الهيئة الاتحادية للرقابة النووية

FANR

Federal Authority for Nuclear Regulation

Regulation

Regulation for the Design of Nuclear Power Plants (FANR-REG-03)

Version 0

Federal Authority for Nuclear Regulation (FANR)
P.O. Box 112021, Abu Dhabi, United Arab Emirates.
regulation@fanr.gov.ae

Contents

Definitions

Article (1)

For purposes of this regulation, the following terms shall have the meanings set forth below. Other capitalised terms used but not defined herein shall have the meaning ascribed to them in Article 1 of the Federal Law by Decree No. 6 of 2009 Concerning the Peaceful Uses of Nuclear Energy (the Law):

Active Component	A component whose functioning depends on an external input such as actuation, mechanical movement or supply of power.
Accident Conditions	Deviations from Normal Operation more severe than Anticipated Operational Occurrences, including DBAs and Severe Accidents.
Accident Management	The taking of a set of actions during the evolution of a beyond DBA: • to prevent the escalation of the event into a Severe Accident; • to mitigate the consequences of a Severe Accident; and • to achieve a safe stable state in the long term.
ALARA	As Low As Reasonably Achievable
Anticipated Operational Occurrence	An operational process deviating from Normal Operation which is expected to occur at least once during the operating lifetime of a Nuclear Facility but which, in view of appropriate Design provisions, does not cause any significant damage to Items Important to Safety or lead to Accident Conditions.
Beyond Design Basis Threats (BDBT)	A threat, identified in the Assessment that, while not included in the Design Basis Threat, remains credible. Threats beyond the DBT need to be taken into account to ensure the Physical Protection of Nuclear Facilities
Channel	An arrangement of interconnected components within a system that initiates a single output. A Channel loses its identity where single output signals are combined with signals from other Channels (e.g. from a monitoring Channel or a Safety actuation Channel).
Common Cause Failure	Failure of two or more SSCs due to a single specific event or cause

Control Systems	Instrumentation, hardware and software used to monitor, maintain or change the Operating State of the plant systems or components. Control Systems are functionally independent of the Protection Systems required Safety Systems actuation (although some components, such as sensors, may be shared).
Cyber Security	The protection of equipment, systems, and networks against attacks by individuals or organisations that would seek to cause harm, damage, or adversely affect the confidentiality, integrity, or availability of an information system or that seek to use an information control system for an unauthorized purpose that will affect the functions performed by such equipment, systems, and networks. Cyber Security provides a high assurance that digital computer, network and communication systems are adequately protected against cyber attacks up to and including the DBT.
Defence-in-Depth	A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of Anticipated Operational Occurrences and to maintain the effectiveness of physical barriers placed between a Radiation Source or Radioactive Material and workers, members of the public or the environment, in Operational States and, for some barriers, in Accident Conditions.
Design Basis Accident (DBA)	Accident Conditions against which a Nuclear Facility is designed according to established Design criteria, and for which the damage to the fuel and the release of Radioactive Material are kept within authorized limits.
Design Basis Threat (DBT)	The attributes and characteristics of potential insiders and/or external adversaries who might attempt unauthorised removal of Nuclear Material or sabotage, against which a Physical Protection System is designed and evaluated.
Diversity	The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of Common Cause Failure.
Dust Storm	Particles of dust energetically lifted by a strong and turbulent wind. Dust Storms are usually associated with hot, dry, and windy conditions. Dust particles typically have a diameter less than 0.08 mm and consequently can be lifted to far greater heights than sand
Functional Isolation	Prevention of influences from the mode of Operation or

failure of one circuit or system on another.

Independent Safety Verification (ISV)	A written verification performed by suitably qualified and experienced individuals, who did not participate in the original Safety Assessment, to determine whether the approach taken in conducting such Safety Assessment was reasonable and in accordance with international best practice.
Items Important to Safety	An item that is part of a Safety Group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public, including: Those SSCs whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public; Those SSCs that prevent Anticipated Operational Occurrences from leading to Accident Conditions; Those features that are provided to mitigate the consequences of malfunction or failure of SSCs.
Operational States	States defined under Normal Operation and Anticipated Operational Occurrences.
Normal Operation	Operation within specified operational limits and conditions. for a Nuclear Facility this includes start-up, power operation (including low power), shutting down and shutdown, maintenance, testing and refuelling
Passive Component	A component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power.
Physical Separation	Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.
Plant States.	Includes Operational States and accident states. Operational states consist of Normal Operation and Anticipated Operational Occurrences. Accident Conditions consist of DBAs and beyond DBAs
Postulated Initiating Event (PIE)	An event identified in Design as leading to Anticipated Operational Occurrences or Accident Conditions. This means that a PIE is not an accident itself; it is the event that initiates a sequence and that leads to an operational occurrence, a DBA or a Severe Accident depending on the additional failures that occur. Typical examples are: equipment failures (including pipe breaks), human errors,

	human induced events and natural events.
Probabilistic Risk Assessment (PRA)	A comprehensive, structured approach to identifying failure scenarios constituting a conceptual and mathematical tool for deriving numerical estimates of risk. Level 1 comprises the Assessment of failures leading to the determination of the frequency of core damage. Level 2 constitutes the Assessment of containment response and leads to the determination of frequency of containment failure resulting in release to the environment of a given percentage of the reactor core's inventory of radionuclides.
Protection System	System which monitors the Operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.
Redundancy	Provision of alternative (identical or diverse) SSCs, so that any one can perform the required function regardless of the state of operation or failure of any other.
Safety Function	A specific purpose that must be accomplished for Safety.
Safety Group	The assembly of equipment designated to perform all actions required for a particular PIE to ensure that the limits specified in the design basis for Anticipated Operational Occurrences and DBAs are not exceeded.
Safety System	A system important to Safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of Anticipated Operational Occurrences and DBAs.
Safety System Settings	The levels at which protective devices are automatically actuated in the event of Anticipated Operational Occurrences or Accident Conditions, to prevent Safety limits being exceeded.
Sandstorm	An ensemble of particles of sand energetically lifted by a strong and turbulent wind. The forward portion of the sandstorm may have the appearance of a wide and high wall. The height to which sand is raised will increase with increasing wind speed and instability.
Severe Accidents	Accident Conditions more severe than a DBA and involving significant core degradation
Single Failure	A failure which results in the loss of capability of a component to perform its intended Safety Function(s), and any consequential failure(s) which result from it.

Single Failure Criterion	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
Structures, Systems and Components (SSCs)	A general term encompassing all the elements of a Facility or Activity which contributes to protection and Safety, except human factors. Structures are the passive elements such as building vessels and shielding. A System comprises several components assembled in such a way as to perform a specific active function and a Component is a discrete element of a system.
Ultimate Heat Sink	A medium into which the residual heat can always be transferred, even if all other means of removing the heat have been lost or are insufficient.

Objective and Scope

Article (2)

1. The objective of this regulation is to establish the requirements for the Design of one or more Nuclear Power Plant. The regulation establishes Design requirements for SSCs important to Safety that must be met for safe operation of a Nuclear Facility, and for preventing or mitigating the consequences of potential events that could jeopardise Safety. It also establishes requirements for a comprehensive Safety Assessment, which is carried out in order to identify the potential hazards that may arise from the Operation of the Nuclear Facility, under the various Plant States (Operational States and incident/Accident Conditions). The Safety Assessment process includes the complementary techniques of deterministic Safety analysis and Probabilistic Risk Assessment.

2. This regulation applies to any applicant seeking a License to construct or operate a Nuclear Facility in the State, or any Licensee operating a Nuclear Facility in the State.

Article (3)

1. The scope of this regulation covers the principal requirements for the Design of a Nuclear Power Plants, including the requirements for Defence-in-Depth and Radiation Protection, general Nuclear Facility Design requirements and Design requirements applicable to specific plant SSCs.

2. Design requirements related to Physical Protection of Nuclear Materials and Nuclear Facilities, including Physical Protection System, access authorisation and control, protection against potential insider threats, Cyber Security, Safety and security interface, and the development of Nuclear Security plan are organised under FANR-REG-08: Regulation for the Physical Protection for Nuclear Materials and Nuclear Facilities.

3. For Beyond Design Basis Threat, Article 41 of this regulation identifies the need for plant-specific Assessments, which allow for the use of different acceptance criteria from the design process, for the impact and consequences of the loss of large areas of the Nuclear Facility due to large fires and explosions stemming from any malicious cause.

General Requirements

Article (4)

1. SSCs important to Safety shall be designed according to internationally recognised codes and standards and shall be of a Design proven by experience analysis and test and shall be selected to be consistent with the plant reliability goals necessary for Safety. Codes and standards shall be identified, and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to ensure that the final quality is commensurate with the necessary Safety Function.
2. Where an unproven Design or feature is introduced or there is a departure from an established engineering practice, Safety shall be demonstrated to be adequate by means of appropriate supporting research programmes, performance tests with specific acceptance criteria, and the examination of operational experience from other relevant applications. New Designs or features shall be adequately tested before being brought into service and shall be monitored in service, to verify that the expected behaviour is achieved.
3. In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes (e.g. failure to trip when necessary). Where failure of a SSC has to be expected and accommodated by the Design, preference shall be given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.

Article (5)

1. A Safety Assessment shall be carried out to confirm that the Design as delivered for fabrication, for Construction and as built meets the Safety requirements set out at the beginning of the Design process.
2. The Safety Assessment shall be part of the Design process, with iteration between the Design and confirmatory analytical activities, and increasing in the scope and level of detail as the design programme progresses.
3. The basis for the Safety Assessment shall be data derived from the Safety analysis (which includes the PRA), previous Construction and operational experience, results of supporting research and proven engineering practice.
4. Lessons Learned and Safety Research - The Design shall take due account of relevant Design, fabrication, Construction, Commissioning, operating and Decommissioning experience that has been gained from other Nuclear Facilities and of the results of relevant research programmes.

Article (6)

The applicant/Licensee shall ensure that an ISV of the Safety Assessment is performed before the Design is submitted to the Authority.

Principal Technical Requirements

Article (7)

1. In the design process, Defence-in-Depth shall be incorporated. The Design therefore shall:

    a. provide multiple physical barriers to the uncontrolled release of Radioactive Materials to the environment;

    b. provide Safety margin, and the Construction shall be of high quality, so as to provide confidence that plant failures and deviations from Normal Operations are minimised and accidents prevented;

    c. provide for control of the Nuclear Facility behaviour during and following events, using inherent and engineered features

    d. provide for supplementing control of the Nuclear Facility, by the use of automatic activation of Safety Systems to minimise operating personnel actions in the early phase of PIEs,

    e. provide for equipment and procedures to control the course and limit the consequences of accidents; and

    f. Provide multiple means for ensuring that each of the fundamental Safety Functions, i.e. control of the reactivity, heat removal, and the confinement of Radioactive Materials is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any PIEs.

2. To maintain Defence-in-Depth, the Design shall prevent as far as practicable:

    a. Challenges to the integrity of physical barriers;

    b. Failure of a barrier when challenged; and

    c. Failure of a barrier as a consequence of failure of another barrier.

3. The Design shall take into account the fact that the existence of multiple levels of defence is not a sufficient basis for continued power Operation in the absence of one level of defence. All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.

4. The objective of the Safety approach shall be:

a. to provide adequate means to maintain the Nuclear Facility in a Normal Operational state;

b. to ensure the proper short term response immediately following a PIE; and

c. To facilitate the management of the Nuclear Facility in and following any DBA, and in those selected Accident Conditions beyond the DBAs.

Article (8)

1. To ensure Safety, the following fundamental Safety Functions shall be performed in Operational States, in and following a DBA and, to the extent practicable, on the occurrence of those selected Accident Conditions that are beyond the DBAs:

    a. Control of reactivity;

    b. Removal of heat from the core;

    c. Confinement of Radioactive Materials and control of operational Discharges, as well as limitation of accidental releases.

2. A systematic approach shall be followed to identify the SSCs that are necessary to fulfil the Safety Functions at the various times following a PIE.

Article (9)

The plant Design for accident prevention and plant Safety characteristics shall be such that its sensitivity to PIEs is minimised. The expected plant response to any PIE shall be as follows:

1. A PIE produces no significant Safety related effect or produces only a change in the Nuclear Facility towards a safe condition by inherent characteristics; or

2. Following a PIE, the Nuclear Facility is rendered safe by passive Safety features or by the action of Safety Systems that are continuously available to perform functions necessary to control the PIE ; or

3. Following a PIE, the Nuclear Facility is rendered Safe by the action of Safety Systems that need to be brought into service in response to the PIE; or

4. Following a PIE, the Nuclear Facility is rendered safe by specified procedural actions.

Article (10)

1. All actual and potential sources of radiation shall be identified and provision shall be made to ensure that sources are kept safe and secure under technical, physical and administrative control.

2. Measures shall be provided to ensure that radiation Doses to the public and to site personnel during Operation, including Maintenance and Decommissioning, do not exceed

prescribed limits (ref: FANR-REG-04; Regulation for Radiation Dose Limits and Optimisation of Radiation Protection for Nuclear Facilities) and also that protection is optimised in accordance with that regulation.

3. The Design shall have as an objective the prevention or, if this fails, the mitigation of radiation exposures resulting from DBAs and selected Severe Accidents. Design provisions shall be made to ensure that potential radiation Doses to the public and the site personnel do not exceed the criteria approved by the Authority.

4. Plant States that could potentially result in high radiation Doses or radioactive releases shall be restricted to a very low likelihood of occurrence, and it shall be ensured that the potential radiological consequences of Plant States with a high likelihood of occurrence are small.

Requirements for Plant Design

Safety Classification

Article (11)

1. All SSCs, including software for instrumentation and control (I&C), that are Items Important to Safety shall be identified and classified on the basis of their function and significance to Safety. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification.

2. The classification of SSCs important to safety should primarily be based on deterministic methods and complemented, where appropriate, by probabilistic methods and engineering judgment.

3. Appropriately designed interfaces shall be provided between SSCs of different classes to ensure that any failure in a system classified in a lower class will not propagate to a system classified in a higher class.

General Design Basis

Article (12)

1. The applicant/Licensee shall ensure that Design specifications are established such that the Authority's regulations will be met.

2. The design basis shall specify the necessary capabilities of the Nuclear Facility to cope with a specified range of Operational States and DBAs within the defined radiological protection criteria established by the Authority. The design basis shall include the specification for Normal Operation, Plant States created by the PIEs, the Safety classification, important assumptions and, in some cases, the particular methods of analysis.

3. Conservative design measures and sound engineering practices shall be applied in the design bases for Normal Operation, Anticipated Operational Occurrences and DBAs so

as to provide a high degree of assurance that no significant damage will occur to the reactor core and that the Radiological Dose criteria approved by the Authority will be met for Normal Operation, Anticipated Operational Occurrences and DBAs.

4. The performance of the Nuclear Facility in Accidents beyond the design basis, including selected Severe Accidents shall also be addressed in the Design. Best-estimate methods and data; e.g., best estimate vs. Design allowable may be used for the purpose.

5. Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and anticipated operational states, and the use of additional temporary systems, to return the plant to a controlled state and/or to mitigate the consequences of a severe accident, provided that it can be shown that the systems are able to function in the environmental conditions to be expected.

Postulated Initiating Events (PIEs)

Article (13)

1. In the Design of the Power Plant, it shall be recognised that challenges to each level of Defence-in-Depth may occur and design measures shall be provided to ensure that the necessary Safety Functions are accomplished and the Safety objectives can be met. These challenges stem from the PIEs.

2. An analysis shall be made to establish all those PIEs that may affect the Safety of the Nuclear Facility including events that are internal to the Nuclear Facility, events that are external to the Nuclear Facility, and combinations of events The PIEs shall be selected on the basis of deterministic or probabilistic techniques or a combination of the two.

Internal Events

Article (14)

An analysis shall be made to establish all hose internal events that may affect the Safety of the Nuclear Facility. These events may include equipment failures or mal-operation, including those described in Articles 15 and 16.

Smoke, Fire and Explosions

Article (15)

1. SSCs important to Safety shall be designed and located so as to minimise, consistent with other Safety requirements, the probabilities and effects of smoke, fires and explosions caused by external or internal events within the design basis. The capability for shutdown, residual heat removal, confinement of Radioactive Material and monitoring of plant parameters shall be maintained. These requirements shall be met by suitable incorporation of redundant and diverse SSCs, Physical Separation and Design for fail-safe operation such that the following objectives are achieved:

a. to prevent fires from starting,

b. to detect and extinguish quickly those fires which do start, thus limiting the damage, and

c. to prevent the spread of those fires which have not been extinguished, thus minimising their effects on essential plant functions.

2. SSC's Important to Safety shall be designed and located to minimise, consistent with other safety requirements, the probability and effect of fires and explosions. A fire hazard analysis (which may include, as appropriate a fire PRA) of the Nuclear Facility shall be carried out to determine the necessary rating of the fire barriers, and fire detection and fire fighting systems of the necessary capability shall be provided.

3. Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located so as to ensure that their rupture or spurious failures or inadvertent Operation does not significantly impair the capability of SSCs important to Safety, and does not simultaneously affect redundant Safety Groups thereby rendering ineffective the measures taken to comply with the Single Failure Criterion.

4. Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the Nuclear Facility, particularly in locations such as the containment and the control room.

5. Internationally recognised fire protection codes and standards should be considered in the Design.

6. See Article 41 for the loss of large area of the Nuclear Facility due to fire and explosion stemming from beyond Design basis malicious acts.

Other Internal Hazards

Article (16)

1. The potential for other internal hazards such as flooding, missile generation, pipe whip, jet impact, or release of fluid from failed systems or from other installations on the site shall be taken into account in the Design of the Nuclear Power Plant. Appropriate preventive and mitigation measures shall be provided to ensure that Nuclear Safety is not compromised. Some external events may initiate internal fires, particulates or floods and may lead to the generation of missiles. Such interaction of external and internal events shall also be considered in the Design.

2. If two fluid systems that are operating at different pressures are interconnected, either the system operating at lower pressure shall be capable of withstanding the higher system pressure, or provision shall be made to preclude the design pressure of the system operating at the lower pressure from being exceeded, on the assumption that a Single Failure occurs.

External Events

Article (17)

1. The design basis natural and human induced external events shall be determined for the proposed combination of site and Nuclear Facility. All events with which significant radiological risk may be associated shall be considered. A combination of deterministic and probabilistic methods shall be used to select a subset of external events that the Nuclear Facility is designed to withstand, and from which the design bases are determined.

2. Natural external events shall be considered in the design process including those which have been identified in site characterisation, such as earthquakes, Dust storms/Sandstorms, cyclones, floods, high winds, tornadoes, tsunami (tidal waves) and extreme meteorological conditions. Human induced external events that shall be considered include those that have been identified in site characterisation and for which design bases have been derived.

Site Related Characteristics

Article (18)

1. For Site related characteristics, in determining the design basis of a Nuclear Facility, various interactions between the Nuclear Facility and the environment, including such factors as population, meteorology, hydrology, geology and seismology, shall be taken into account. The availability of off-site services upon which the Safety of the Nuclear Facility and protection of the public may depend, such as the electricity supply and fire fighting and security services shall also be taken into account.

2. Particular attention must be given to Sandstorms, Dust storms, extreme ambient temperatures, and the radiant energy from sunlight. Consideration must be given to the qualification of equipment to function in these environmental conditions, the ability of operating personnel to operate equipment and the ability of heating, ventilation and air conditioning (HVAC) systems to accommodate heat loads and the need to filter small particles to prevent degradation of equipment and effects on personnel.

Combinations of Randomly Occurring Individual Events

Article (19)

Where possible combinations of randomly occurring individual events could credibly lead to Anticipated Operational Occurrences or Accident Conditions, they shall be considered in the Design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original PIE.

Design Rules

Article (20)

1. The engineering Design rules for SSCs shall be specified and shall comply with recognised national standard engineering practices or those consensus codes and standards or practices already used internationally or established in another country and whose use is applicable and is accepted by the Authority

2. The Design including seismic) of the Nuclear Facility shall provide for a sufficient Safety margin to account for uncertainties in events, data and analytical models.

Design Limits

Article (21)

A set of Design limits consistent with the key physical parameters for each SSC shall be specified for Operational States and DBAs.

Operational States

Article (22)

1. The Nuclear Facility shall be designed to operate safely within a defined range of parameters (for example, of pressure, temperature, power), and a minimum set of specified support features for Safety Systems (for example, auxiliary feed water capacity and an Emergency electrical power supply) shall be assumed to be available. The Design shall be such that the response of the Nuclear Facility to a wide range of Anticipated Operational Occurrences will allow safe Operation or shutdown, if necessary, without the necessity of invoking provisions beyond the first, or at the most the second, level of Defence-in-Depth

2. The potential for Accidents to occur in low power and shutdown (LPSD) states, such as start-up, refuelling, maintenance and shutdown, when the availability of Safety Systems may be reduced and/or plant configurations maybe different from full power operation, shall be addressed in the Design, Safety analysis and PRA. Specifically, the Design shall include provisions to:

    a. Monitor and control reactivity during shutdown and refuelling such that the reactor is always maintained subcritical,

    b. Monitor water level and temperature in the reactor pressure vessel and have the capability to add make up water such that the active fuel is always covered

    c. Have the ability to quickly establish and maintain containment integrity in the event core cooling or reactivity limits are exceeded.

    d. Ensure high reliability of decay heat removal during LPSD conditions.

3. The design process shall establish a set of requirements and limitations for safe operation including:

    a. Safety System Settings;

    b. Control system and procedural constraints on process variables and other important parameters;

    c. Requirements for Maintenance, testing and Inspection of the Nuclear Facility to ensure that SSCs function as intended in the Design, with the ALARA principle taken into consideration;

    d. Clearly defined operational configurations, including operational restrictions in the event of Safety System outages; and

    e. Limiting conditions for Operation (including low power and shutdown) to ensure design specifications are met and low risk is maintained.

4. These requirements and limitations shall be a basis for the establishment of operational limits and conditions under which the licensee will be authorised to operate the Nuclear Facility.

Design Basis Accidents (DBAs)

Article (23)

1. A set of DBAs shall be derived from the listing of PIEs for the purpose of setting the boundary conditions according to which the SSCs Important to Safety shall be designed.

2. Where prompt and reliable action is necessary in response to PIEs, provision shall be made to initiate the necessary actions of Safety Systems automatically. Where prompt action is not necessary, manual initiation of systems or other operating personnel actions may be permitted, provided that the need for the action be revealed in sufficient time and that adequate procedures (such as administrative, operational and Emergency procedures) and training be defined to ensure the reliability of such actions.

3. The operating personnel actions that may be necessary to diagnose the state of the Nuclear Facility and to put it into a stable long term shutdown condition in a timely manner shall be taken into account and facilitated by the provision of adequate instrumentation and procedures to monitor the plant status and controls for manual operation of equipment.

4. Any equipment necessary in manual response and recovery processes shall be placed at the most suitable location to ensure its ready availability at the time of need and to allow human access in the anticipated environmental conditions.

Severe Accidents

Article (24)

1. Certain very low probability plant states that are beyond DBA conditions and which may arise owing to multiple failures of Safety Systems leading to significant core degradation may jeopardise the integrity of many or all of the barriers to the release of radioactive material. These event sequences are called Severe Accidents. Consideration shall be given to severe accidents by providing in the design reasonably practicable preventive and/or mitigative measures. These measures need not involve the application of conservative engineering practices used in setting and evaluating DBAs, but rather should be based upon realistic or best estimate assumptions, methods and analytical criteria. On the basis of operational experience, relevant safety analysis and results from safety research, design activities shall take into account the following :

   a. Provisions to promote in-vessel core melt retention

   b. Provisions to prevent and/or withstand in-vessel and ex-vessel steam explosion

   c. Provisions for combustible gas control

   d. Provisions for mitigation of molten core debris concrete interaction

   e. Provisions to prevent and mitigate high pressure core melt ejection from the Reactor Pressure Vessel

   f. Provisions to prevent early containment failure under severe accident conditions

   g. Accident Management procedures shall be established, taking into account representative and dominant Severe Accident scenarios

   h. The effectiveness of the severe accident measures shall be confirmed by demonstrating that the Authority's safety target is met.

   i. Articles 47, 76 and 80 identify measures that intended to reduce the likelihood of some scenarios that were leading contributor to severe accidents, namely: Pressurised Thermal Shock (PTS) Anticipated Transient without Scram (ATWS) and Station Blackout (SBO).

Design for Reliability of SSCs

Article (25)

1. SSCs important to Safety shall be designed to be capable of withstanding Anticipated Operational Occurrences and DBAs associated with all PIEs with sufficient reliability and consistent with assumptions in the PRA and with sufficient reliability.

2. The potential for Common Cause Failures of Items Important to Safety shall be considered to determine where the principles of Diversity, Redundancy and independence shall be applied to achieve the necessary reliability.

Single Failure Criterion

Article (26)

1. The Single Failure criterion shall be applied to each Safety Group incorporated in the Nuclear Facility Design [Note: In this publication, Safety Functions, or systems contributing to performing those Safety Functions, for which Redundancy is necessary to achieve the necessary reliability have been identified by the statement 'on the assumption of a single failure]

2. Fluid and electric systems are considered to be designed against an assumed Single Failure if neither (1) a Single Failure of any Active Component (assuming Passive Component function properly) nor (2) a Single Failure of any Passive Component (assuming Active Components function properly), results in a loss of the capability of the system to perform its Design intent.

3. Single Failure of a Passive Component of electrical systems should be assumed in designing against a Single Failure.

4. Any non-compliance with the Single Failure Criterion shall be exceptional, and shall be clearly justified in the Safety analysis.

5. In the Single Failure analysis, it may not be necessary to assume the failure of a Passive Component designed, manufactured, Inspected and maintained in service to an extremely high quality, provided that it remains unaffected by the PIE. However, when it is assumed that a Passive Component does not fail, such an analytical approach shall be justified, with account taken of the loads and environmental conditions, as well as the total period of time after the initiating event for which functioning of the component is necessary.

Article (27)

The principle of fail-safe Design shall be considered and incorporated into the Design of systems and components important to Safety for the Nuclear Facility as appropriate: if a system or component fails, plant systems shall be designed to pass into a safe state.

Auxiliary Services

Article (28)

Auxiliary services (e.g. supply of electricity, cooling water and compressed air or other gases, and means of lubrication) that support equipment forming part of a system important to Safety shall be considered part of that system and shall be classified accordingly. Their reliability, Redundancy, Diversity and independence and the provision of features for isolation and for testing of functional capability shall be commensurate with the reliability of the system that is supported.

Equipment Outages

Article (29)

The Design for equipment outages shall be such as to ensure that reasonable on-line Maintenance and testing of systems important to Safety can be conducted without shutting down the Nuclear Facility or putting the Nuclear Facility into a configuration that results in unacceptable risk and with an acceptable level of risk to shutdown the Nuclear Facility. The time allowed for equipment outages and the actions to be taken shall be analysed using PRA or other engineering justifications and defined for each case before the start of Nuclear Facility Operation based on risk considerations and included in the Nuclear Facility operating instructions.

Article (30)

The Design for reliability shall consider the environmental conditions, including the harsh environmental conditions caused by Sandstorms, Dust Storms, and extreme ambient temperatures. Single-Failure considerations shall be applied to temperature control and air filtration systems that provide assurance of achieving the design basis environmental conditions for equipment applicable to Single-Failure Design.

Design for Security

Article (31)

1. Security related Design features including location and physical layout of the site, layout of buildings and structures, topographical features of the surrounding area, physical barriers and access controls shall be considered consistent with the requirements in FANR REG-08, Regulation for Nuclear Facility Security.
2. The Design shall consider the interfaces and interactions between Safety and security so that one does not compromise the other and Operations are safe and secure.

Equipment Qualification

Article (32)

A qualification procedure shall be adopted to confirm that Items Important to Safety are capable of meeting, throughout their Design operational lives, the demands for performing their functions while being subject to the environmental conditions (e.g., vibration, temperature, pressure, jet impingement, electromagnetic interference, irradiation, humidity, exposure to fine particles (as may be caused by Sandstorms or Dust Storms) or any likely combination thereof) prevailing at the time of need. The environmental conditions to be considered shall include the variations expected in Normal Operation, Anticipated Operational Occurrences and DBAs. In the qualification programme, consideration shall be given to ageing effects caused by various environmental factors (such as vibration, irradiation and extreme temperature) over the expected lifetime of the equipment. Where the equipment is subject to external natural events and is needed to perform a Safety Function in or following such an event, the qualification programme shall replicate as far as practicable the conditions imposed on the equipment by the natural phenomenon. Items can be qualified either by test or by analysis or by a combination of both.

Provision for In-Service Testing, Maintenance, Repair, Inspection and Monitoring

Article (33)

1. SSCs Important to Safety shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability over the lifetime of the Nuclear Facility to demonstrate that design bases and reliability targets are being met. The Nuclear Facility layout shall be such that these activities are facilitated and can be performed to standards commensurate with the importance of the Safety Functions to be performed, with no significant reduction in system availability and without undue exposure of the site personnel to radiation.
2. If the SSCs important to Safety cannot be designed to be able to be tested, inspected or monitored to the extent desirable, then a proven alternative and/or indirect method such as surveillance of reference items or use of verified and validated calculational methods shall be specified.

Ageing

Article (34)

Appropriate margins shall be provided in the Design for all SSCs important to Safety so as to take into account relevant ageing, wear mechanisms embrittlement and other potential age related degradation, in order to ensure the capability of the structure, system or component to perform the necessary Safety Function throughout its design life. Ageing and wear effects in all normal operating conditions, testing, Maintenance, Maintenance outages, and Plant States in a PIE and post-PIE shall also be taken into account. Provision shall also be made for monitoring, testing, sampling and Inspection, to assess ageing mechanisms identified and predicted at the Design stage, and to identify unanticipated behaviour or degradation that may occur in service and for periodic equipment replacement or comparable preventive Maintenance programme.

Human Factors - Design for Optimal Operating Personnel Performance

Article (35)

1. The design shall be 'operator friendly' and shall be aimed at limiting the effects of human errors. Attention shall be paid to plant layout and procedures (administrative, Operational and Emergency), including Maintenance and Inspection, to facilitate the interface between the operating personnel and the Nuclear Facility.

2. Systematic consideration of human factors and the human–machine interface shall be included in the design process at an early stage and shall continue throughout the entire process, to ensure an appropriate and clear distinction of functions between operating personnel and the automatic systems provided.

3. The human–machine interface shall be designed to provide the operating personnel with comprehensive but easily manageable information, compatible with the necessary decision and action times. Similar provisions shall be made for the supplementary Control Room.

4. Verification and validation of aspects of human factors shall be included at appropriate stages to confirm that the Design adequately accommodates all necessary operating personnel actions.

5. To assist in the establishment of design criteria for information display and controls, the operating personnel shall be considered to have dual roles: that of a systems manager, including Accident Management, and that of an equipment operating personnel.

6. In the systems manager role, the operating personnel shall be provided with information that permits the following: (1) the ready Assessment of the general state of the Nuclear Facility in whichever condition it is, whether in Normal Operation, in an Anticipated Operational Occurrence or in an Accident Condition, and confirmation that the designed automatic Safety actions are being carried out; and (2) the determination of the appropriate operating personnel initiated Safety actions to be taken.

7. As equipment operating personnel, the operating personnel shall be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the necessary Safety actions can be initiated safely.

8. The Design objectives shall include promoting the success of operating personnel actions with due regard for the time available for action, the physical environment to be expected and the psychological demands to be made on the operating personnel. The need for intervention by the operating personnel on a short time-scale shall be kept to a minimum.

9. Any equipment necessary in manual response and recovery processes shall be located to ensure its ready availability at the time of need and to allow human access in the anticipated environmental conditions

Other Design Considerations

Article (36)

Sharing of items Important to Safety between nuclear power plant units for the purpose of accident management shall be permitted only provided that it has been demonstrated that such sharing does not prevent the other units from performing all Safety functions on the assumption of a single failure. Systems that are not safety systems may be shared between several units provided that such sharing would not increase either the likelihood or the consequences of a severe accident.

Article (37)

All systems within a Nuclear Facility that may contain fissile or Radioactive Materials shall be designed to maintain their integrity during Operational States and in DBAs.

Article (38)

Nuclear Facilities coupled with heat utilisation units (such as for district heating) and/or water desalination units shall be designed to prevent transport of Radioactive Materials from the Nuclear Facility to the desalination or district heating unit under any condition of Normal Operation, Anticipated Operational Occurrences, DBAs and Severe Accidents.

Article (39)

The Design shall incorporate appropriate features to facilitate transport and handling of fresh fuel, Spent Nuclear Fuel and Radioactive Waste. Consideration shall be given to access to facilities and lifting and packaging capabilities.

Article (40)

1. The Nuclear Facility shall be provided with a sufficient number of safe escape routes, clearly and durably marked with reliable Emergency lighting, ventilation and other building services essential to the safe use of these routes. The escape routes shall meet the relevant international requirements for radiation zoning and fire protection and the relevant national requirements for industrial Safety and Nuclear Facility security.
2. Suitable alarm systems and means of communication shall be provided so that all persons present in the Nuclear Facility and on the site can be warned and instructed, even under Accident Conditions.
3. The availability of diverse means of communication necessary for Safety, within the Nuclear Facility, as stipulated in the Emergency Plan, shall be ensured at all times.

Article (41)

The applicant/licensee shall perform a design-specific assessment of the potential effects of the impact of a large, commercial aircraft. The Authority's requirements that apply to the design, construction, testing, operation, and maintenance of design features and fictional capabilities selected by the applicant/licensee solely to meet design-basis events will not apply to beyond-design basis events. These Assessments shall use best-estimate, realistic analyses to identify and incorporate imminent threat procedures, spent fuel management schemes, design features, and functional capabilities to avoid or mitigate the effects of those malicious acts by showing 1) that for a reactor accident: either the reactor core remains cooled or the containment remains intact or demonstrate how is the risk compares against the Authority's probabilistic targets of core damage frequency and large release frequency, and 2) that for spent fuel storage accidents: either spent fuel cooling or spent fuel integrity is maintained or demonstrate how is the risk compares against the Authority's probabilistic targets, such that public health and Safety and the environment are protected.

Interaction of Systems

Article (42)

If there is a probability that it will be necessary for systems (Items) Important to Safety to operate simultaneously, their possible interaction shall be evaluated. In the analysis, account shall be taken not only of physical interconnections, but also of the possible effects of one system's Operation, mal-operation or failure on the physical environment of other essential systems, in order to ensure that changes in the environment do not affect the reliability of system components in functioning as intended.

Decommissioning

Article (43)

1. At the Design stage, consideration shall be given to the incorporation of features that will facilitate the Decommissioning and dismantling of the Nuclear Facility. In particular, account shall be taken in the Design of:

    a. The choice of materials, such that eventual quantities of Radioactive Waste are minimised and decontamination is facilitated;

    b. The access capabilities that may be necessary; and

    c. The facilities necessary for storing Radioactive Waste generated in both Operation and Decommissioning of the Nuclear Facility.

2. Provisions shall be established for monitoring throughout the life of the Nuclear Facility on-site environmental parameters that could affect Decommissioning.

Safety Analysis

Article (44)

1. A Safety Analysis of the Nuclear Facility Design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied. On the basis of this analysis, the design basis for Items Important to Safety shall be established and confirmed. It shall also be demonstrated that the Nuclear Facility as designed is capable of meeting any approved limits or criteria for radioactive releases and potential radiation Doses for each category of plant Operation and that Defence-in-Depth will be maintained
2. The computer programmes, analytical methods and plant models used in the Safety analysis shall be verified and validated, and consideration shall be given to uncertainties.

Article (45)

1. The deterministic Safety analysis shall include the following:
   a. Confirmation that operational limits and conditions are in compliance with the assumptions and intent of the Design for Normal Operation of the Nuclear Facility;
   b. Use of source terms that are consistent with the accident sequences and phenomena associated with the events being analysed.
   c. Characterisation of the PIEs that are appropriate for the Design and site of the Nuclear Facility;
   d. Analysis and evaluation of event sequences that result from design basis PIEs;
   e. Comparison of the results of the analysis with radiological acceptance criteria and design Safety limits;
   f. Establishment and confirmation of the design basis; and
   g. Demonstration that the management of Anticipated Operational Occurrences and DBAs is possible by automatic response of Safety Systems in combination with prescribed actions of the operating personnel.
2. The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified. The Safety analysis of the Nuclear Facility Design shall be updated with regard to significant changes in plant configuration, operational experience, and advances in technical knowledge and understanding of physical phenomena, and shall be consistent with the current or “as built” state.

Article (46)

A Design and site specific PRA shall be performed and a summary report shall be submitted to the Authority for review. The PRA shall be conducted in accordance with FANR-REG-05, Regulation for the Application of PRA at Nuclear Facilities. The results of the PRA shall be considered in the Design of the Power Plant.

Requirements for Design of Plant Systems - Reactor Core and Associated Features

Article (47)

1. The reactor core and associated coolant, control and Protection Systems shall be designed with appropriate margins to ensure that the specified design limits are not exceeded and that radiation Safety standards are applied in all Operational States and in DBAs, with account taken of the existing uncertainties.

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, DBAs and external events to the extent necessary to ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure cooling of the core.

3. The maximum degree of positive reactivity and its maximum rate of increase by insertion in Operational States and DBAs shall be limited so that no resultant failure of the reactor pressure boundary will occur, cooling capability will be maintained and no significant damage will occur to the reactor core.

4. The Design shall ensure that the possibility of re-criticality or reactivity excursion following a design-basis PIE is minimised.

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 Nuclear Facility.

Fuel Elements and Assemblies

Article (48)

1. Fuel elements and assemblies shall be designed to withstand the anticipated irradiation and environmental conditions in the reactor core in combination with all processes of deterioration that can occur in Normal Operation and in Anticipated Operational Occurrences.

2. Specified fuel design limits shall not be exceeded in Normal Operation. Leakage of fission products shall be restricted by Design limits and kept to a minimum.

3. In DBAs, the fuel elements shall remain in position and shall not suffer distortion that would render post-accident core cooling shutdown or core cooling insufficiently effective; and the specified limits for fuel elements for DBAs shall not be exceeded.

4. Fuel assemblies shall be designed to permit adequate Inspection of their structure and component parts after irradiation

Control of the Reactor Core

Article (49)

1. The provisions of Articles 47(3), 47(4) and 48 shall be met for all levels and distributions of neutron flux that can arise, including those: following shutdown, during or after refuelling, during Anticipated Operational Occurrences, and during DBAs. Adequate means of detecting and suppressing spatial power oscillations shall be provided to ensure that there are no regions of the core in which the provisions of Articles 47(3), 47(4) and 48 could be breached without being detected. The Design of the core shall sufficiently reduce the demands made on the control system for maintaining flux shapes, levels and stability within specified limits in all Operational States.

2. Provision shall be made for the removal of non-radioactive substances, including corrosion products, which may compromise the Safety of the system, for example by clogging coolant Channels.

Reactor Shutdown

Article (50)

1. Means shall be provided to ensure that there is a capability to shut down the reactor in Operational States and DBAs, and that the shutdown condition can be maintained even for the most reactive core conditions including a Single Failure of the rod with the highest reactivity worth. The effectiveness, speed of action and shutdown margin of the means of shutdown shall be such that the Design Safety limits are not exceeded. For the purpose of reactivity control and flux shaping in normal power operation, a part of the means of shutdown may be used provided that the shutdown capability is maintained with an adequate margin at all times.

2. The means for shutting down the reactor shall consist of at least two different systems to provide Diversity.

3. At least one of the two systems shall be capable, on its own, of quickly rendering the Nuclear Reactor subcritical by an adequate margin from Operational States and in DBAs, on the assumption of a Single Failure. Exceptionally, a transient re-criticality may be permitted provided that the specified fuel and component limits are not exceeded.

4. At least one of these two systems shall be capable, on its own, of rendering the reactor subcritical from Normal Operational states, in Anticipated Operational Occurrences and in DBAs, and of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the core.

5. In judging the adequacy of the means of shutdown, consideration shall be given to failures arising anywhere in the Nuclear Facility that could render part of the means of shutdown inoperative (such as failure of the most active control rod to insert) or could result in a Common Cause Failure.

6. The means of shutdown shall be adequate to prevent or withstand inadvertent increases in reactivity by insertion during shutdown, including refuelling. In meeting this provision, deliberate actions that increase reactivity in the shutdown state (such as absorber

movement for Maintenance, dilution of boron content and refuelling actions) and a Single Failure in the shutdown means shall be taken into account.

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

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

Reactor Coolant System

Article (51)

1. The reactor coolant system, its associated auxiliary systems, and the control and Protection Systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded in Operational States. Provision shall be made to ensure that the operation of pressure relief devices, even in DBAs, will not lead to releases of Radioactive Material from the Nuclear Facility exceeding criteria established by the Authority. The reactor coolant pressure boundary shall be equipped with adequate isolation devices to limit any loss of radioactive fluid.

2. The component parts containing the reactor coolant, such as the reactor pressure vessel, piping and connections, valves, fittings, pumps and heat exchangers, together with the devices by which such parts are held in place shall be designed in to withstand the static and dynamic loads anticipated in all Operational States and in DBAs. The materials used in the fabrication of the component parts shall be selected so as to minimise activation of the material.

3. The reactor pressure vessel shall be designed and constructed to be of the highest quality with respect to materials, design standards, capability of Inspection and fabrication. The pressure retaining boundary for reactor coolant shall be designed so that flaws are very unlikely to be initiated, and any flaws that are initiated would propagate in a regime of high resistance to unstable fracture with fast crack propagation, to permit timely detection of flaws. Specifically, the applicant/Licensee shall propose fracture toughness criteria for protection of the Reactor Pressure Vessel against pressurised thermal shock (PTS) events that address projected values of RT_{PTS}, accepted by the Authority, for each reactor vessel beltline material for the *End Of Life fluence* of the material; where:

    a. RT_{PTS} means the reference temperature, RT_{NDT}, evaluated for the EOL fluence for each of the vessel beltline materials,

    b. RT_{NDT} means the reference temperature for a reactor vessel material, under any conditions. For the reactor vessel beltline materials, RT_{NDT} must account for the effects of neutron radiation, and

    c. End of Life (EOL) fluence means the best-estimate neutron fluence projected for a specific vessel beltline material at the clad-base-metal interface on the inside surface of the vessel at the location where the material receives the highest fluence on the expiration date of the operating license.

4. The Design shall consider all conditions to which the boundary material is subjected in Operational States, including those for Maintenance and testing, and under DBA 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.

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 minimise the likelihood of failure and associated consequential damage to other items of the primary coolant system important to Safety in all Operational States and in DBAs, with due allowance made for deterioration that may occur in service.

In-Service Inspection of the Reactor Coolant Pressure Boundary

Article (52)

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 Nuclear Facility, to carry out at appropriate intervals adequate Inspections and tests of the boundary. Provision shall be made to implement a material surveillance programme 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.

2. 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.

3. 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 the determination of which Inspections are necessary for Safety.

4. It shall be ensured that it is possible to inspect the relevant parts of the secondary cooling system for which the Safety analysis of the Nuclear Facility indicates particular failures may result in serious consequences.

Inventory of Reactor Coolant

Article (53)

Provision shall be made for controlling the inventory and pressure of coolant to ensure that specified design limits are not exceeded in any Operational State, with volumetric changes and leakage taken into account. The systems performing this function shall have adequate capacity (flow rate and storage volumes) to meet this requirement. They may be composed of components needed for the processes of power generation or may be specially provided for performing this function.

Clean-up of the Reactor Coolant

Article (54)

Adequate facilities shall be provided for removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel. The capability of the necessary systems shall be based on the specified fuel design limit on permissible leakage with a conservative margin to ensure that the Nuclear Facility can be operated with a level of circuit activity which is as low as reasonably practicable, and that radioactive releases meet the ALARA principle and are within the prescribed limits.

Removal of Residual Heat from the Core

Article (55)

1. Means for removing residual heat shall be provided. Their Safety Function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified fuel design limits and the design basis limits of the reactor coolant pressure boundary are not exceeded.

2. Interconnections and isolation capabilities and other appropriate design features (such as leak detection) shall be provided such that the system provides sufficient reliability, on the assumptions of a Single Failure and the loss of off-site power, and with the incorporation of suitable Redundancy, Diversity and independence.

Emergency Core Cooling

Article (56)

1. Core cooling shall be provided in the event of a loss of coolant Accident so as to minimise fuel damage and limit the escape of fission products from the fuel. The cooling provided shall ensure that:

    a. The limiting parameters for the cladding or fuel integrity (such as peak temperature and cladding oxidation) will not exceed the acceptable value for DBAs.

    b. Possible chemical reactions are limited to an allowable level;

    c. The alterations in the fuel and internal structural alterations will not significantly reduce the effectiveness of the means of Emergency core cooling; and

    d. Cooling of the core shall be ensured with sufficient margin and for a sufficient time to ensure fuel integrity limits are maintained.

2. Design features (such as leak detection, appropriate interconnections and isolation capabilities) and suitable Redundancy in components shall be provided in order to fulfil these requirements with sufficient reliability for each PIEs, on the assumption of a Single Failure.
3. Adequate consideration shall be given to extending the capability to remove heat from the core so that, following a Severe Accident acceptable temperatures can be maintained in SSCs important to the safety function of confinement of Radioactive Materials.
4. The applicant/Licensee shall ensure that the Emergency core cooling system pumps are provided with adequate margin between the available and the required net positive suction head to prevent pump cavitations and the attendant improper Operation of the Emergency core cooling system following design basis events. The applicant/Licensee shall perform a mechanistic evaluation of the emergency core cooling recirculation functions with account taken of the potential susceptibility of recirculation sump screens and associated flow paths to debris blockage that might impede the long-term Operation of the Emergency core cooling system or containment spray system. The applicant/Licensee shall also ensure that its evaluation account for the potential for debris passing through sump screens and affect equipment downstream (such as valves, pumps, and Nuclear Fuel assemblies).

Article (57)

The Emergency core cooling system shall be designed to permit appropriate periodic Inspection of important components and to permit appropriate periodic testing to confirm the following:

1. The structural integrity and leak tight integrity of its components;
2. The operability and performance of the Active Components of the system in Normal Operation, as far as feasible; and
3. The operability of the system as a whole under the Plant States specified in the design basis, to the extent practicable.

Heat Transfer to an Ultimate Heat Sink

Article (58)

1. Systems shall be provided to transfer residual heat from SSCs important to Safety to an Ultimate Heat Sink. This function shall be carried out at high levels of reliability in Operational States and in DBAs. All systems that contribute to the transport of heat (by conveying heat, by providing power or by supplying fluids to the heat transport systems) shall be designed in accordance with the importance of their contribution to the function of heat transfer as a whole.
2. The reliability of the systems that transfer heat to the Ultimate Heat Sink shall be achieved by an appropriate choice of measures including the use of proven components, Redundancy, Diversity, Physical Separation, interconnection and isolation.

3. Natural phenomena and human induced events shall be taken into account in the Design of the systems that transfer heat to the Ultimate Heat Sink and in the possible choice of Diversity in the Ultimate Heat Sinks and in the storage systems from which fluids for heat transfer are supplied.

4. Adequate consideration shall be given to extending the capability to transfer residual heat from the core to an Ultimate Heat Sink so as to ensure that, in the event of a Severe Accident, acceptable temperatures can be maintained in SSCs important to the Safety Function of confinement of Radioactive Materials.

Containment System

Article (59)

1. A containment system shall be provided in order to ensure that any release of Radioactive Materials to the environment in a DBA would be below limits approved by the Authority. This system may include, depending on design requirements: leak tight structures; associated systems for the control of pressures and temperatures; and features for the isolation, management and removal of fission products, hydrogen, oxygen and other substances that could be released into the containment atmosphere.

2. All identified DBAs shall be taken into account in the Design of the containment system. In addition, consideration shall be given to the provision of features for the mitigation of the consequences of selected Severe Accidents in order to limit the release of Radioactive Material to the environment.

Article (60)

1. The strength of the containment structure, including access openings and penetrations and isolation valves, shall be designed with sufficient margins of Safety on the basis of the potential internal over-pressures, under-pressures and temperatures, dynamic effects such as missile impacts, and reaction forces anticipated to arise as a result of DBAs. 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 phenomena 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.

2. Provision for maintaining the integrity of the containment in the event of a severe accident shall be considered. In particular, the effects of any predicted combustion of flammable gases shall be taken into account.

Containment Pressure Testing and Leakage

Article (61)

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 Nuclear Facility and over the Nuclear Facility’s lifetime.

Article (62)

1. The containment system shall be designed so that the prescribed maximum leakage rate is not exceeded in DBAs.
2. The containment structure, and the equipment and components affecting the leak tightness of the containment system shall be designed and constructed so that the leak rate can be tested at the design pressure after all penetrations have been installed. The Design shall include provisions for the determination of the leakage rate of the containment system at periodic intervals over the service lifetime of the reactor, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure.

Containment Penetrations

Article (63)

1. The number of penetrations through the containment shall be kept to a minimum.
2. All penetrations through the containment shall meet the same design requirements as the containment structure itself. They shall be protected against reaction forces stemming from pipe movement or accidental loads such as those due to missiles, jet forces and pipe whip.
3. If resilient seals (such as elastomeric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have the capability for leak testing at the containment design pressure, independent of the determination of the leak rate of the containment as a whole, to demonstrate their continued integrity over the lifetime of the Nuclear Facility.
4. Consideration shall be given to the capability of penetrations to remain functional in the event of a Severe Accident.

Containment Isolation

Article (64)

1. Each line that penetrates the containment as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of a DBA in which the leak tightness of the containment is essential to preventing radioactive releases to the environment that

exceed prescribed limits. These lines shall be fitted with at least two containment isolation valves arranged in series (normally with one outside and the other inside the containment, but other arrangements may be acceptable depending on the Design), and each valve shall be capable of being reliably and independently actuated. Isolation valves shall be located as close to the containment as is practicable. Containment isolation shall be achievable on the assumption of a Single Failure. If the application of this requirement reduces the reliability of a Safety System that penetrates the containment, other isolation methods may be used.

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

3. Containment isolation valves shall be capable of operating in the timeframe necessary for them to perform their Safety Function.

4. Consideration shall be given to the capability of isolation devices to maintain their function in the event of a Severe Accident.

Article (65)

1. Access by personnel to the containment shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor operations and in DBAs. Where provision is made for entry of personnel for surveillance purposes during certain low power operations, provisions for ensuring the Safety of personnel in such operations shall be specified in the Design. These requirements shall also apply to equipment air locks, where provided.

2. Consideration shall be given to the capability of containment air locks to maintain their function in the event of a Severe Accident.

Internal Structures of the Containment

Article (66)

1. The Design shall provide for ample 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 DBAs do not result in damage to the pressure bearing structure or to other systems of importance in limiting the effects of DBAs.

2. Consideration shall be given to the capability of internal structures to withstand the effects of a Severe Accident.

Removal of Heat from the Containment

Article (67)

1. The capability to remove heat from the reactor containment shall be ensured. The Safety Function shall be fulfilled by reducing the pressure and temperature in the containment, and maintaining them at acceptably low levels, after any accidental release of high energy fluids in a DBA. The system performing the function of removing heat from the containment shall have adequate reliability and Redundancy to ensure that this can be fulfilled, on the assumption of a Single Failure.

2. Consideration shall be given to the capability to remove heat from the reactor containment in the event of a Severe Accident.

Control and Clean-up of the Containment Atmosphere

Article (68)

1. Systems to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment shall be provided as necessary. 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.

2. Consideration shall be given to the control of fission products, hydrogen and other substances that may be generated or released in the event of a Severe Accident.

Article (69)

1. The coverings and coatings for components and structures within the containment system shall be carefully selected, and their methods of application specified, to ensure fulfilment of their Safety Functions and to minimise interference with other Safety Functions in the event of deterioration of coverings and coatings.

2. Containment systems, including the sump, shall be designed to ensure that containment and system functions necessary to mitigate DBAs will be reliably performed considering generation of debris and other environmental conditions within the containment during the Accident.

Instrumentation and Control

Article (70)

1. Instrumentation shall be provided to monitor plant variables and systems over the respective ranges for Normal Operation, Anticipated Operational Occurrences, DBAs and Severe Accidents in order to ensure that adequate information can be obtained on the status of the Nuclear Facility. Instrumentation shall be provided for measuring all the main

variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information on the Nuclear Facility necessary for its reliable and safe Operation. Provision shall be made for automatic recording of measurements of any inputs to derived parameters or derived parameters that are important to Safety, such as the sub-cooling margin of the coolant water. Instrumentation shall be environmentally qualified for the Plant States concerned and shall be adequate for measuring plant parameters and thus classifying events for the purposes of Accident Management and Emergency Response.

2. Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the course of DBAs and the status of essential equipment; and for predicting, as far as is necessary for Safety, the locations and quantities of Radioactive Materials that could escape from the locations intended in the Design. The instrumentation and recording equipment shall be adequate to provide information as far as practicable for determining the status of the Nuclear Facility in a Severe Accident and for taking decisions in Accident Management.

Article (71)

1. A control room shall be provided from which the Nuclear Facility can be safely operated in all its Operational States, and from which measures can be taken to maintain the Nuclear Facility in a stable, safe state or to bring it back into such a state after the onset of Anticipated Operational Occurrences, DBAs and Severe Accidents. Appropriate measures shall be taken and adequate information provided to safeguard the occupants of the control room against consequent hazards, such as undue radiation levels resulting from an Accident Condition or the release of Radioactive Material or explosive or toxic gases, which could hinder necessary actions by the operating personnel.

2. Special attention shall be given to identifying those events, both internal and external to the control room, which may pose a direct threat to its continued Operation, and the Design shall provide for reasonably practicable measures to minimise the effects of such events.

3. 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 Nuclear Facility. Ergonomic factors shall be taken into account in the Design of the control room.

4. Devices shall be provided to give visual and, if appropriate, also audible indications of Operational States and processes that have deviated from normal and could affect Safety.

Article (72)

Sufficient I&C equipment shall be available, preferably at a single location (supplementary control room) that is physically and electrically separate from the control room, so that the reactor can be placed and maintained in a shut-down state, residual heat can be removed, and the essential plant variables can be monitored should there be a loss of ability to perform these essential Safety Functions in the control room.

Use of Computer Based Systems in Systems Important to Safety

Article (73)

1. If the Design is such that a system Important to Safety is dependent upon the reliable performance of a computer based system, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the life-cycle of the system, and in particular the software development cycle. The entire development shall be subject to an appropriate Quality Assurance programme.

2. The level of reliability necessary shall be commensurate with the Safety importance of the system. The necessary level of reliability shall be achieved by means of a comprehensive strategy that uses various complementary means (including an effective regime of analysis and testing) at each phase of development of the process, and a validation strategy to confirm that the design requirements for the system have been fulfilled.

3. The level of reliability assumed in the Safety analysis for a computer based system shall include a specified conservatism to compensate for the inherent complexity of the technology and the consequent difficulty of analysis.

Article (74)

Various Safety actions shall be automated so that operating personnel action is not necessary within a justified period of time from the onset of Anticipated Operational Occurrences or DBAs. In addition, appropriate information shall be available to the operating personnel to monitor the effects of the automatic actions.

Article (75)

The Protection System shall be designed:

1. To initiate automatically the Operation of appropriate systems, including, as necessary, the reactor shutdown systems, in order to ensure that specified design limits are not exceeded as a result of Anticipated Operational Occurrences;

2. To detect DBAs and initiate the Operation of systems necessary to limit the consequences of such Accidents within the design basis; and

3. To be capable of overriding unsafe actions of the control system.

Article (76)

1. The Protection System shall be designed for reliability and periodic testability commensurate with the Safety Function(s) to be performed. Redundancy and

independence designed into the 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 reliability of Operation of the Protection System can be otherwise demonstrated.

2. The Protection System shall be designed to ensure that the effects of Normal Operation, Anticipated Operational Occurrences and DBAs on redundant Channels do not result in loss of its function; or else such a loss shall be demonstrated to be acceptable on some other basis. Design techniques such as testability, including a self-checking capability where necessary, fail-safe behaviour, functional Diversity and Diversity in component Design or principles of Operation shall be used to the extent practicable to prevent loss of a protection function. The Protection System shall, unless its reliability is ensured by some other means, be designed to permit periodic testing of its functioning when the reactor is in Operation, including the possibility of testing Channels independently to determine failures and losses of Redundancy that may have occurred. The Design shall permit all aspects of functionality from the sensor to the input signal to the final actuator to be tested in Operation.

3. The Design shall be such as to minimise the likelihood that operating personnel action could defeat the effectiveness of the Protection System in Normal Operations and expected operational occurrences, but not to negate correct operating personnel actions in DBAs.

4. The Nuclear Facility shall have a diverse protection system to interrupt power to the control rods and to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of anticipated transient without scram.

Article (77)

Where a computer based system is intended to be used in a Protection System, the following requirements shall apply:

1. The quality of hardware and software shall be commensurate with the importance of the safety functions to be performed;

2. The whole development process, including control, testing and Commissioning of Design changes, shall be systematically documented and reviewable;

3. In order to confirm confidence in the reliability of the computer based systems, an Assessment of the computer based system by expert personnel independent of the designers and suppliers shall be undertaken; and

4. Where the necessary integrity of the system cannot be demonstrated with a high level of confidence, a diverse means of ensuring fulfilment of the protection functions shall be provided.

Article (78)

Interference between the Protection System and the non-safety related Control Systems shall be prevented by avoiding interconnections or by suitable Functional Isolation. If signals are used in common by both the Protection System and any Control System, appropriate separation (such as by adequate decoupling) shall be ensured and it shall be demonstrated that all Safety requirements are met.

Emergency Control Centre

Article (79)

An on-site (within the site area) technical support centre, separated from the plant control room and an operation support centre and an off-site emergency operation centre shall be provided to serve as emergency facilities in the event of an Emergency. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings shall be available there. Emergency power supply system should be equipped to cope with a loss of off-site power. The facilities shall provide means of communication with the control room, the supplementary control room and other important points in the plant, and with the on-site and off-site Emergency Response organizations. Appropriate measures shall be taken to protect the occupants for a protracted time against hazards resulting from a Severe Accident, where applicable.

Emergency Power Supply

Article (80)

1. After certain PIEs, various systems and components important to Safety will need emergency power. It shall be ensured that the emergency power supply is able to supply the necessary power in any Operational State or in a DBA, on the assumption of the coincidental loss of off-site power. The need for power will vary with the nature of the PIE, and the nature of the Safety duty to be performed will be reflected in the choice of means for each duty; in respect of number, availability, duration, capacity and continuity, for example.

2. The combined means to provide emergency power (such as by means of water, steam or gas turbine, diesel engines or batteries) shall have a reliability and form that are consistent with all the requirements of the Safety Systems to be supplied, and shall perform their functions on the assumption of a Single Failure. It shall be possible to test the functional capability of the emergency power supply

3. Emergency power shall be capable of being provided in a time frame and for a duration of time following loss of normal power to support Safety Functions necessary to maintain Nuclear Facility Safety.

4. Each Nuclear Facility must be able to withstand for a specified duration and recover from a station blackout. The specified station blackout duration shall be based on the following factors: the redundancy, reliability of the onsite Emergency ac power sources, the expected frequency of loss of offsite power; and the probable time needed to restore offsite power.

Article (81)

In the Design of the Nuclear Power Plant, account shall be taken of power grid plant interactions, including the independence of and number of power supply lines to the Nuclear Facility, in relation to the necessary reliability of the power supply to plant systems important to Safety. Accordingly:

1. An Assessment shall be performed to verify that there is a high degree of confidence that the Nuclear Facility Design can reliably cope with and recover from the frequency and duration of potential loss-of-offsite-power (LOOP) caused by grid failures.
2. This Assessment shall be updated when major modifications are made to the electrical grid and periodically throughout the life of the Nuclear Facility (i.e., potential load growth, effects of additional transmission lines, interaction of the Nuclear Facility with the electrical grid and other generators on the system).
3. The Assessment shall also include the potential increase in risk that may result from Maintenance activities on the electrical grid.

Waste Treatment and Control Systems

Article (82)

1. Adequate systems shall be provided to treat radioactive liquid and gaseous effluents in order to keep Doses arising from Discharge of Radioactive Material within the Dose limits established by REG-04, Regulation for Radiation Dose Limits and Optimisation of Radiation Protection for Nuclear Facilities and subject to optimisation of protection as defined in that Regulation.
2. Adequate systems shall be provided for the handling of Radioactive Wastes and for storing these safely on the site for a period of time consistent with the availability of the Disposal route on the site. Transport of solid wastes from the site shall be effected according to the decisions of competent authorities

Article (83)

1. The Nuclear Facility shall include suitable means to monitor and control the release of radioactive liquids and gases to the environment.

a. Gaseous and liquid radiological effluent monitors are to be provided for the automatic termination of releases in the event that effluent release set points are exceeded.

b. Adequate systems shall be provided to accommodate radioactive liquid and gaseous waste safely when processing is not available."

Article (84)

A ventilation system with an appropriate filtration system shall be provided:

1. To prevent unacceptable dispersion of airborne radioactive substances within the Nuclear Facility;
2. To reduce the concentration of airborne radioactive substances to levels compatible with the need for access to the particular area;
3. To keep the level of airborne radioactive substances in the Nuclear Facility below prescribed limits and criteria and ALARA in Normal Operation, Anticipated Operational Occurrences and DBAs; and
4. To ventilate rooms containing inert or noxious gases without impairing the capability to control radioactive releases.

Article (85)

1. A monitored ventilation system with an appropriate filtration system shall be provided to control the release of airborne radioactive substances to the environment.
2. Filter systems shall be sufficiently reliable and so designed that under the expected prevailing conditions the necessary retention factors are achieved. Filter systems shall be designed such that the efficiency can be tested.

Fuel Handling and Storage Systems

Article (86)

The handling and Storage systems for non-irradiated fuel shall be designed:

1. To prevent criticality by a specified margin by physical means or processes, preferably by the use of geometrically safe configurations, even under Plant States of optimum moderation;
2. To permit appropriate Maintenance, periodic Inspection and testing of components important to Safety; and
3. To minimise the probability of loss of or damage to the fuel.

Article (87)

1. The SSCs for the handling of irradiated fuel shall be designed to:

    a. prevent criticality at all times

b. prevent unacceptable handling stresses on the fuel elements or fuel assemblies;

c. prevent the inadvertent dropping of heavy objects such as spent fuel casks, cranes or other potentially damaging objects on the fuel assemblies and dropping of spent fuel in transit;

d. provide proper means for Radiation Protection;

e. adequately identify fuel assemblies; and

f. Facilitate decontamination of fuel handling equipment when necessary.

2. The SSCs for the Storage of irradiated fuel in water pools shall be designed to:

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

b. to permit adequate heat removal in operational states and in design basis accidents;

c. to permit inspection of irradiated fuel;

d. to permit appropriate periodic inspection and testing of components important to safety;

e. to prevent the dropping of spent fuel in transit;

f. to prevent unacceptable handling stresses on the fuel elements or fuel assemblies;

g. to prevent the inadvertent dropping of heavy objects such as spent fuel casks, cranes or other potentially damaging objects on the fuel assemblies;

h. to permit safe storage of suspect or damaged fuel elements or fuel assemblies;

i. to provide proper means for radiation protection;

j. to adequately identify individual fuel modules;

k. to control soluble absorber levels if used for criticality safety;

l. to facilitate maintenance and decommissioning of the fuel storage and handling facilities;

m. to facilitate decontamination of fuel handling and storage areas and equipment when necessary; and

n. to ensure that adequate operating and accounting procedures can be implemented to prevent any loss of fuel.

Radiation Protection

Article (88)

1. The Design shall address the optimisation of Radiation Protection, including by means of the following:

    a. appropriate layout and shielding of SSCs containing Radioactive Materials;

    b. paying attention to the Design of the Power Plant and equipment so as to minimise the number and duration of human activities undertaken in radiation fields and reduce the likelihood of contamination of the site personnel;

    c. making provision for the treatment of Radioactive Materials in an appropriate form and condition, for either their Disposal, their Storage on the site or their removal from the site; and

    d. Making arrangements to reduce the quantity and concentration of Radioactive Materials produced and dispersed within the Nuclear Facility or released to the environment.

2. Full account shall be taken of the potential build-up of radiation levels with time in areas of personnel occupancy and of the need to minimise the generation of Radioactive Materials as wastes.

Article (89)

1. Provision shall be made in the Design and layout of the Nuclear Facility to minimise exposure and contamination from all sources. Such provision shall include adequate Design of SSCs in terms of: minimizing exposure during Maintenance and Inspection; shielding from direct and scattered radiation; ventilation and filtration for control of airborne Radioactive Materials; limiting the activation of corrosion products by proper specification of materials; means of monitoring; control of access to the Nuclear Facility; and suitable decontamination facilities.

2. The shielding Design shall facilitate Maintenance and Inspection so as to minimise exposure of Maintenance personnel.

3. The Nuclear Facility layout and procedures shall provide for the control of access to radiation areas and areas of potential contamination, and for minimizing contamination from the movement of Radioactive Materials and personnel within the Nuclear Facility. The plant layout shall provide for efficient Operation, Inspection, Maintenance and replacement as necessary to minimise radiation exposure.

4. Provision shall be made for appropriate decontamination facilities for both personnel and equipment and for handling any Radioactive Material and Radioactive Waste arising from decontamination activities.

Article (90)

Equipment shall be provided to ensure that there is adequate radiation monitoring in Operational States, DBAs and, as practicable, Severe Accidents:

1. Stationary Dose rate meters shall be provided for monitoring the local radiation Dose rate at places routinely occupied by operating personnel and where the changes in radiation levels in Normal Operation or Anticipated Operational Occurrences may be such that access shall be limited for certain periods of time. Furthermore, stationary Dose rate meters shall be installed to indicate the general radiation level at appropriate locations in the event of DBAs and, as practicable, Severe Accidents. These instruments shall give sufficient information in the control room or at the appropriate control position that Nuclear Facility personnel can initiate corrective action if necessary.

2. Monitors shall be provided for measuring the Activity of radioactive substances in the atmosphere in those areas routinely occupied by personnel and where the levels of Activity of airborne Radioactive Materials may on occasion be expected to be such as to necessitate protective measures. These systems shall give an indication in the control room, or other appropriate locations, when a high concentration of radionuclides is detected.

3. Stationary equipment and laboratory facilities shall be provided for determining in a timely manner the concentration of selected radionuclides in fluid process systems as appropriate, and in gas and liquid samples taken from plant systems or the environment, in Operational States and in Accident Conditions.

4. Stationary equipment shall be provided for monitoring the effluents prior to or during Discharge to the environment.

5. Instruments shall be provided for measuring radioactive surface contamination.

6. Facilities shall be provided for monitoring of individual Doses to and contamination of personnel.