessary, to

(i) reduce the amount of fission products that might be released to the environment during an accident; and

(ii) prevent deflagration or detonation that could jeopardize the integrity or leak tightness of the containment.

(c) the design supports the isolation of the sources of compressed air and other non-condensable gases into the containment atmosphere following an accident;

(d) the design, in the case of ingress of non-condensable gas resulting from a postulated initiating event, prevents the containment pressure from exceeding the design limit;

(e) the design provides for isolation of compressed air sources to prevent any bypass of containment;

(f) for coverings, coatings, and materials,

(i) the coverings and coatings for components and structures within the containment are carefully selected, and their methods of application specified; and

(ii) the choice of materials inside containment take into account the impact on post-accident containment conditions, including fission product behaviour, acidity, equipment fouling, radiolysis, fires, and other factors that may affect containment performance and integrity, and fission product release.

Severe Accidents

50. An authorised person shall ensure that

(a) the containment design is proven, through demonstration in a representative set of severe accidents, that are likely to occur as a result of core damage, to provide for a containment boundary that is capable of contributing to the reduction of radioactivity releases to allow sufficient time for the implementation of off-site emergency procedures;

(b) damage to the containment structure is limited to prevent uncontrolled releases of radioactivity, and to maintain the integrity of structures that support internal components;

(c) the ability of the containment system to withstand loads associated with severe accidents is demonstrated in the design documentation, through provision for the management of

(i) various heat sources, including residual heat, metal-water reactions, combustion of gases, and standing flames;

(ii) pressure control;

(iii) combustible gases;

(iv) sources of non-condensable gases;

(v) radioactive material leakage;

(vi) the effectiveness of isolation devices;

(vii) functionality and leak tightness of air locks and containment penetrations; and

(viii) the effects of an accident on the integrity and functionality of internal structures;

(d) the design organisation takes into consideration the incorporation of complementary design features and demonstrates the effectiveness of the design to

(i) prevent a containment melt-through or failure due to the thermal impact of the core debris;

(ii) facilitate cooling of the core debris; and

(iii) minimize generation of non-condensable gases and radioactive products.

Heat Transfer to an Ultimate Heat Sink

51. An authorised person shall ensure that

(a) the design includes systems for transferring residual heat from systems, structures and components important to safety to an ultimate heat sink;

(b) natural phenomena and human-induced events are taken into account in the design of the heat transfer systems and in the choice of diversity and redundancy; and

(c) the design extends the capability to transfer residual heat from the core to an ultimate heat sink so that, in the event of a severe accident, acceptable conditions can be maintained in systems, structures and components, radioactive materials can be confined and releases to the environment can be limited.

Emergency Heat Removal System

52. An authorised person shall ensure that

(a) the design includes an emergency heat removal system which provides for removal of residual heat;

(b) where the design of the plant requires an emergency heat removal system to mitigate the consequences of a design basis accident, then the emergency heat removal system is designed as a safety system;

(c) correct operation of the emergency heat removal system equipment after an accident is not made dependent on power supplies from the electrical grid or from the turbine generators associated with any reactor unit that is located on the same site as the reactor involved in the accident;

(d) where water is required for the emergency heat removal system, the design provides for the water to come from a source that is independent of normal supplies;

(e) the design supports maintenance and reliability testing without a reduction in system effectiveness below that required by the operational limits and conditions;

(f) as far as practicable, inadvertent operation of the emergency heat removal system, or of part of the emergency heat removal system, does not have a detrimental effect on installation safety; and

(g) where the fire water supply or system components are interconnected to the emergency heat removal system, the operation of one does not impair the operation of the other.

Emergency Power Supply

53. An authorised person shall ensure that

(a) the design of the nuclear installation includes 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;

(b) the nuclear installation design includes an alternate power source as part of the emergency power supply system to supply the necessary power in design extension conditions;

(c) the design specifications for the emergency power supply and for the alternate power source at the nuclear installation include the requirements for capability, availability, duration of the required power supply, capacity and continuity;

(d) the alternate power source is capable of supplying the necessary power to

(i) preserve the integrity of the reactor coolant system; and

(ii) 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;

(e) equipment that is necessary to mitigate the consequences of melting of the reactor core is capable of being supplied by any of the available power sources;

(f) the alternate power source is independent of and physically separated from the emergency power supply and the connection time of the alternate power supply is consistent with the depletion time of the battery;

(g) the emergency power supply system includes appropriate control, monitoring and testing facilities.

(h) the combined means to provide emergency power, including water, steam or gas turbines, diesel engines or batteries have the reliability and are of the type that are consistent with the requirements of the safety systems to be supplied with power, and their functional capability are testable;

(i) the design basis for a diesel engine or other prime mover that provides emergency power supply to items important to safety include

(i) the capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period;

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

(iii) the auxiliary systems of the prime mover including coolant systems;

(j) in the event of loss of alternating current power sources, there is continuous supply of power to equipment that monitor key plant parameters and equipment used in completing short term actions necessary for safety;

(k) the design of the emergency power supply system includes features that enable the safe use of non-permanent equipment used in restoring electrical power supply; and

(l) the emergency power supply system is tested under load conditions representing full load demand.

Control Facilities

54. (1) An authorised person shall ensure that the design

(a) provides for a main control room, from which the installation can be safely operated, and from which measures can be taken to maintain the installation in a safe state or to bring it back into a safe state after the onset of anticipated operational occurrence, design basis event, and, to the extent practicable, following a design extension conditions; and

(b) identifies events both internal and external to the main control room that may pose a direct threat to the continued operation of the installation and provides practicable measures to minimize the effects of these events.

(2) The authorised person shall ensure that

(a) the safety functions initiated by automatic control logic in response to an accident can be initiated manually from the main and secondary control rooms;

(b) the layout of the controls and instrumentation, and the mode and format used to present information provide

(i) operating personnel with an adequate overall picture of the status and performance of the installation; and

(ii) the necessary information to support operator actions;

(c) the design of the main control room enables

(i) appropriate lighting levels to be kept and thermal environment to be maintained; and

(ii) noise levels to be minimized to applicable standards and codes;

(d) the design of the main control room takes into account ergonomic factors, including hardwired display panels and computer displays, which are as user friendly as possible, to provide both physical and visual accessibility to the controls and the displays, without adverse impact on health and comfort;

(e) cabling for the instrumentation and control equipment in the main control room are arranged in a manner that prevents fire in the secondary control room from disabling the equipment in the main control room;

(f) the design provides visual and, where appropriate, audible indications of installation states and processes that have deviated from normal operation and that could affect safety;

(g) the design allows for the display of information needed to monitor the effects of the automatic actions of the control, safety, and safety support systems; and

(h) the main control room is provided with secure communication channels to the emergency support centre and to off-site emergency response organizations, and that the communication channels allow for extended operating periods.

(3) The authorised person shall ensure that for the Safety Parameter Display System,

(a) the main control room contains a safety parameter display system that presents sufficient information on safety-critical parameters for the diagnosis and mitigation of design basis accident and design extension condition;

(b) the safety parameter display system has the capability to

(i) display safety critical parameters within the full range expected in normal operation and during accidents;

(ii) track data trends;

(iii) indicate when a process or a safety limit is being approached or exceeded; and

(iv) display the status of safety systems.

(c) the design and installation permit the same information to be made available in a secure manner to the emergency support centre;

(d) the system is integrated and harmonized with the overall control room human-system interface design;

(4) The authorised person shall ensure that the design

(a) provides for a secondary control room that is physically and electrically separate from the main control room, and from which the installation can be placed and kept in a safe shutdown state when the ability to perform essential safety functions from the main control room is lost;

(b) identifies the events that may pose a direct threat to the continued operation of the main control room and the secondary control room; and

(c) of the main control room and the secondary control room guarantees that no event can simultaneously affect both control rooms to the extent that the essential safety functions cannot be performed.

(5) The authorised person shall ensure that

(a) for any postulated initiating event, at least one control room is habitable, and accessible by means of a qualified route;

(b) instrumentation, control equipment, and displays are available in the secondary control room, to enable

(i) the essential safety functions to be performed;

(ii) the essential installation variables to be monitored, and operator actions to be supported;

(c) safety functions initiated by automatic control logic in response to an accident can be initiated manually from both the main control room and the secondary control room;

(d) the design of the secondary control room enables

(i) appropriate lighting levels and thermal environment to be maintained; and

(ii) noise levels to be aligned with applicable standards and codes;

(e) ergonomic factors apply to the design of the secondary control room in a manner that enables physical and visual access to controls and displays, including hardwired display panels and computerized displays that are user friendly as possible, without adverse impact on health and comfort;

(f) the cabling for the instrumentation and control equipment in the secondary control room is constructed in a manner that prevents fire in the main control room from disabling the equipment in the secondary control room;

(g) the secondary control room is equipped with a safety parameter display system similar to that in the main control room and that as a minimum, provides the information required to facilitate the management of the reactor when the main control room is uninhabitable;

(h) the secondary control room is provided with secure communication channels to the emergency support centre and to off-site emergency response organisations; and

(i) the secondary control room allows for extended operating periods.

(6) The authorised person shall ensure that

(a) the design provides for an emergency support centre that

(i) is separate from the installation control rooms;

(ii) is to be used by the emergency support staff in the event of an emergency;

(iii) maintains appropriate lighting levels and thermal environment;

(iv) has noise levels which are minimized to applicable standards and codes; and

(v) includes a safety parameter display system similar to those in the main control room and in the secondary control room;

(b) information about the radiological conditions in the installation and its immediate surroundings, and about meteorological conditions in the vicinity of the installation, are accessible from the emergency support centre;

(c) the emergency support centre includes a secure means of communication with

(i) the main control room;

(ii) the secondary control room;

(iii) other important points in the installation; and

(iv) on-site and off-site emergency response organizations.

(d) the design enables the emergency support centre,

(i) to provide for the protection of occupants over protracted periods from the hazards resulting from a severe accident; and

(ii) to be equipped with adequate facilities to allow extended operating periods.

(7) The authorised person shall ensure that

(a) where an operator action is required for actuation of a safety system or safety support system equipment,

(i) there are clear, well-defined, validated, and readily available operating procedures that identify the necessary actions; and

(ii) there is instrumentation in the control rooms to provide clear and unambiguous indication of the necessity for operator action;

(b) where the operator action is required

(i) inside the main control room, there is at least fifteen minutes available between the time the need for the action arises and the time the action is to be taken; and

(ii) outside the main control there is at least thirty minutes available between the time the need for the action arises and the time the action is to be taken;

(c) provision is made for the use of alternative action times, where justified, with due allowance made for the complexity of the action to be taken, and for the time needed for the activities required in diagnosing the event and accessing to the remote station; and

(d) for automatically initiated safety systems and control logic actions, the design facilitates backup manual initiation from inside the appropriate control room.

Waste Treatment and Control

55. (1) An authorised person shall ensure that the design includes

(a) provisions to treat liquid and gaseous effluents in a manner that will keep the quantities and concentrations of discharged contaminants within prescribed limits in the *Basic Ionising Radiation Control Regulations*, and that will support application of the as low as reasonably achievable principle; and

(b) adequate provision for the safe on-site handling and storage of radioactive and non-radioactive wastes for a period of time consistent with options for off-site management or disposal.

(2) The authorised person shall ensure that

(a) for control of liquid releases to the environment,

(i) the design provides a suitable means for the control of the releases to the environment in a manner that conforms with the as low as reasonably achievable principle; and

(ii) the means for the control of release includes a liquid waste management system of sufficient capacity to collect, hold, mix, pump, test, treat, and sample liquid waste before discharge, taking into account, expected waste and accidental spills or discharges;

(b) for control of airborne material within the installation, the design includes gaseous waste management systems capable of

(i) controlling gaseous contaminants so as to conform to the as low as reasonably achievable principle and keeping concentrations within the prescribed limits;

(ii) collecting potentially active gases, vapours, and airborne particulates for monitoring;

(iii) passing potentially active gases, vapours, and airborne particulates through pre-filters, absolute filters, charcoal filters, or high efficiency particulate air filters where applicable; and

(iv) delaying releases of potential sources of noble gases by way of an off-gas system of sufficient capacity;

(c) the design, in respect of control of airborne material, provides a ventilation system with an appropriate filtration system capable of

(i) preventing unacceptable dispersion of all airborne contaminants within the plant;

(ii) reducing the concentration of airborne radioactive substances to levels compatible with the need for access to each particular area;

(iii) keeping the level of airborne radioactive substances in the plant below prescribed limits, in compliance with the as low as reasonably achievable principle, during normal operation; and

(iv) ventilating rooms containing inert or noxious gases without impairing the capability to control radioactive releases;

(d) for the purpose of control of gaseous releases to the environment the ventilation system includes filtration to

(i) control the release of gaseous contaminants and hazardous substances to the environment;

(ii) ensure conformation to the as low as reasonably achievable principle; and

(iii) maintain airborne contaminants within prescribed limits.

(e) in respect of the control of gaseous releases the filtration system,

(i) has the capability to reliably achieve the necessary retention factors under the expected prevailing conditions; and

(ii) is designed in a manner that facilitates appropriate testing of efficiency.

Fuel Handling and Storage

56. (1) An authorised person shall ensure that

(a) for handling and storage of non-irradiated fuel, the design of the fuel handling and storage systems provide for nuclear criticality safety through:

(i) the maintenance of an approved sub-criticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions,

(ii) the minimising of on-site consequences to personnel of postulated criticality accidents, and

(iii) the mitigation of off-site consequences of postulated criticality accidents;

(b) the design of the fuel handling and storage systems

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

(ii) permit inspection of non-irradiated fuel;

(iii) prevent loss of or damage to the fuel; and

(iv) satisfy the requirements of the *Safeguards Regulations* for recording and reporting accountancy data, and for monitoring flows and inventories related to non-irradiated fuel containing fissile material.

(c) in respect of handling and storage of irradiated fuel, the design of the handling and storage systems provide for nuclear criticality through

(i) the maintenance of an approved sub-criticality margin by physical means or processes, preferably by the use of geometrically safe configurations, under both normal and credible abnormal conditions;

(ii) the minimizing of on-site consequences to personnel of postulated criticality accidents, and

(iii) the mitigation of off-site consequences of postulated criticality accidents;

(d) the design of the handling and storage systems

(i) permit adequate heat removal under normal operation, anticipated operational occurrence, and design basis accident;

(ii) permit inspection of irradiated fuel;

(iii) permit periodic inspection and testing of components important to safety;

(iv) prevent the dropping of used fuel in transit;

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

(vi) prevent the inadvertent dropping of heavy objects and equipment on fuel assemblies;

(vii) permit inspection and safe storage of suspect or damaged fuel elements or fuel assemblies;

(viii) provide proper means for radiation protection;

(ix) adequately identify individual fuel modules;

(x) facilitate maintenance and decommissioning of the fuel storage and handling facilities;

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

(xii) enable the implementation of adequate operating and accounting procedures to prevent loss of fuel;

(xiii) include measures to prevent a direct threat or sabotage to irradiated fuel; and

(xiv) satisfy national safeguards requirements for recording and reporting accountancy data, and for monitoring flows and inventories related to irradiated fuel containing fissile material.

(e) a design for a water pool used for fuel storage makes provisions for

(i) controlling the chemistry and activity of any water in which irradiated fuel is handled or stored;

(ii) monitoring and controlling the water level in the fuel storage pool;

(iii) detecting leakage; and

(iv) preventing the pool from emptying in the event of a pipe break.

(2) the authorised person shall ensure that for the detection of failed fuel, the design provides a means for reliable detection of fuel defects in the reactor, and subsequent removal of failed fuel if action levels are exceeded.

Radiation Protection

57. An authorised person shall ensure that

(a) provision is made to maintain doses to operating personnel at the nuclear installation below the dose limits and to keep doses as low as reasonably achievable, taking into consideration the relevant dose constraints;

(b) materials used in the manufacture of structures, systems and components are selected on the basis of their capacity to minimize activation as far as is reasonably practicable.

(c) for the purposes of radiation protection, provision is made for preventing the release or the dispersion of radioactive substances, radioactive waste and contamination at the plant;

(d) the plant layout adequately controls access of operating personnel to areas with radiation hazards and areas of possible contamination and prevents or reduces exposures and contamination by means of the control and by means of a ventilation system equipped with filtration capabilities;

(e) the plant is divided into zones that are related to

(i) their expected occupancy;

(ii) radiation levels and contamination levels in operational states including refuelling, maintenance and inspection; and

(iii) potential radiation levels and contamination levels in accident conditions;

(f) shielding is provided to prevent or reduce radiation exposure;

(g) the plant layout enables doses received by operating personnel during normal operation, refuelling, maintenance and inspection to be kept as low as reasonably achievable, and due account to be taken of the necessity for any special equipment to be provided to meet these requirements;

(h) plant equipment subject to frequent maintenance or manual operation are located in areas of low dose rate to reduce the exposure of workers;

(i) facilities are provided for the decontamination of operating personnel and plant equipment;

(j) equipment is provided at the nuclear installation 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;

(k) stationary dose rate meters are 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 that may require access to be allowed only for certain specified periods of time;

(l) stationary dose rate meters, which provide sufficient information in the control room or in the appropriate control position, are installed to indicate the general radiation levels at suitable plant locations in accident conditions, to enable operating personnel to initiate corrective actions where necessary;

(m) stationary monitors are 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 may necessitate protective measures;

(n) the stationary monitors required to be installed under paragraph (m), are installed in areas that are subject to contamination as a result of equipment failure or other unusual circumstances, and that they provide an indication in the control room or in other appropriate locations when a high activity concentration of radionuclides is detected;

(o) stationary equipment and laboratory facilities are 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;

(p) stationary equipment are provided for monitoring radioactive effluents and effluents with possible contamination prior to or during discharges from the plant to the environment;

(q) instruments for measuring surface contamination in the nature of stationary monitors, portal radiation monitors, and hand and foot monitors, are provided at the main exit points from controlled areas and supervised areas to facilitate the monitoring of operating personnel and equipment;

(r) facilities are provided for monitoring exposure and contamination of operating personnel and processes are established for assessing and for recording the cumulative doses to workers over time;

(s) processes are established to assess exposures and other radiological impacts, if any, in the vicinity of the plant, through environmental monitoring of dose rates or activity concentrations, with particular reference to

(i) exposure pathways to people, including the food chain;

(ii) radiological impacts, if any, on the local environment;

(iii) the possible buildup, and accumulation in the environment, of radioactive substances; and

(iv) the possibility of unauthorised routes for radioactive releases;

(t) the design and layout of the installation makes suitable provision to minimize exposure and contamination from all sources and provides an appropriate design for systems, structures and components to

(i) control access to the installation;

(ii) provide shielding from direct and scattered radiation;

(iii) monitor radiation levels; and

(iv) prevent radiation levels in operating areas from exceeding the prescribed limits, through the use of the shielding design;

(v) provide appropriate permanent layout and shielding of systems, structures and components containing radioactive materials through the use of the shielding design, and the use of temporary shielding for maintenance and inspection work;

(iv) provide for efficient operation, inspection, maintenance, replacement and for the limits of the amount of activated material and its build-up through the installation layout;

(v) to shield access routes, where needed;

(vi) enable operator access for actions credited for post-accident conditions;

(vii) minimize the movement of radioactive materials and the spread of contamination; and

(viii) minimize the generation of radioactive waste.

Interaction Between the Electrical Power Grid and the Plant

58. For a nuclear power plant, the authorised person shall ensure that the design of the plant prevents disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply from compromising the functionality of the items important to safety.

Safety Analysis Provisions

Safety Analysis

59. An authorised person shall ensure

(a) that a safety analysis of the installation that incorporates hazards analysis, deterministic safety analysis, and probabilistic safety assessment techniques is conducted to enable the challenges to safety at the various categories of installation states to be evaluated and assessed;

(b) that the safety analysis establishes and confirms the design basis for items important to safety and their links to initiating events and event sequences;

(c) that the design demonstrates the capability of the nuclear installation to comply with authorised limits on discharges with regard to radioactive releases and with the dose limits in every operational state, and is capable of meeting acceptable limits for accident conditions;

(d) that the nuclear installation as designed demonstrates the capability to comply with authorised limits on discharges with regard to radioactive releases and with the dose limits in every operational state, and is capable of meeting acceptable limits for accident conditions;

(e) that the safety analysis provides assurance that defence in depth has been implemented in the design of the plant;

(f) through the safety analysis that the design of the plant has adequately taken into consideration uncertainties and that adequate margins are available to avoid cliff-edge effects and early radioactive releases or large radioactive releases;

(g) that 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;

(h) that the first step of each part of the safety analysis identifies postulated initiating event, using a systematic methodology including failure modes and effects analysis; and

(i) postulated initiating event identification considers both direct and indirect events.

Analysis Objective

60. An authorised person shall ensure that the safety analysis

(a) establishes the design-basis requirements for parameters important to safety, and demonstrate the compliance of the installation design with the applicable expectations;

(b) reflects the as-built plant;

(c) demonstrates that the design can withstand and effectively respond to identified postulated initiating event;

(d) demonstrates the effectiveness of the safety systems and safety support systems;

(e) derives the operational limits and conditions for the plant, including

(i) operational limits and set points important to safety, and

(ii) allowable operating configurations, and constraints for operational procedures;

(f) establishes requirements for emergency response and accident management;

(g) determine post-accident environmental conditions, including radiation fields and worker doses, to confirm that operators are able to carry out the actions credited in the analysis;

(h) confirms that the dose and derived acceptance criteria are met for each anticipated operational occurrence and design basis accident; and

(i) demonstrates that every safety goals has been met.

Hazards Analysis

61. An authorised person shall ensure that

(a) a hazards analysis is conducted to demonstrate the ability of the design to effectively respond to credible common-cause events;

(b) the hazards analysis identifies

(i) applicable acceptance criteria, which is the success path criteria;

(ii) the hazardous materials in the installation and at the installation site;

(iii) the qualified mitigating systems, structures and components credited during and following the event-all non-qualified safety or safety support systems that are assumed to have failed, except in cases where their continued operation would result in more severe consequences;

(iv) operator actions and operating procedures for the event; and

(v) the installation or operating procedure parameters for which the event is limiting;

(c) the hazards analysis confirms that

(i) the installation design incorporates sufficient diversity and separation to cope with credible common-cause events;

(ii) credited systems, structures and components are qualified to survive and function during and after credible common-cause events, as applicable; and

(d) the hazards analysis guarantees through its findings that

(i) the installation can be brought to a safe shutdown state,

(ii) the integrity of the fuel in the reactor core can be maintained,

(iii) the integrity of the reactor coolant pressure boundary and containment can be maintained, and

(iv) safety-critical parameters can be monitored by the operator;

(e) the hazards analysis report includes

(i) the findings of the analysis and the basis for those findings;

(ii) a general description of the physical characteristics of the installation that outlines the prevention and protection systems to be provided;

(iii) the list of safe shutdown equipment;

(iv) definition and description of the characteristics associated with hazards for each area that contains hazardous materials;

(v) description of the performance criteria for detection systems, alarm systems, and mitigation systems, including requirements comprising seismic or environmental qualification;

(vi) description of the control and operating room areas and the protection systems provided for these areas, including additional facilities for maintenance and operating personnel;

(vii) description of the operator actions and operating procedures of importance to the given analysis;

(viii) identification of the installation parameters for which the event is limiting;

(ix) explanation for the inspection, testing, and maintenance parameters needed to protect system integrity; and

(x) definition of the emergency planning and coordination requirements for effective mitigation, including any necessary measures to compensate for the failure or inoperability of any active or passive protection system or feature.

Deterministic Safety Analysis

62. An authorised person shall ensure that the deterministic safety analysis

(a) establishes and confirms the design bases for all items important to safety;

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

(c) analyses and evaluates event sequences that result from postulated initiating events, to confirm the qualification requirements;

(d) compares the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;

(e) demonstrates that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator;

(f) demonstrates 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; and

(g) confirms that operational limits and conditions comply with the assumptions and intent of the design for normal operation of the installation;

Probabilistic Safety Analysis

63. An authorised person shall ensure that

(a) the design takes due account of the probabilistic safety analysis of the installation for each mode of operation and for each installation state, including shutdown, with particular reference to

(i) establishing that a balanced design has been achieved and 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;

(ii) providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions in the nature of cliff edge effects are prevented; and

(iii) comparing the results of the analysis with the acceptance criteria for risk where these have been specified;

(b) the probabilistic safety analysis includes an assessment that takes into consideration internal and external events and each mode of operation;

(c) measures that are consistent with the management system of the authorised person are implemented to ensure the quality of the probabilistic safety analysis, including data and information used in the analysis;

(d) the probabilistic safety analysis based on realistic analysis using state-of-the-art tools, methods and data to calculate the radiological release and consequences of spectrum of events ranging from those of high anticipated frequency through those of rare anticipated frequency, as in severe reactor accidents;

(e) uncertainties are addressed in conformity to internationally recognised probabilistic safety analysis standard and best practice;

(f) a high-quality probabilistic safety analysis is performed and used to complement the nuclear facility design, construction, operation and safety analysis;

(g) the probabilistic safety analysis

(i) is based upon the design of the nuclear installation and site-specific information;

(ii) assesses accident sequences leading up to and including reactor core damage and loss of containment integrity, and the corresponding quantity and composition of radioactive material available for release to the environment which is Level 2 of the probabilistic safety analysis;

(iii) is used to assess the safety of the nuclear facility;

(iv) establishes performance goals for safety significant systems, structures and components

(v) compare the nuclear installation risk with the probabilistic targets from the Authority; and

(vi) result includes identification of the most safety significant event sequences, human actions, plant configurations, new information, issues and changes to the approved referenced plant design.

(2) The Authorised person shall

(a) update the probabilistic safety analysis over the life of the nuclear installation, at appropriate intervals, to reflect the operating experience, design modifications, and other changes reflecting the as-built and as-operated plant that could affect the probabilistic safety analysis;

(b) ensure that the results from the updated probabilistic safety analysis are used to incorporate current probabilistic safety analysis insight in the nuclear installation design and operational programmes;

(c) conduct a peer review of the probabilistic safety analysis when it is initially developed and at each major update and present a summary of the results of the peer review to the Authority;

(d) ensure that the peer review

(i) is performed by qualified personnel and that each member of the peer review team has the technical expertise in the specific methods used to perform the probabilistic safety analysis elements; and

(ii) outcome compares the probabilistic safety analysis against the characteristics and attributes, documents the results, and identifies both strengths and weaknesses of the probabilistic safety analysis;

(e) ensure that the probabilistic safety analysis and related documentation are updated and made available at the site of the authorised person, for the inspection and audit of the Authority upon request;

(f) provide a summary of the probabilistic safety analysis results to the Authority in connection with the application for a construction licence and for an operating licence;

(g) ensure that the summary required under paragraph (f) includes an overview of the probabilistic safety analysis results, conclusions and an explanation of how the results and the conclusions have been utilised to complement design, construction and operation;

(h) ensure that the summary describes the results of the peer review process; and

(i) provide to the Authority at the time of a major probabilistic safety analysis update, a summary report describing the update, the reasons for the update and how it is using the results.

Other Miscellaneous Provisions

Environmental Protection and Mitigation

64. An authorised person shall ensure that in the design of facilities for

(a) environmental protection,

(i) adequate provision is made in the design to protect the environment and to mitigate the impact of the installation on the environment; and

(ii) a systematic approach is used to assess the potential bio-physical environmental effects of the installation on the environment, and the effects of the environment on the installation;

(b) the release of nuclear and hazardous substances,

(i) the design demonstrates through processes, monitoring, control, prevention, and mitigation measures, that the releases of nuclear and hazardous substances will conform to the as low as reasonably achievable principle; and

(ii) the life cycle assessment identifies various sources of nuclear and hazardous substances in the design, operation, and decommissioning stages, along with their possible environmental impacts on human and non-human biota.

(c) the purpose of safe release of nuclear and hazardous substances takes into consideration,

(i) resource requirements for the installations, including fuel, energy, and water;

(ii) depletion of ground and surface water resources;

(iii) contamination of air, soil, and water resources;

(iv) nuclear and hazardous substances used;

(v) types of waste generated-gaseous, liquid and solid;

(vi) quantities of waste generated;

(vii) impact of cooling water intake on entrainment and impingement; and

(viii) impact of water output on the thermal regime of the receiving environment.

(d) technological options are considered in establishing design objectives for controlling and monitoring releases during start-up, normal operation, shutdown, and potential abnormal and emergency situations; and

(e) technological options for the design of cooling water systems take into consideration closed-cycle technology.

Nuclear Security

65. (1) A licensee shall, after the site approval, establish the preliminary security plan containing physical protection system design, training and qualification requirements for security personnel and contingency plan.

(2) The licensee shall ensure that

(a) the design of the physical protection system is based on unacceptable radiological consequences and high radiological consequences established in the *Nuclear Security Regulations* and relevant protection levels

(b) the physical protection system is designed taking into consideration the threat assessment or design basis threat;

(c) a list of codes and standards for the initial design of the physical protection system is agreed upon with the Authority;

(d) the physical protection system is designed based on a graded approach by identifying the level and effectiveness of physical protection measures that provide protection against unauthorized removal of nuclear or other radioactive material and sabotage;

(e) the design denies unauthorized access by persons to targets and equipment, and minimize opportunity of insiders; and

(f) the respective physical protection system procedures are submitted to the Authority for approval.

(3) The licensee shall design the physical protection system incorporating defense in depth and ensure that the design provides

(a) reliability that the failure of a single security component does not equate to the failure of the security element; and,

(b) balanced security to provide equivalent protection regardless of what path or scenario an adversary may employ.

Nuclear Safeguards

66. (1) An authorised person shall ensure that

(a) the nuclear installation is designed in a manner that enables nuclear material to be controlled and accounted for and the Authority and the International Atomic Energy Agency to independently verify the declarations made about that nuclear material;

(b) the design

(i) facilitates safeguards inspection activities;

(ii) minimizes the need for the Authority and the International Atomic Energy Agency inspectors to revisit the site for clarification of information collected during previous visits;

(iii) mitigates safeguards issues during off normal or unusual events; and

(iv) clarifies the location to install backup or emergency power and for how long this needs to be available.

(2) The authorised person shall submit the conceptual design to the Authority for evaluation of the safeguards considerations made in the design and shall

(a) at the subsystem design stage,

(i) make a preliminary definition of Material Balance Areas and Key Measurement Points, in consultation with the Authority;

(ii) assess whether the design supports the physical infrastructure necessary for safeguards instrumentation and equipment; and

(iii) perform an analysis to verify that no unmonitored opportunities for diversion or misuse exist;

(b) submit a Design Information Questionnaire at the final stage of the design to the Authority for review; and

(c) keep as-built or as-is design documentation up to date.

Penalties

67. A person who contravenes any of the provisions of these Regulations commits an offence and is liable to penalty provision in Regulation 80 of the *Basic Ionising Radiation Control Regulations*.

Appeals

68. A person who is not satisfied with a decision taken by the Authority may appeal in accordance with sections 81, 82, 83, 84 and 85 of the Nuclear Regulatory Authority Act, 2015 (Act 895).

Interpretation

69. In these regulations unless the context otherwise requires,

"accident" means an unintended event, and encompasses operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety;

"Anticipated operational occurrence" means an operational process that deviates from normal operation and which is expected to occur at least once during the operating lifetime of a facility but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions;

"best estimate" means an unbiased estimate obtained by the use of a mathematical model or calculation method to realistically predict plant behaviour and important parameters;

"combustion" means a chemical process that involves oxidation sufficient to produce heat or light.

"Common-Cause Failure" means a concurrent failure of two or more structures, systems or components due to a single specific event or cause, which may be in the nature of earthquakes, tornadoes, floods, and other natural phenomena, design deficiency, manufacturing flaws, operation and maintenance errors and human-induced destructive events;

"commissioning" means a process of activities intended to demonstrate that installed systems, structures, and components and equipment perform in accordance with their specifications and design intent before they are put into service;

“Complementary Design Feature” means a design feature outside of the design basis envelope that is introduced to cope with beyond design basis accidents, including severe accidents;

“confinement” means a continuous boundary without openings or penetrations which may be in the form of windows and that prevents the transport of gases or particulates out of the enclosed space;

“containment” means a confinement structure designed to maintain confinement at both high temperature and pressures and for which isolation valving on penetrations is permitted;

“conservatism” means use of assumptions, based on experience or indirect information, about a phenomena or behaviour of a system being at or near the limit of expectation, which increases safety margins or makes predictions regarding consequences more severe than if best-estimate assumptions had been made;

“core damage” means core degradation resulting from event sequences more severe than design basis accidents;

“crediting” means assuming the correct operation of systems, structures and components or correct operator action, as part of an analysis;

“critical groups” means a group of members of the public that is reasonably homogeneous with respect to its exposure for a given radiation source, and is typical of individuals receiving the highest effective dose or equivalent dose as applicable, from the given source;

“Design Basis Threat” means a set of malevolent acts that the Authority considers possible;

“design organization” means the organization responsible for preparation of the final detailed design of the plant to be built;

“design extension conditions” means postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in

accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits;

“Deterministic Safety Analysis” means an analysis of plant responses to an event which is performed using either conservative or best estimate , predetermined rules and assumptions and embraces those concerning the initial plant state, availability and performance of the plant systems, and operator actions;

“Direct Trip Parameter” means a value based on direct measurement of a specific challenge to the derived acceptance criteria and, if applicable, a direct measure of the event;

“diversity” means the presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common-cause failure;

“environment” means the components of the Earth, comprising

(a) land, water, and air, including all layers of the atmosphere;

(b) every organic and inorganic matter and living organism; and

(c) interacting natural systems that include components referred to in paragraphs (a) and (b);

“exclusion zone” means exclusion area means that area surrounding the reactor, in which the authorised person has the authority to determine all activities including exclusion or removal of personnel and property from the area;

“ex-Mission Time” means the duration of time within which a system or component is required to operate or be available to operate and fulfil its function following an event;

“external event” means events unconnected with the operation of a nuclear installation or the conduct of an activity which could have an effect on the safety of the nuclear installation;

“Fail-Safe Design” means design whose most probable failure modes do not result in a reduction of safety;

“fire” means a process of combustion characterized by heat emission and accompanied by smoke or flame, or both;

“Heat Sink” means a system or component that provides a path for heat-transfer from a source which may be heat generated in the fuel, to a large heat absorbing medium;

“Human Factors” means factors that influence human performance as it relates to the safety of the nuclear installation, including activities during design, construction, and commissioning, operation, maintenance and decommission independent

“systems” mean systems that do not share any components;

“internal event” means an event internal to the nuclear installation that results from human error or failure in a system, structure, or component;

“Jet Impact” means the potential internal hazard associated with high pressure fluid released from a pressure-retaining component;

“Leak-Before-Break” means a situation where leakage from a flaw is detected during normal operation, allowing the reactor to be shut down and depressurized before the flaw grows to the critical size for rupture;

“malevolent act” means an illegal action or an action that is committed with the intent of causing wrongful harm.

“Missile Generation” means the internal hazard associated with the sudden high-speed propulsion of debris;

“normal operation” means the operation of a nuclear installation within specified operational limits and conditions including start-up, power operation, shutting down, shutdown, maintenance, testing and refuelling;

“nuclear power plant” means a fission reactor installation constructed to generate electricity on a commercial scale;

“installation state” means a configuration of nuclear installation components, comprising the physical and thermodynamic states of the materials and the process fluids in them;

“operational limits and conditions” means the set of limits and conditions that can be monitored by or on behalf of the operator, and that can be controlled by the operator;

“Postulated initiating event” means an event identified in the design as leading to either an anticipated operational occurrence or accident conditions.

“practicable” means an action that is technically feasible and justifiable while taking cost-benefit considerations into account;

“Pressure Boundary” means a boundary of any pressure-retaining vessel, system, or component of a nuclear or non-nuclear system;

“Probabilistic Safety Assessment” means a comprehensive and integrated assessment of the safety of the nuclear installation that, by considering the initial installation state and the probability, progression, and consequences of equipment failures and operator response, derives numerical estimates of a consistent measure of the safety of the installation;

“process” means a set of interrelated activities that transform inputs into outputs;

“Process system” means a system whose primary function is to support or contribute to the production of steam or electricity;

“Proven Design” means a design of a component that can be proven either by showing compliance with accepted engineering standards, or by a history of experience, or by test, or some combination of these;

“Residual Heat” means the sum of heat originating from radioactive decay, fission in the fuel in the shutdown state, and the heat stored in reactor related structures, systems and components;

“Risk Significant System” means an installation system whose failure to meet design and performance specifications could result in unreasonable risk to the health and safety of persons, to national security, or to the environment;

“Safeguards” means a system of international inspections and other verification activities undertaken by the International Atomic Energy Agency in order to evaluate, on an annual basis, the compliance of the Republic with its obligations pursuant to the safeguards agreements between the Republic and the International Atomic Energy Agency;

“Safety Analysis” means an analysis by means of appropriate analytical tools that establishes and confirms the design basis for the items important to safety; and ensures that the overall installation design is capable of meeting the acceptance criteria for each installation state;

“Safety Culture” means the characteristics of the work environment, including the values, rules and common understandings, that influence employee perceptions and attitudes about the importance that the organisation places on safety;

“Safety Group” means the assembly of structures, systems and components designated to perform the actions required for a particular postulated initiating event to ensure that the specified limits for Anticipated operational occurrences and Design basis accidents are not exceeded;

“Safety Support System” means a system designed to support the operation of one or more safety systems;

“safety system” means a system 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;

“Severe Accident” means a beyond design basis accident that involves significant core degradation;

“Single Failure” means a failure that results in the loss of capability of a system or component to perform its intended function and any consequential failure that results from the loss of capability;

“shutdown state” means a situation characterized by sub-criticality of the installation during which automatic actuation of safety systems could be blocked and support systems may remain in abnormal configurations;

“structures, systems and components” means a general term encompassing all of the elements of a facility or activity which contribute to protection and safety, except human factors;

“Trip Parameter” means a measurement of a variable that is used to trigger a safety system action when the trip parameter set point is reached;

“Trip Parameter Set Point” means the trip parameter value at which activation of a safety system is triggered;

“Ultimate Heat Sink” means a medium, normally in the nature of water or the atmosphere, to which the residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient;

“usability” means the extent to which a product can be used by specified users, to achieve specified goals, with effectiveness, efficiency, and satisfaction in a specified context of use; and

“vital area” means an area containing equipment, systems, or devices the sabotage of which could directly or indirectly lead to unacceptable radiological consequences.

Schedule I– Defence-In-Depth Concept

There are five levels of defence with their specified purposes.

The Levels of Defence

The levels of defence are

a. *(a) Level One which has* the aim of preventing deviations from normal operation, and preventing failures of systems, structures, and components;
b. *(b)Level Two which has* the aim of detecting and intercept deviations from normal operation in order to prevent anticipated operations occurrences from escalating to accident conditions, and returning the plant to a state of normal operation;
c. *(c) Level Three which has* the aim of minimizing the consequences of accidents by providing inherent safety features, fail-safe design, additional equipment, and mitigating procedures;
d. *(d) Level Four which has* the aim of ensuring that radioactive releases caused by severe accidents are kept as low as practicable; and
e. *(e) Level Five which has* the aim of mitigating the radiological consequences of potential releases of radioactive materials that may result from accident conditions.

Purpose of First Level of Defence

The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to the requirement that the plant should be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning.

Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance and testing, the ease

of access for these activities, the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

Purpose of Second Level of Defence

The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.

This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear installation, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, and their confirmation.

Purpose of Third Level of Defence

In spite of provisions for prevention, accident conditions may occur and measures taken at this level are aimed at preventing core damage in particular. Based on this, engineered safety features and protection systems are provided to prevent escalation towards severe accidents and also to confine radioactive materials within the containment system.

The engineered safety features are designed on the basis of the postulated accidents representing the limiting loads of sets of similar events. Design and operating procedures are aimed at maintaining the effectiveness of the barriers, especially the containment, in the event of such a postulated accident. Active and passive engineered safety systems are used.

Purpose of Fourth Level of Defence

The broad aim of the fourth level of defence is to ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive releases in the unlikely event that a severe plant condition occur, are both kept as low as reasonably achievable, economic and social factors being taken into account.

Measures for accident management are aimed at controlling the course of severe accidents and mitigating their consequences. The most important objective for mitigation of the consequences

of an accident in Level 4 is the protection of the confinement. Such protection ensures the effective functioning of the containment under severe plant conditions. Other measures for accident management are also used.

Purpose of Fifth Level of Defence

The purpose of the fifth level of defence in depth is to ensure that there is a readily available/implementable on-site and off-site emergency plan should there be the very much unlikely case of a radioactive release from a severe accident. These plans cover the functions of collecting and assessing information about the levels of exposures expected to occur in such very unlikely conditions, and the short-term and long-term protective actions that will constitute the intervention needed. Both on-site and off-site emergency plans are exercised periodically to the extent necessary to ensure the readiness of the organizations involved.