REGISTERED No. M - 302
L.-7646

The Gazette of Pakistan

EXTRAORDINARY
PUBLISHED BY AUTHORITY

ISLAMABAD, TUESDAY, DECEMBER 31, 2019

PART II

Statutory Notifications (S. R. O.)

GOVERNMENT OF PAKISTAN
PAKISTAN NUCLEAR REGULATORY AUTHORITY

NOTIFICATION

Islamabad, the 19th October, 2019

S.R.O. 1659 (I)/2019.—In exercise of the powers conferred by Section 16(2)(a) read with Section 56 of the Pakistan Nuclear Regulatory Authority Ordinance, 2001 Pakistan Nuclear Regulatory Authority is pleased to make and promulgate the following regulations:

1. **Short Title, Extent, Applicability and Commencement**.—(1) These regulations may be called the "Regulation on the Safety of Nuclear Power Plant Design - (PAK/911) (Rev.2)".

(2) These regulations extend to the whole of Pakistan.

(3) These regulations shall be applicable to the design of all nuclear power plants built in Pakistan.

(4) These regulations shall come into force at once.

Price. Rs: 20.00

[2062(2019)/Ex. Gaz.]

2. **Definitions.**—In these regulations, unless there is anything repugnant in the subject or context,

(a) *"accident"* means any unintended event, including operating error, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of safety or protection;

(b) *"accident conditions"* means deviations from normal operation that are less frequent and more severe than anticipated operational occurrences, including design basis accident and design extension conditions;

(c) *"accident management"* means taking a set of actions during the accident conditions:

(i) to prevent the escalation of event into a severe accident;

(ii) to mitigate the consequences of severe accident; and

(iii) to achieve a long term safe stable state.

(d) *"active component"* means a component whose functioning depends on an external input such as actuation, mechanical movement or supply of power;

(e) *"anticipated operational occurrences"* means operational processes deviating from normal operation which are expected to occur at least once during the operating lifetime of a facility, but which, in view of appropriate design provisions, do not cause any significant damage to items important to safety or lead to accident conditions;

(f) *"assessment"* means the process, and the result, of analysing systematically and evaluating the hazards associated with facilities and activities, and associated protection and safety measures;

(g) *"audit"* means a documented activity performed to determine by investigation, examination and evaluation of objective evidence of the adequacy of, and adherence to, established procedures, instructions, specifications, regulations, standards, administrative or operational programs and other applicable documents; and the effectiveness of implementation;

(h) *"cliff edge effect"* means an instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value;

(i) *"commissioning"* means the process by which systems and components of a facility, having been constructed, are made operational and verified to be in accordance with design and to have met the required performance criteria;

(j) *"common cause failure"* means failure of two or more structures, systems or components due to a single specific event or cause;

(k) *"common mode failure"* means failure of two or more structures, systems or components in the same manner or mode due to a single event or cause. Common mode failure is a type of common cause failure in which the structures, systems or components fail in the same way;

(l) *"construction"* means the process of manufacturing and assembling the components of a facility, the carrying out of civil works, the installation of components and equipment and the performance of associated tests;

(m) *"decommissioning"* means administrative and technical actions taken to allow the removal of some or all of the regulatory controls from a facility;

(n) *"design"* means the process and the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts;

(o) *"design basis accident"* means a postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits;

(p) *"design extension conditions"* means postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits;

(q) *"design organization"* means the organization responsible for preparation of the final detailed design of the facility to be built;

(r) *"diversity"* means the presence of two or more independent (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, including common mode failure;

(s) *"documentation"* means recorded or pictorial information describing, defining, specifying, reporting or certifying activities, requirements, procedures or results;

(t) *"early radioactive release"* means a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time;

(u) *"equipment qualification"* means generation and maintenance of evidence to ensure that equipment will operate on demand, under specified service conditions, to meet system performance requirements;

(v) *"examination"* means an element of inspection consisting of investigation of materials, components, supplies or service, to determine conformance with those specified requirements, which can be determined by such investigation;

(w) *"facility"* means nuclear power plant, and is also called as plant*;*

(x) *"fuel assembly"* means a set of fuel elements and associated *components which* are loaded into and subsequently removed from a reactor core as a single unit;

(y) *"fuel element"* means a rod of nuclear fuel, its cladding and any associated components necessary to form a structural entity;

(z) *"functional isolation"* means prevention of adverse consequences from the mode of operation or failure of one circuit or system on another;

(aa) *"inspection"* means examination, observation, surveillance, measurement or test undertaken to assess structures, systems, components and materials as well as operational activities, technical and organizational processes, procedures and personnel competence;

(bb) *"item important to safety"* means an item that is part of a safety group and whose malfunction or failure could lead to radiation exposure of the workers or the public;

(cc) *"large radioactive release"* means a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and the environment;

(dd) *"licensee"* means the holder of a valid licence issued by the Authority;

(ee) *"limit"* means the value of quantity used in certain specified activities or circumstances that must not be exceeded and is acceptable to or notified by the Authority;

(ff) *"management system"* means a set of interrelated or interacting elements (a system) for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner;

(gg) *"normal operation"* means operation within specified operational limits and conditions;

(hh) *"nuclear safety"* means the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks;

(ii) *"operating personnel"* means individual workers engaged in the operation of an authorized facility;

(jj) *"operation"* means all activities performed to achieve the purpose for which an authorized facility was constructed;

(kk) *"operational limits and conditions (OLCs)"* means a set of rules, setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the Authority for safe operation of an authorized facility;

(ll) *"operational states"* means states defined under normal operation and anticipated operational occurrences;

(mm) *"passive component"* means a component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power;

(nn) *"physical separation"* means separation by geometry (distance, orientation, etc); by appropriate barriers; or by a combination thereof;

(oo) *"possible radiation risk"* means the maximum possible radiological consequences that could occur when radioactive material is released or in the activity, with no credit being taken for the safety system or protective measures in place to prevent this;

(pp) *"postulated initiating event (PIE)*" means an event identified during design as capable of leading to anticipated operational occurrences or accident conditions;

(qq) *"practically eliminated"* means the possibility of certain conditions that would be physically impossible to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise;

(rr) *"probabilistic safety assessment (PSA)"* means a comprehensive, structured approach to identify failure

scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk;

(ss) *"protection system"* means system that monitors the operation of a reactor and which, on sensing abnormal conditions, automatically initiates actions to prevent an unsafe or potentially unsafe condition;

(tt) *"redundancy"* means provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other;

(uu) *"residual heat"* means sum of the heat originating from radioactive decay and shutdown fission and the heat stored in reactor related structures and in heat transport media;

(vv) *"safety function"* means specific purpose that must be accomplished for safety;

(ww) *"safety group"* means assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for the anticipated operational occurrence and design basis accident are not exceeded;

(xx) *"safety limits"* means limits on operational parameters within which an authorized facility has been shown to be safe;

(yy) *"severe accident"* means accident conditions involving significant core degradation;

(zz) *"single failure"* means a failure which results in the loss of capability of a single system or component to perform its intended safety function, and any consequential failure which results from it;

(aaa) *"single failure criterion"* means a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure;

(bbb) *"siting"* means process of selecting a suitable site for a facility, including appropriate assessment and definition of the related design bases;

(ccc) *"specification (technical condition)"* means a written statement of requirements to be satisfied by a product, a service, a material or process, indicating the procedure by means of which it may be determined whether specified requirements are satisfied;

(ddd) *"structures, systems and components"* means a general term encompassing all of the elements (items) of a facility or activity that contribute to protection and safety, except human factors;

(eee) *"testing"* means determination or verification of the capability of an item to meet specified requirements by subjecting the item to a set of physical, chemical, environmental or operational conditions;

(fff) *"treatment"* means operations intended to benefit safety and economy by changing the characteristics of the waste; and

(ggg) *"ultimate heat sink"* means a medium into which the transferred residual heat can always be accepted, even if all other means of removing the heat have been lost or are insufficient.

3. **Purpose.—**The purpose of these regulations is to delineate regulatory requirements pertaining to the design of structures, systems and components important to safety that must be met for safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardize safety. It also establishes requirements for a comprehensive safety assessment, which shall be carried out in order to identify the potential hazards that may arise from the operation of the plant, under various plant states (operational states and accident conditions).

4. **Scope.—**(1) These regulations shall be applicable to land based stationary nuclear power plants with water cooled reactors designed for electricity generation.

(2) These regulations do not address:

(a) Matters relating to physical protection or to the system of accounting for, and control of, nuclear material;

(b) Conventional industrial safety that under no circumstances could affect the safety of the plant; and

(c) Non-radiological effects arising from the operation of the plants.

5. **Interpretation.**—The decision of the Chairman regarding interpretation of any word or phrase of these regulations shall be final and binding.

6. **Safety Objective and Concepts.**—(1) These regulations establish regulatory requirements so that the plants shall be designed and operated with the aim to achieve fundamental safety objective of protecting people and the environment from the harmful effects of ionizing radiation. To ensure that plants are operated and activities are conducted to achieve the highest standards of safety that can reasonably be achieved, measures shall be taken to:

(a) Control the radiation exposure of people and the release of radioactive material to the environment;

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

(c) Mitigate the consequences of such events, if they do occur.

(2) The fundamental safety objective shall be applied for all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well

as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste.

(3) Radiation Protection in Design

(a) It shall be ensured that for all operational states of a plant and any associated activities, doses from exposure to radiation within the plant or exposure due to any planned radioactive release from the plant are kept below the dose limits and kept as low as reasonably achievable. Moreover, measures shall be implemented for mitigating the radiological consequences of any accidents, if they do occur.

(b) The plants shall be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, this does not preclude limited exposures or the release of authorized amounts of radioactive substances to the environment from the plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept as low as reasonably achievable and in compliance with regulatory and operational limits as well as radiation protection requirements.

(4) Safety in Design

(a) To achieve the highest level of safety in the design of a nuclear power plant, measures shall be taken to do the following, consistent with acceptance criteria and safety objective, to:

(i) Prevent accidents with harmful consequences resulting from the loss of control over the reactor core or other sources of radiation, and to mitigate the consequences of any accidents that do occur;

(ii) Ensure that for all accidents taken into account, in the design of the plant, any radiological consequences are below the defined limits and are kept as low as reasonably achievable; and

(iii) Ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such accident are mitigated to the extent practicable.

(b) In the design of a plant, a comprehensive safety assessment of the design shall be carried out to identify all possible sources of radiation and to evaluate the possible doses that could be received by workers at the plant and by members of the public, as well as the possible effects on the environment, as a result of operation of the plant. The safety assessment shall be carried out to examine normal operation of the plant, performance of the plant in anticipated operational occurrences, and the accident conditions. On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents shall be established, the effectiveness of the items important to safety shall be demonstrated and the inputs (prerequisites) for emergency planning shall be established.

(c) Measures shall be taken to control exposure for all operational states at levels that are as low as reasonably achievable and to minimize the likelihood of an accident that could lead to the loss of control over a source of radiation

(d) Measures shall be taken to ensure that the radiological consequences of an accident are mitigated. Such measures shall include the provision of safety features, safety systems, the establishment of accident management guidelines and establishment of off-site intervention measures to mitigate exposures, if an accident occurs.

(e) The design for safety of a nuclear power plant applies the safety principle that practical measures shall be taken to mitigate the consequences of nuclear or radiation incidents on human life and health and for the environment. Plant event sequences that could result in high radiation doses or radioactive releases must be practically eliminated and plant event sequences with a significant frequency of occurrence must have no or only minor potential radiological consequences.

(5) Defence in Depth

(a) The concept of defence in depth shall be applied to all safety related activities, whether organizational, behavioural or design related and operation whether in full power, low power or various shutdown states to provide a graded protection against a wide variety of transients, 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.

(b) Application of the concept of defence in depth in the design of a plant shall provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event when prevention fails. The independent effectiveness of each of the different levels of defence shall be achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels of defence.

(c) There are five levels of defence in depth:

(i) The aim of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety;

(ii) The aim of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions;

(iii) The aim of the third level of defence is to provide inherent and engineered safety features, safety systems and procedures that are capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state;

(iv) The aim of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth; and

(v) The aim of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions.

MANAGEMENT OF SAFETY IN DESIGN

7. **Management Responsibilities.—**The licensee shall have the overall responsibility for safety throughout the lifetime of the plant. However, all organizations including the design organization, engaged in activities important to safety shall be responsible to ensure that safety matters are given the highest priority.

8. **Management System for Plant Design.—**(1) The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.

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

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

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

9. **Safety of the Plant Design.—**(1) The licensee shall establish a formal system for ensuring the safety of the plant design throughout the lifetime of the nuclear power plant.

(2) The formal system for ensuring the safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the licensee's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements.

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

(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 on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;

(c) The knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, this knowledge is maintained up to date by the licensee, and due account is taken of past operating experience and validated research findings;

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

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

(f) The necessary engineering expertise and scientific and technical knowledge are maintained;

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

(h) Adequate documentation is maintained to facilitate future decommissioning of the plant.

PRINCIPAL TECHNICAL REQUIREMENTS

10. **Fundamental Safety Functions.—**(1) Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states:

(a) Control of reactivity;

(b) Removal of heat from the reactor and from the fuel storage; and

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

(2) A systematic approach shall be taken to identify those items important to safety that are necessary to fulfil the fundamental safety functions and to identify the inherent features that are contributing to fulfil, or that are affecting, the fundamental safety functions for all plant states.

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

11. **Radiation Protection in Design.—**(1) The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.

(2) The design shall ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated and that there are no or only minor potential radiological consequences for plant states with a significant likelihood of occurrence.

(3) Acceptable limits for radiation protection associated with the relevant categories of plant states shall be established, in accordance with PNRA regulations.

12. **Design of a Nuclear Power Plant.—**(1) The design shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.

(2) The design shall ensure that the safety requirements of the licensee, the requirements of the Authority, as well as applicable national and international codes and standards are all met. The design shall take into account human capabilities, limitations, and factors that could influence human performance. Adequate information shall be provided for ensuring the safe operation and maintenance of the plant and to allow subsequent plant modifications to be made. Recommended practices shall be provided for incorporation into the administrative and operational procedures for the plant (i.e. the operational limits and conditions).

(3) The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programs.

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

(5) The design shall ensure that the generation of radioactive waste and discharges are kept to the minimum practicable in terms of both activity and volume, by means of appropriate design measures and operational and decommissioning practices.

13. **Application of Defence in Depth.—**(1) The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as practicable.

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

(3) The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times and any relaxation shall be justified for specific modes of operation.

(4) The design shall:

(a) Provide for multiple physical barriers to prevent the release of radioactive material to the environment;

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

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

(d) Provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;

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

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

(5) To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as practicable:

(a) Challenges to the integrity of physical barriers;

(b) Failure of one or more barriers;

(c) Failure of a barrier as a consequence of the failure of another barrier; and

(d) The possibility of harmful consequences of errors in operation and maintenance.

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

(7) The levels of defence in depth shall be independent, as far as practicable, to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall, as far as practicable, be independent of safety systems.

14. **Interface of Safety with Physical Protection.—**Safety and physical protection measures for a nuclear power plant shall be designed

and implemented in an integrated manner so that they do not compromise one another.

15. **Proven Engineering Practices.—**(1) Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.

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

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

(4) Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programs, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.

16. **Operational Experience and Safety Research.—**The design shall take due account of relevant operational experience that has been gained in operating plants and of the results of relevant research programs.

17. **Safety Assessment.—**(1) A comprehensive deterministic safety assessment and PSA shall be carried out throughout the design process to ensure that all relevant safety requirements are met by the design of the plant throughout all stages of the lifetime of the plant to confirm that the design meets requirements as delivered for fabrication, as for construction, as built, as operated and as modified.

(2) The safety assessments shall be commenced at an early stage in the design process, with iteration between the design and confirmatory

analytical activities, and increasing in the scope and level of detail as the design program progresses. The basis for the safety assessment shall be data derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice.

(3) The safety assessments shall be documented in a form that facilitates independent evaluation.

(4) The licensee shall ensure that the individuals or the groups separate from those carrying out the design activities shall perform an independent verification of the safety assessment, before the design is submitted to the Authority.

18. **Provision for Construction.—**(1) Items important to safety for a nuclear power plant shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.

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

19. **Features to Facilitate Radioactive Waste Management and Decommissioning.—**(1) Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning of the plant.

(2) In particular, the design shall take due account of the:

(a) Choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;

(b) Access capabilities and the means of handling that might be necessary; and

(c) Facilities necessary for the management (i.e. segregation, characterization, classification, pre-treatment, treatment and conditioning) and storage of radioactive waste generated in

operation and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

GENERAL PLANT DESIGN

DESIGN BASIS

20. **Categories of Plant States.—**(1) Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant.

(2) Plant states shall typically cover:

(a) Normal operation;

(b) Anticipated operational occurrences, which are expected to occur over the operating lifetime of the plant;

(c) Design basis accidents; and

(d) Design extension conditions, including accidents with core melt.

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

21. **Design Basis for Items Important to Safety.—**(1) The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.

(2) The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the plant management to operate the plant safely.

(3) Conservative design measures shall be applied and sound engineering practices shall be adhered to in the design bases for normal operation, anticipated operational occurrences and design basis accidents so as to provide a high degree of assurance that no significant damage will occur to the reactor core and that radiation doses will remain within prescribed limits and will be as low as reasonably achievable.

(4) In addition to the design basis accidents, the performance of the plant in specified design extension conditions including selected severe accidents shall also be addressed in the design. The assumptions and methods used for these evaluations may be on a best estimate basis. The analysis results of selected severe accidents shall be described to evaluate the possible radiation risks associated with the facility or activity.

22. **Design Limits.—**(1) A set of design limits consistent with the key physical parameters for each item important to safety for the nuclear power plant shall be specified for all operational states and for accident conditions.

(2) The design limits shall be specified and shall be consistent with relevant regulatory requirements, agreed national and international codes and standards.

23. **Postulated Initiating Events.—**(1) The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.

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

(3) The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

(4) An analysis of the postulated initiating events for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed.

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

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

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

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

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

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

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

(8) Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the

design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.

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

(10) The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

(11) The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

(12) Any equipment that is necessary for actions to be taken in manual response and recovery processes shall be placed at the most suitable location to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

24. **Internal and External Hazards.—**(1) All foreseeable internal and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered when establishing the plant layout and for determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

(2) Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects

of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards.

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

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

(5) The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Cause and likelihood shall be considered in postulating potential concurrent hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

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

(7) The design shall be such that items important to safety that are necessary to fulfil the fundamental safety functions are either capable of withstanding the effects of external events considered in the design or protected from such effects by other features such as passive barriers and to ensure that required safety function will be performed.

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

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

25. **Engineering Design Rules.—**(1) The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology.

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

(3) The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events.

26. **Design Basis Accidents.—**(1) A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.

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

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

(4) The design basis accidents shall be analyzed in a conservative manner. This approach involves postulating certain failures in safety

systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

27. **Design Extension Conditions.—**(1) A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.

(2) An analysis of design extension conditions for the plant shall be performed. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release would be practically eliminated. The effectiveness of provisions to ensure the functionality of the containment shall be analyzed. The best estimate approach could be used for the analysis.

(3) The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.

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

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

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

(c) Have reliability commensurate with the function that they are required to fulfil.

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

(6) The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is practically eliminated.

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

28. **Combinations of Events and Failures.—**Where the results of engineering judgement, deterministic safety assessments and PSA indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event.

29. **Physical Separation and Independence of Safety Systems.—**(1) Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate.

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

30. **Safety Classification.—**(1) All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

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

(a) Safety functions to be performed by the item;

(b) Consequences of failure to perform a safety function;

(c) Frequency with which the item will be called upon to perform a safety function; and

(d) Time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function.

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

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

31. **Reliability of Items Important to Safety.**—(1) The reliability of items important to safety shall be commensurate with their safety significance.

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

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

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

33. **Single Failure Criterion.—**(1) The single failure criterion shall be applied to each safety group incorporated in the plant design.

(2) Spurious action shall be considered to be one mode of failure when applying the concept of single failure criterion to a safety group or safety system.

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

34. **Fail-Safe Design.—**(1) The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.

(2) Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the

failure of a support feature does not prevent the performance of the intended safety function.

35. **Support Service Systems.—**(1) Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

(2) The reliability, redundancy, diversity and independence of support service systems and the provision of features for their isolation and for testing their functional capability shall be commensurate with the significance to safety of the system being supported.

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

36. **Operational Limits and Conditions for Safe Operation.—**(1) The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.

(2) The requirements and operational limits and conditions established in the design for the nuclear power plant shall include:

(a) Safety limits;

(b) Limiting settings for safety systems;

(c) Operational limits and conditions for operational states;

(d) Control system constraints and procedural constraints on process variables and other important parameters;

(e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;

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

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

DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT

37. **Calibration, Testing, Maintenance, Repair, Replacement, Inspection and Monitoring of Items Important to Safety.**—(1) Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.

(2) The plant layout shall be such that activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be commensurate with the importance of the safety functions to be performed, and shall be performed without undue exposure of workers.

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

(4) Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions.

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

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

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

38. **Qualification of Items Important to Safety.**—(1) A qualification program for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.

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

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

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

(5) The items important to safety shall be seismically qualified.

39. **Ageing Management.—**(1) The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out

and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.

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

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

HUMAN FACTORS

40. **Design for Optimal Operator Performance.—**(1) Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.

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

(3) Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

(4) The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the likelihood and effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant in all plant states.

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

(6) The operator shall be provided with the necessary information to:

(a) Assess the general state of the plant in any condition;

(b) Operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);

(c) 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) Determine both the need for and the time for manual initiation of the specified safety actions.

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

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

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

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

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

OTHER DESIGN CONSIDERATIONS

41. **Safety Systems, and Safety Features for Design Extension Conditions, of Units of a Multiple Unit Nuclear Power Plant.—**(1) Each unit shall have its own systems important to safety to control and mitigate the anticipated operational occurrences, design basis accidents and design extension conditions.

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

(3) In accident conditions, inter connecting support systems among the units is allowed if it can be justified that it facilitates the accident management of one unit by giving the possibility to restore a safety function. Such a sharing shall not be permitted if it would increase either the likelihood or the consequences of an accident at any unit of the plant.

42. **Systems Containing Fissile Material or Radioactive Material.—**(1) All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as to:

(a) Prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment;

(b) Prevent accidental criticality and overheating;

(c) Ensure that releases of radioactive material are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and

(d) Facilitate mitigation of radiological consequences of accidents.

43. **Nuclear Power Plants Used for Cogeneration of Heat and Power, Heat Generation or Desalination.—**Nuclear power plants coupled with heat utilization units or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear power plant to the desalination unit or the heat utilization unit under conditions of operational states as well as in accident conditions.

44. **Escape Routes from the Plant.—**(1) The plant shall be provided with sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential for safe use of these escape routes.

(2) Escape routes from the plant shall meet the relevant national and international requirements for radiation zoning and fire protection, and the relevant national requirements for industrial safety and physical protection of the plant.

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

45. **Communication Systems at the Plant.—**(1) Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.

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

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

46. **Control of Access to the Plant.—**(1) The nuclear power plant shall be isolated from its surroundings with a suitable layout of various structural elements so that access to it can be controlled.

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

47. **Prevention of Unauthorized Access to, or Interference with, Items Important to Safety.—**Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.

48. **Prevention of Harmful Interactions of Systems Important to Safety.—**(1) The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.

(2) In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

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

49. **Interactions Between the Electrical Power Grid and the Plant.—**The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

50. **Proximity Effects from Multiple Units.—**The design shall ensure that incident at one reactor will not affect the adjacent units.

SAFETY ANALYSIS

51. **Safety Analysis of the Plant Design.—**(1) A safety analysis of the design for the nuclear power plant shall be conducted, by both deterministic analysis and probabilistic analysis, and shall be applied to enable the challenges to safety in various categories of plant states to be evaluated and assessed.

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

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

(4) The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases.

(5) The applicability of the analytical assumptions, methods and degree of conservatism used in the plant design shall be updated and verified. The safety analysis of the plant design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomenon, and shall be consistent with the current or 'as built' design.

Deterministic Approach

(6) The deterministic safety analysis shall mainly provide but not limited to:

(a) Establishment and confirmation of the design bases for all items important to safety;

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

(c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;

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

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

(f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.

Probabilistic Approach

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

(a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;

(b) Providing assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented;

(c) Comparing the results of the analysis with the following acceptance criteria for PSA:

(i) The full scope Level-1 PSA core damage frequency shall be less than $1x10^{-5}$ per reactor year; and

(ii) The large early release frequency of radioactive material shall be less than $1x10^{-6}$ per reactor year.

(d) Providing assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;

(e) Identifying systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences; and

(f) Assessing the adequacy of plant emergency procedures.

DESIGN OF SPECIFIC PLANT SYSTEMS

REACTOR CORE AND ASSOCIATED FEATURES

52. **Performance of Fuel Elements and Assemblies.—**(1) Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.

(2) The processes of deterioration to be considered shall 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 distortions or chemical effects.

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

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

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

53. **Structural Capability of the Reactor Core.—**(1) The fuel elements and fuel assemblies and their supporting structures shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.

(2) The reactor core and associated internal components located within the reactor vessel shall be designed and mounted in such a way that they will withstand the static and dynamic loading expected in operational states, design basis accidents and external events to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor sub-critical and to ensure cooling of the core.

54. **Control of the Reactor Core.—**(1) Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for

maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.

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

(3) In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burn-up, changes in physical properties and production of gas.

(4) The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions, not involving degradation of the reactor core, shall be limited or compensated for to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core.

(5) The reactor core and associated coolant, control and protection systems shall be designed to enable adequate inspection and testing throughout the service lifetime of the plant

55. **Reactor Shutdown.—**(1) Means shall be provided to ensure that there is a capability to shutdown the reactor in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.

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

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

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

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

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

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

REACTOR COOLANT SYSTEMS

56. **Design of Reactor Coolant Systems.—**(1) The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.

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

(3) The design of the reactor coolant pressure boundary shall be such that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture and to rapid crack propagation, thereby permitting the timely detection of flaws.

(4) The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could exhibit embrittlement are avoided.

(5) The design of the components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall be such as to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to

safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service.

(6) The component parts containing the reactor coolant, such as the reactor pressure vessel or the pressure tubes, piping and connections, valves, fittings, pumps, circulators and heat exchangers, together with the devices by which such parts are held in place shall be designed in such a way as to withstand the static and dynamic loads anticipated in all operational states and in design basis accidents. The materials used in the fabrication of the component parts shall be selected so as to minimize activation of the material.

(7) The design shall reflect consideration of all conditions of the pressure boundary material in operational states, including those for maintenance and testing and under design basis accident conditions, with account taken of the expected end-of-life properties affected by erosion, creep, fatigue, the chemical environment, the radiation environment and ageing, and any uncertainties in determining the initial state of the components and the rate of possible deterioration.

57. **Overpressure Protection of the Reactor Coolant Pressure Boundary.—**Provision shall be made to ensure that the operation of pressure relief devices will protect the pressure boundary of the reactor coolant systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant directly to the environment.

58. **Inventory of Reactor Coolant.—**Provision shall be made for controlling the inventory, temperature and pressure of the reactor coolant to ensure that specified design limits are not exceeded in any operational state of the nuclear power plant, with due account taken of volumetric changes and leakage.

59. **Cleanup of Reactor Coolant.—**(1) Adequate facilities shall be provided at the nuclear power plant for the removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products deriving from the fuel, and non-radioactive substances.

(2) The capabilities of the necessary plant systems shall be based on the specified design limit on permissible leakage of the fuel, with a

conservative margin to ensure that the plant can be operated with a level of circuit activity that is as low as reasonably practicable, and to ensure that the requirements are met for radioactive releases to be as low as reasonably achievable and below the authorized limits on discharges.

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

61. **Emergency Cooling of the Reactor Core.—**(1) Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the pressure boundary of the primary coolant system is not maintained.

(2) The means provided for cooling of the reactor core shall be such as to ensure that:

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

(b) Possible chemical reactions are kept to an acceptable level;

(c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core; and

(d) Cooling of the reactor core will be ensured for a sufficient time.

(3) Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of Regulation 61(2) of these regulat tons with adequate reliability for each postulated initiating event.

(4) The emergency core cooling system shall be designed to permit appropriate periodic inspection of important components and permit appropriate periodic testing to confirm the following:

(a) Structural integrity and leak tight integrity of its components;

(b) Operability and performance of the active components of the system in normal operation, as far as feasible; and

(c) Operability of the system as a whole under the plant states specified in the design basis, to the extent practicable.

62. **Heat Transfer to an Ultimate Heat Sink.—**(1) The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.

(2) Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.

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

63. **In-Service Inspection of the Reactor Coolant Pressure Boundary.—**(1) The components of the reactor coolant pressure boundary shall be designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the pressure boundary.

(2) Provision shall be made to implement a material surveillance program for the reactor coolant pressure boundary, particularly in locations of high irradiation, and for other important components as appropriate, in order to determine the metallurgical effects of factors such as irradiation, stress corrosion cracking, thermal embrittlement and ageing of structural materials.

(3) It shall be ensured that it is possible to inspect or test either directly or indirectly the components of the reactor coolant pressure boundary, according to the safety importance of those components, so as to demonstrate the absence of unacceptable defects or of safety significant deterioration.

(4) Indicators for the integrity of the reactor coolant pressure boundary (such as leakage) shall be monitored. The results of such measurements shall be taken into consideration in determination of which inspections are necessary for safety.

(5) If the safety analysis of the nuclear power plant indicates that particular failures in the secondary cooling system may result in serious consequences, it shall be ensured that it is possible to inspect the relevant parts of the secondary cooling system.

CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

64. **Containment System for the Reactor.—**(1) A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant:

(a) Confinement of radioactive substances in all plant states;

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

(c) Radiation shielding in all plant states.

65. **Strength of the Containment Structure.—**The strength of the containment structure, including access opening and penetrations and isolation valves, shall be calculated with sufficient margins of safety on the basis of potential internal overpressures, under pressures and temperatures, dynamic effects such as missile impacts and reaction forces anticipated to arise as a result of design basis accidents. The effects of other potential energy sources, including for example, possible chemical and radiolytic reactions shall also be considered. In calculating the necessary strength of the containment structure, natural phenomenon and human induced events shall be taken into consideration, and provision shall be made to monitor the condition of the containment and its associated features.

66. **Control of Radioactive Releases from the Containment.—**(1) The design of the containment shall be such as to ensure that any release of radioactive material from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized

limits on discharges in operational states and is below acceptable limits in accident conditions

(2) The containment structure and the systems and components affecting the leak tightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations through the containment have been installed and, if necessary, during the operating lifetime of the plant, so that the leak rate can be tested at the containment design pressure

(3) The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip.

67. **Isolation of the Containment.—**(1) Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leak tightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.

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

(3) Exceptions to the requirements for containment isolation stated in Regulation 67(2) of these regulations shall be permissible for specific classes of lines such as instrumentation lines, or in cases in which application of the methods of containment isolation specified in Regulation 67(2) of these regulations would reduce the reliability of a safety system that includes a penetration of the containment.

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

68. **Access to the Containment.—**(1) Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.

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

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

69. **Control of Containment Conditions.—**(1) Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any build up 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.

(2) The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions.

(3) The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after any accidental release of high energy fluids. The systems performing the

function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled.

(4) Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.

(5) The design shall also include features to enable the safe use of non-permanent equipment for restoring the capability to remove heat from the containment.

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

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

(b) 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.

(7) Systems for cleaning up the containment atmosphere shall have suitable redundancy in components and features to ensure that the safety group can fulfil the necessary safety function, on the assumption of a single failure. A reliable venting system shall be designed to be independent of AC power and to operate with limited operator actions from the control room.

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

70. **Containment Testing and Surveillance.—**(1) The containment shall be designed to permit appropriate:

(a) Periodic inspection of all important areas; and

(b) Surveillance program.

(2) The containment structure shall be designed and constructed so that it is possible to perform a pressure test at a specified pressure to demonstrate its structural integrity before operation of the plant and over the plant's lifetime.

INSTRUMENTATION AND CONTROL SYSTEMS

71. **Provision of Instrumentation.—**(1) Instrumentation shall be provided for determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant, for obtaining essential information on the plant that is necessary for its safe and reliable operation, for determining the status of the plant in accident conditions and for making decisions for the purpose of accident management.

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

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

73. **Protection System.—**(1) A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.

(2) The protection system shall be designed:

(a) To be capable of overriding unsafe actions of the control system; and

(b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system.

(3) The design of the protection system shall:

(a) Prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but not counteract correct operator actions in accident conditions;

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

(c) Make relevant information available to the operator for monitoring the effects of automatic actions.

74. **Reliability and Testability of Instrumentation and Control System.—**(1) Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function to be performed.

(2) Redundancy and independence designed into protection system shall be sufficient at least to ensure that:

(a) No single failure results in loss of protection function; and

(b) The removal from service of any component or channel does not result in loss of the necessary minimum redundancy, unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

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

(4) Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility

of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display.

(5) When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities.

75. **Use of Computer Based Equipment in Systems Important to Safety.—**(1) If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.

(2) For computer based equipment in safety systems or safety related systems:

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

(b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable;

(c) An assessment of the equipment shall be undertaken by experts, who are independent of the design team and the supplier team, to provide assurance of its high reliability;

(d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided;

(e) Common cause failures deriving from software shall be taken into consideration; and

(f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation.

76. **Separation of Protection Systems and Control Systems.—** (1) Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.

(2) If signals are used in common by both the protection system and any control system, appropriate separation (such as by adequate de-coupling) shall be ensured and the signal system shall be classified as part of the protection system. It shall be demonstrated that all safety requirements of "Functions of Protection System", "Reliability and Testability of the Protection System" and "Use of Computer Based Systems in Protection" are fulfilled.

77. **Control Room.—**(1) A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.

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

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

(4) The layout of the instrumentation and the mode of presentation of information shall provide the operating personnel with an adequate overall picture of the status and performance of the plant.

(5) Devices shall be provided to give an efficient way of visual and, if appropriate, also audible indication of operational status and processes that have deviated from normal and could affect safety.

(6) The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.

78. **Emergency Control Room.—**(1) Instrumentation and control equipment shall be kept available, preferably at a single location (an emergency control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The emergency control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.

(2) The requirements of Regulation 77(2) of these regulations for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the emergency control room at the nuclear power plant.

79. **Emergency Control Centre.—**(1) An on-site emergency control centre, separate from both the plant control room and the emergency control room, shall be provided from which an emergency response can be directed at the nuclear power plant.

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

80. **Technical Support Centre.—**(1) An on-site technical support centre, separate from both the plant control room and the emergency control room, shall be established from which technical support can be provided to the operation staff during accident conditions.

(2) Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided in the on-site technical support centre. The on-site technical support centre shall provide means of communication with the control room, the emergency control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

(3) The technical support centre shall remain operable and habitable for a protracted period of time in situations generated by accidents and hazards considered in the design of the plant. This requirement shall be fulfilled with significant margins.

EMERGENCY POWER SUPPLY

81. **Design for Withstanding the Loss of Off-Site Power.—**(1) The emergency power supply at the nuclear power plant shall be capable of supplying the necessary power in anticipated operational occurrences and in design basis accidents in the event of the loss of off-site power. The design shall also include an alternate power source to supply the necessary power in design extension conditions.

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

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

(4) The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the

event of the loss of off-site power combined with failure of the emergency power supply.

(5) Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources.

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

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

(8) The design basis for any diesel engine or other prime mover that provides an emergency power supply to items important to safety shall include the:

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

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

(c) Auxiliary systems of the prime mover, such as coolant systems.

(9) The design shall include necessary features to enable the use of non-permanent power sources which may or may not be available at the site.

SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

82. **Performance of Supporting Systems and Auxiliary Systems.—**The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent

with the safety significance of the system or component that they serve at the nuclear power plant.

83. **Heat Transport Systems.—**(1) Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions.

(2) The design of heat transport systems shall be such as to ensure that non-essential parts of the systems can be isolated.

84. **Process Sampling Systems and Post-Accident Sampling Systems.—**(1) Process sampling systems and post-accident sampling systems shall be provided for determining, in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.

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

85. **Compressed Air Systems.—**The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanness of the air to be provided.

86. **Air Conditioning Systems and Ventilation Systems.—**(1) Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states.

(2) Systems shall be provided for the ventilation of buildings at the nuclear power plant with appropriate capability for the cleaning of air in order to:

(a) Prevent unacceptable dispersion of airborne radioactive substances within the plant;

(b) Reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;

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

(d) Ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents; and

(e) Control releases of gaseous radioactive material to the environment below the authorized limits and to keep them as low as reasonably achievable.

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

87. **Fire Protection Systems.—**(1) Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis.

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

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

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

(5) Fire detection systems and fire extinguishing systems that are necessary to protect against a possible fire following a postulated

initiating event shall be appropriately qualified to resist the effects of the postulated initiating event.

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

88. **Lighting Systems.—**Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.

89. **Overhead Lifting Equipment.—**(1) Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.

(2) The overhead lifting equipment shall be designed so that:

(a) Measures are taken to prevent the lifting of excessive loads;

(b) Conservative design measures are applied to prevent any unintentional dropping of loads that could affect items important to safety;

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

(d) Such equipment can be used only in specified plant states (by means of safety interlocks on the crane); and

(e) Such equipment, for use in areas where items important to safety are located, is seismically qualified.

OTHER POWER CONVERSION SYSTEMS

90. **Steam Supply System, Feedwater System and Turbine Generators.—**(1) The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or in accident conditions.

(2) The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.

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

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

TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

91. **Systems for Treatment and Control of Waste.—**(1) Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.

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

(3) The design of the plant shall incorporate appropriate features to facilitate the movement, transport and handling of radioactive waste. Consideration shall be given to the provision of access to facilities and to capabilities for lifting and for packaging.

92. **Systems for Treatment and Control of Effluents.—**(1) Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.

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

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

(4) The cleanup equipment for the gaseous radioactive substances shall provide the necessary retention factor to keep radioactive releases below the authorized limits on discharges. Filter systems shall be designed so that their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air.

FUEL HANDLING AND STORAGE SYSTEMS

93. **Fuel Handling and Storage Systems.—**(1) Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

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

(3) The design of the plant shall be such as to prevent any significant damage to fuel and other items important to safety during the transfer of fuel or casks, or in the event of fuel or casks being dropped.

(4) Adequate consideration shall be given to control hydrogen that may be generated or released within the spent fuel storage building in the event of loss of spent fuel cooling and to maintain integrity and functionality of fuel building.

(5) The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed to:

(a) Prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by use of geometrically safe configurations, even under conditions of optimum moderation;

(b) Permit inspection of the fuel;

(c) Permit maintenance, periodic inspection and testing of components important to safety;

(d) Prevent damage to the fuel;

(e) Prevent the dropping of fuel in transit;

(f) Provide for the identification of individual fuel assemblies;

(g) Provide proper means for meeting the relevant requirements for radiation protection; and

(h) Ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel.

(6) In addition, the fuel handling and storage systems for irradiated fuel shall be designed to:

(a) Permit adequate removal of heat from the fuel in operational states and in accident conditions;

(b) Prevent the dropping of spent fuel in transit;

(c) Prevent causing unacceptable handling stresses on fuel elements or fuel assemblies;

(d) Prevent the potential damage due to dropping of heavy objects on the fuel such as spent fuel casks, cranes or other objects;

(e) Permit safe keeping of suspect or damaged fuel elements or fuel assemblies;

(f) Control levels of soluble absorber if this is used for criticality safety;

(g) Facilitate maintenance and future decommissioning of fuel handling and storage facilities;

(h) Facilitate decontamination of fuel handling and storage areas and equipment when necessary;

(i) Accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core; and

(j) Facilitate the removal of fuel from storage and its preparation for off-site transport.

(7) With the goal to practically eliminate significant releases, for reactors using a water pool system for fuel storage, the design of the plant shall:

(a) Provide the necessary spent fuel pool cooling capabilities to prevent the uncovering of the fuel assemblies in operational states and accident conditions relevant for the spent fuel pool;

(b) Provide features to prevent the uncovering of the fuel assemblies in the event of a leak or pipe break;

(c) Provide capabilities to restore the water inventory; and

(d) Include the following means for:

(i) Monitoring and controlling the water temperature in operational states and accident conditions relevant for the spent fuel pool;

(ii) Monitoring the water level in operational states and accident conditions relevant for the spent fuel pool;

(iii) Monitoring the activity in water and air in operational states and accident condition relevant for the spent fuel pool ;

(iv) Monitoring water chemistry in operational states; and

(v) Enabling the use of non-permanent equipment to ensure the long term spent fuel pool cooling.

RADIATION PROTECTION

94. **Design for Radiation Protection.—**(1) Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.

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

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

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

(5) The plant layout shall be such as to ensure that access of operating personnel to areas with radiation hazards and areas of possible contamination is adequately controlled, and that exposures and contamination are prevented or reduced by this means and by means of ventilation systems.

(6) The plant shall be divided into zones that are related to their expected occupancy, and to radiation levels and contamination levels in operational states (including refuelling, maintenance and inspection) and to potential radiation levels and contamination levels in accident conditions. Shielding shall be provided so that radiation exposure is prevented or reduced.

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

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

(9) Facilities shall be provided for the decontamination of operating personnel and plant equipment.

95. **Means of Radiation Monitoring.—**(1) Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.

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

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

(4) Stationary monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by operating personnel and where the levels of activity of airborne radioactive substances might be such as to necessitate protective measures. These systems shall provide an indication in the control room or in other appropriate locations when a high activity concentration of radionuclides is detected. Monitors shall also be provided in areas subject to possible contamination as a result of equipment failure or other unusual circumstances.

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

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

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

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

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

(a) Exposure pathways to people, including the food chain;

(b) Radiological impacts, if any, on the local environment;

(c) The possible build up, and accumulation in the environment, of radioactive substances; and

(d) The possibility of there being any unauthorized routes for radioactive releases.

96. **Repeal.—** The "Regulation on the Safety of Nuclear Power Plants Design (PAK/911) (Rev.1)" notified vide S.R.O. 43(I)/2002 dated 21 January, 2002 are hereby repealed.

MOHAMMAD SALEEM ZAFAR,
Member (Corporate).

PRINTED BY THE MANAGER, PRINTING CORPORATION OF PAKISTAN PRESS, ISLAMABAD.
PUBLISHED BY THE DEPUTY CONTROLLER, STATIONERY AND FORMS, UNIVERSITY ROAD, KARACHI.