CODE NO. AERB/NPP-LWR/SC/D

CODE NO. AERB/NPP-LWR/SC/D

GOVERNMENT OF INDIA

AERB SAFETY CODE

DESIGN OF LIGHT WATER REACTOR BASED NUCLEAR POWER PLANTS

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY CODE NO. AERB/NPP-LWR/SC/D

DESIGN OF LIGHT WATER REACTOR BASED NUCLEAR POWER PLANTS

Approved by the Board in December 2014

Atomic Energy Regulatory Board
Mumbai-400 094
India

January 2015

Price:

Order for this code should be addressed to:

Chief Administrative Officer
Atomic Energy Regulatory Board
Niyamak Bhavan
Anushaktinagar
Mumbai-400 094
India

FOREWORD

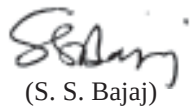
Activities concerning establishment and utilisation of nuclear facilities and use of radioactive sources are to be carried out in India in accordance with the provisions of the Atomic Energy Act 1962. In pursuance of the objective of ensuring safety of members of the public and occupational workers as well as protection of environment, the Atomic Energy Regulatory Board (AERB) has been entrusted with the responsibility of laying down safety standards and enforcing rules and regulations for such activities. The Board, therefore, has undertaken a programme of developing safety codes, safety standards, related safety guides and safety manuals for the purpose. While some of these documents cover aspects such as siting, design, construction, operation, quality assurance and decommissioning of nuclear and radiation facilities, other documents cover regulatory aspects of these facilities.

AERB safety codes and standards are formulated on the basis of nationally and internationally accepted safety criteria for design, construction and operation of specific equipment, structures, systems and components of nuclear and radiation facilities. Safety codes establish the objectives and set minimum requirements that shall be fulfilled to provide adequate assurance for safety. Safety guides elaborate various requirements and furnish approaches for their implementation. Safety manuals deal with specific topics and contain detailed scientific and technical information on the subject. These documents are prepared by experts in the relevant fields and are extensively reviewed by advisory committees of the Board before they are published. The documents are revised when necessary, in the light of experience and feedback from users as well as new developments in the field.

Since nuclear power plants (NPP) with light water based reactors are now being built in India for expansion of nuclear power programme, AERB took initiative in framing design requirements for such NPP. In drafting the code, the relevant International Atomic Energy Agency (IAEA) documents under the Nuclear Safety Standards (NUSS) program, especially IAEA Safety Standard Series No. SSR-2/1 (2012) on 'Safety of Nuclear Power Plants: Design' and its revised version No. SSR-2/1 (Rev.1) of July 17, 2014 have been used extensively. This safety code helps in implementing overall safety philosophy and practices adopted by AERB and the safety principles delineated by IAEA which are adopted worldwide for achieving nuclear and radiological safety.

A committee consisting of AERB staff and other professionals experienced in this field has prepared this code. Experts have reviewed the code and the relevant AERB advisory committee and advisory committee on nuclear safety have further reviewed it before issue.

AERB wishes to thank all individuals and organisations who have prepared and reviewed the draft and helped in its finalisation. The list of experts who have participated in this task, along with their affiliations, is included for information.



(S. S. Bajaj)
Chairman, AERB

SPECIAL DEFINITIONS
(Specific for the present Code)

Additional Safety Systems/Features

Item designed to perform a safety function or which has a safety function, in design extension conditions without core melt.

Accident Conditions

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

Beyond Design Basis Accident

This term is superseded by design extension conditions.

Complementary Safety Features

A design feature outside of the design basis envelope that is introduced to cope with design extension conditions with core melt/severe accidents.

Controlled State

This is a state of the plant, following an anticipated operational occurrence or accident condition, in which the fundamental safety functions can be ensured and can be maintained for a time sufficient to implement provisions to reach a safe state/safe shutdown state.

Design Authority

The defined function of a licensee's organisation with requisite knowledge and with responsibility for maintaining the design integrity and the overall basis for safety of its nuclear facilities throughout the full lifecycle of those facilities. Design authority relates to the attributes of an organisation rather than the capabilities of individual post holders.

Design Basis Accident

Accident conditions against which a nuclear power plant is designed according to established design criteria (including single failure criteria), and for which the damage to the fuel and the release of radioactive material are kept within authorised limits.

Design Extension Conditions

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

Design Organisation

The design organisation is the organisation responsible for preparation of the final detailed design of the plant to be built.

Fail-safe Design

Design whose most probable failure modes do not result in a reduction of safety.

Heat Sink

A system or component that provides a path for heat-transfer from a source such as heat generated in the fuel, to a large heat absorbing medium.

Leak-before-break

A situation where leakage from a flaw is detected during normal operation, allowing the reactor to be shut down and depressurised before the flaw grows to the critical size for rupture.

Plant States (Considered in Design)

<table>
<tr><th colspan="2">Operational States</th><th colspan="3">Accident Conditions</th><th>Practically eliminated</th></tr>
<tr><td rowspan="2">Normal operations</td><td rowspan="2">Anticipated operational occurrences</td><td rowspan="2">Design basis accidents</td><td colspan="2">Design extension conditions</td><td rowspan="2">Large release of radioactivity from containment</td></tr>
<tr><td>Accidents without core melt</td><td>Accidents with core melt</td></tr>
</table>

Responsible Organisation

Responsible Organisation is an organisation having overall responsibility for siting, design, construction, commissioning, operation and decommissioning of a facility.

Safe shutdown state

Safe shutdown state is the state of the plant, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and maintained continuously.

Safe State

State of plant, following design extension condition without core melt, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

Safety Case

A collection of arguments and evidence in support of the safety of a facility or activity.

(i) This will normally include the findings of a safety assessment and a statement of confidence in these findings.

(ii) For a repository, the safety case may relate to a given stage of development. In such cases, the safety case should acknowledge the existence of any unresolved issues and should provide guidance for work to resolve these issues in future development stages.

Safety Group

Assembly of structures, systems and components designated to perform all actions required for a particular postulated initiating event to ensure that the specified limits for anticipated operational occurrences and design basis accidents are not exceeded. It may include certain safety and safety support systems, and any interacting process system.

Safety Support System

A system designed to support the operation of one or more safety systems.

Safety System

A system provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

Safety System Settings

The levels at which safety systems are automatically actuated in the event of anticipated operational occurrences or design basis accidents, to prevent safety limits from being exceeded.

Severe Accident

A design extension condition (beyond design basis accident) that involves significant core degradation.

Single Failure

A failure that results in the loss of capability of a system or component to perform its intended function(s) and any consequential failure(s) that result from it.

CONTENTS

1. INTRODUCTION

1.1 General

This safety code presents the requirements for the design of light water based Nuclear Power Plants (NPP) and is intended to ensure the highest level of safety that can reasonably be achieved for the protection of workers, the public and the environment from harmful effects of ionising radiation arising from nuclear power plants. It is recognised that as technology and scientific knowledge advance, safety requirements will change over time and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. The safety requirements in this code reflect the present national and international benchmarks.

1.2 Objective

1.2.1 This safety code establishes:

(i) design requirements for the structures, systems and components (SSC) of a light water based nuclear power plant for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, if they do occur and

(ii) organisational processes important to safety, that are required to be met.

1.2.2 This code is intended for use by organisations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning of nuclear power plants; in analysis, verification and review; in the provision of technical support; as well as by AERB.

1.3 Scope

1.3.1 This code is primarily meant for land based stationary nuclear power plants with light water based reactors designed for electricity generation or for other heat utilization applications (such as heating or desalination). This document may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design. However, this safety code has to be seen in conjunction with other AERB safety codes.

1.3.2 This safety code does not address:

(a) Specific matters relating to nuclear security

(b) Conventional industrial safety

(c) Non-radiological impacts arising from the operation of nuclear power plants.

1.3.3 Terms in this safety code are to be understood as defined and explained in the AERB Safety Glossary, unless otherwise stated here (see under Special Definitions).

1.4 Structure

1.4.1 This safety code follows the relationship between the safety objective and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety objective, safety principles and concepts that form the basis for deriving the safety requirements that must be met for the nuclear power plant, as well as the safety design criteria. Section 3 establishes the general requirements to be satisfied by the design organisation in the management of safety in the design process. Section 4 establishes requirements for the principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provision for construction, interfaces of safety with nuclear security, and for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 establishes requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. The requirements for general plant design apply to all items (i.e. structures, systems and components) important to safety. Section 6 establishes requirements for the design of specific plant systems such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems. Section 7 establishes requirements for additional support provisions for accident management infrastructure needed to handle extreme events along with unexpected failure of existing safety features/systems.

2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS

2.1 General

2.1.1 Protection of workers, public and the environment from harmful effects of ionising radiation is the fundamental safety objective from which the safety principles and requirements for minimising the risks associated with nuclear power plants are derived. The fundamental safety objective applies to all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated physical transport of radioactive material and the management of spent nuclear fuel and radioactive waste.

2.1.2 Safety requirements are to be developed and safety measures are to be implemented in order to achieve the above fundamental safety objective. The safety principles as agreed by international community and prescribed in IAEA document on safety fundamentals have been adopted as one of the bases for these requirements. Different principles may be more or less important in relation to particular circumstances. However, appropriate application of all relevant principles is required. Most of the requirements presented in this publication are derived from the following safety principles[1] [1]:

Responsibility for safety (Principle 1)

The prime responsibility for safety must rest with the person or organisation responsible for facilities and activities that give rise to radiation risks.

Leadership and management for safety (Principle 3)

Effective leadership and management for safety must be established and sustained in organisations concerned with, and facilities and activities that give rise to, radiation risks.

Optimisation of protection (Principle 5)

Protection must be optimised to provide the highest level of safety that can reasonably be achieved.

1 Principle number referred is from Ref [1]. Safety principle 2 (Role of government), safety principle 4 (Justification of facilities and activities) and safety principle 10 (Protective actions to reduce existing or unregulated Radiation risks) are not applicable to this document.

Limitation of risks to individuals (Principle 6)

Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.

Protection of present and future generations (Principle 7)

People and the environment, present and future, must be protected against radiation risks.

Prevention of accidents (Principle 8)

All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.

Emergency preparedness and response (Principle 9)

Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.

2.1.3 To ensure that nuclear power plants are operated and activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures shall be taken:

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

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

(c) to mitigate the consequences of such events, if they were to occur; and

(d) to ensure integration of safety with security measures in design and in implementation**.**

2.1.4 Safety requirements which are particularly important in the design of nuclear power plants are:

(a) Radiation protection

(b) Safety in design

(c) Defence in depth (DiD)

(d) Maintaining the integrity of design of the plant throughout the lifetime of the plant

(e) Nuclear Security.

2.2 Radiation Protection

2.2.1 In order to satisfy the safety principles, it is required to ensure that for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the prescribed limits and kept as low as reasonably achievable (ALARA). In addition, it is required to implement measures for mitigating the radiological consequences of any accidents, were they to occur.

2.2.2 To apply the safety principles, it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, these principles do not preclude limited exposures or the release of authorised amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled in compliance with regulatory and operational limits, as well as radiation protection requirements.

2.3 Safety in Design

2.3.1 General Design Objective

To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, measures shall be taken to:

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

(b) ensure that for all the accidents taken into account in the design of the installation, any radiological consequences would be below the acceptable limits and would be kept as low as reasonably achievable;

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

(d) incorporate design features such that even in the accident with core melt, only limited countermeasures are needed in the public domain and sufficient time is available to implement these measures.

2.3.2 Radiation Protection Objective

The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences of nuclear or radiation incidents on human life and health, and the environment such that event sequences:

(a) that could result in high radiation doses or large radioactive releases must be practically eliminated[2]; and

(b) with a significant frequency of occurrence must have no or only minor potential radiological consequences.

An essential objective is that the necessity for off-site intervention measures to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required to be taken by the responsible authorities. [refer clause 2.4.2 (d)]

2.3.3 Safety Assessment

To demonstrate that the fundamental safety objective is achieved in the design of a nuclear power plant, a comprehensive safety assessment of the design is required to be carried out. All possible sources of radiation shall be identified and evaluated for possible radiation doses that could be received by workers at the installation and by members of the public, as well as the possible effects on the environment, as a result of operation of the plant. The safety assessment process shall cover:

(a) all normal operation states,

(b) anticipated operational occurrences (AOO),

(c) design basis accidents (DBA), and

(d) event sequences that may lead to 'design extension conditions' including severe accidents.

2.3.4 The performance of the plant shall be assessed for:

(i) selected anticipated operational occurrences, and

(ii) accident conditions which could result due to:

(a) a single Postulated initiating event (PIE) with consequential failures with superimposition of one failure in conformity with single failure criteria which is independent of the initiating events of any of the active or passive elements of the safety systems, or one human error;

(b) an external or internal hazard (e.g. earthquake, flooding, fire) with consequential failures affecting one or several safety (or safety related) systems; and

2 The possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high level of confidence to be extremely unlikely to arise.

(c) accidents with credible multiple failures other than a postulated hazard, affecting similar equipment in the same safety (or safety related) system.

2.3.5 On the basis of the safety analysis, the capability of the design to withstand postulated initiating events and accidents shall be established, the effectiveness of the items important to safety shall be demonstrated, and the inputs (prerequisites) for emergency planning shall be established. Based on the analysis during the design stage, provision for design extension conditions shall be envisaged and measures such as additional safety systems/features and/or complementary safety features shall be introduced to ensure that the radiological consequences of an accident could be mitigated.

2.4 Concept of Defence in Depth

2.4.1 The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth. This concept is applied to all safety related activities, whether organisational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subjected to independent levels of provisions in a hierarchical manner, so that if a failure were to occur in a level, it would be detected and compensated for or corrected by appropriate measures by the subsequent level. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accident conditions, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

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

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

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

(b) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, the establishment of operating procedures to prevent such initiating events, or else to minimise their consequences, and to return the plant to a safe state.

(c) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated single initiating events including its consequential failures might not be controlled at a preceding level and that a design basis accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or design provisions, safety systems and procedures be provided that are capable of preventing damage to the reactor core/irradiated fuel or significant off-site releases and returning the plant to a safe state.

(d) The purpose of the fourth level of defence is to control accident conditions in which the design basis may be exceeded. The design basis may get exceeded due to postulated multiple failures resulting due to common cause failure for other reasons than a postulated hazard, affecting similar equipment in the same safety (or safety related) system. These event sequences shall be categorised as design extension conditions (DEC) without core melt and DEC with core melt depending upon the consequences. Aim for the first kind of event sequences is to limit the progression of accident and thereby avoid core melting. The second kind of event sequences are called

severe accidents where aim is to confine and control the core melt so as to mitigate the consequences. Thus the fourth level of defence is basically intended for providing additional safety systems/features for preventing extensive fuel damage or core melt and complementary safety features for limiting the consequences of accident conditions with core melt.

For postulated multiple failures leading to accident without core melt, the targeted radiological consequence should be such that there shall be no necessity of protective measures for people living in the vicinity.

Accident with core melt which can lead to large release is to be practically eliminated. For accidents with core melt which could not be practically eliminated, complementary safety features shall be provided to confine and limit the core melt progression and to ensure integrity of the containment, so as to limit the release of radioactive material such that only limited protective measures in area and time are needed for the public, and that sufficient time is available to implement these measures.

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

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

2.5 Maintaining the Integrity of Design of the Plant throughout the Lifetime

2.5.1 The design, construction and commissioning of a nuclear power plant might be shared between a number of organisations: the architect/engineer, the designer/vendor of the reactor and its supporting systems, the technical support organisation (TSO) of vendor, the suppliers of major components, and the suppliers of other systems that are important to the safety of the plant.

2.5.2 The prime responsibility for safety rests with the organisation responsible for operating the nuclear power plant that gives rise to radiation risks. The responsible organisation should set up a formal process to maintain the

integrity of design of the plant. A formally designated entity i.e. design authority within the responsible organisation shall take responsibility for this process.

2.5.3 The formally designated entity (design authority) that has overall responsibility for the design process shall be responsible for approving design changes and for ensuring that the requisite knowledge is maintained throughout the plant life.

2.5.4 The management system requirements that are placed on design authority shall also apply to all the designers related with design process i.e. vendors/ consultants/TSOs etc. However, overall responsibility for maintaining the integrity of design of the plant would rest with the design authority, and hence, ultimately, with the responsible organisation.

2.6 Nuclear Security

2.6.1 The aim of the nuclear security is to minimise the risk of unauthorised removal of nuclear material and radioactive material, to minimise sabotage on nuclear power plants, and to minimise the risk of adverse impact during the above acts. Detailed requirements are not within the scope of this safety code.

3. MANAGEMENT OF SAFETY IN DESIGN

3.1 Responsibilities in the Management of Safety in Plant Design

An applicant for a license to construct and/or operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets safety objectives. As part of fulfilling this responsibility, the responsible organisation shall set up from the beginning a 'design authority' with responsibility for, and the requisite knowledge to maintain, the design integrity and the overall basis for safety of the plant throughout its lifecycle. The responsible organisation may be a party involved in the development process of the design partly or fully, or may be adopting the design developed by vendor(s) with adequate arrangement for design support service from the vendors (or their replacement) to the design authority for the whole plant life. In either case, the design authority within the responsible organisation has overall responsibility for the design including the design changes effected throughout the life of the plant.

3.1.1 All organisations, including the design authority and related design organisations, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.

3.1.2 Ownership of the safety case should reside within the responsible organisation that has the primary responsibility for safety. Ownership and responsibility require:

(a) an understanding of the safety case, the standards applied in it, its assumptions and the limits and conditions derived from it;

(b) the technical capability to understand and act upon the safety case including work produced by others;

(c) the ability to use the safety case to manage safety; and

(d) that users of safety case should be involved in its preparation to ensure that it reflects operational needs and reality.

3.2 Management System for Plant Design

The design authority within the responsible organisation shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design. The management system shall ensure that the responsible organisation, develops and retains sufficient number of technically qualified and adequately trained

staff at all levels, maintains necessary technical and scientific knowledge, and is provided with adequate resources to fulfil its role [2].

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

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

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

3.3 Safety of the Plant Design throughout the Lifetime of the Plant

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

3.3.1 The responsible organisation shall establish a formal system within its management system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant including decommissioning. The formal system should provide for arrangements with external organisations for assignment of tasks where detailed specialised knowledge is not available with the design authority. These external organisations including original designers (vendors) or their replacements for the design of specific parts of the plant shall have formal responsibility for maintaining their specialized knowledge of design and sharing the same with the design authority within the responsible organisation during the lifetime of the plant.

3.3.2 The design authority within the responsible organisation shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following:

(a) That the plant design is fit for purpose and meets the requirement for the optimisation of protection and safety by keeping radiation risks as low as reasonably achievable.

(b) That the design verification, engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design.

(c) That the aspects of design, having implications on operability, shall be reviewed. This should ensure the acceptance of the design by responsible organisation for ensuring proper operability, maintainability, layout, inspectability etc. in the designs.

(d) That the knowledge of the design and the safety case that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the responsible organisation, and that due account is taken of past operating experience and validated research findings.

(e) That management of design requirements and configuration control are maintained.

(f) That the necessary interfaces with original vendor designers and suppliers engaged in design work are established and controlled.

(g) That the necessary engineering expertise and scientific and technical knowledge is maintained within the operating organisation.

(h) That all design changes to the plant are reviewed, verified, documented and approved.

(i) That adequate documentation is maintained to facilitate future decommissioning of the plant.

3.3.3 An indicative list of design capabilities required by the design authority within the responsible organisation for maintaining design integrity throughout the life of the plant is given below:

(a) A detailed understanding of why the design is as it is.

(b) An understanding of experimental and research knowledge on which the design is based.

(c) The design inputs such as basic functional requirements, performance requirements, safety goals and safety principles, applicable codes, standards and regulatory requirements, design conditions, probabilistic safety assessment, loads such as seismic loads, and interface requirements.

(d) The design outputs such as specifications, design limits, operating limits, safety limits, and failure or fitness for service criteria.

(e) A detailed knowledge of the design calculations (stress analysis, thermal hydraulic analysis, reactor core physics aspects including fuel management, and shielding) which demonstrates the adequacy of the design and the ability to reproduce the design calculations, if needed.

(f) An understanding of the inspections, analysis, testing, computer code validation and acceptance criteria used by participating design organisations to verify that the design output meets the design requirements.

(g) The assumptions made in all the steps above, including assumptions related to operating modes or procedures, and expected life history.

(h) The implications of operating experience on the design.

4. PRINCIPAL TECHNICAL REQUIREMENTS

4.1 Fundamental Safety Functions

Fulfillment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states:

(i) control of reactivity,

(ii) removal of heat from the reactor and from the spent fuel storage pool and

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

4.1.1 A systematic approach shall be taken for identifying those items important to safety that are necessary to fulfill the fundamental safety functions and for identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states.

4.1.2 Means of monitoring the status of the plant shall be provided under all plant states for ensuring that the required safety functions are fulfilled.

4.2 Design for a Nuclear Power Plant

The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated or maintained safely within the operational limits and conditions until safely decommissioned, and that impacts on the environment are minimised.

4.2.1 The design for a nuclear power plant shall be such as to ensure that the requirements of the operating organisation, the safety requirements of AERB and the requirements of established relevant Acts, Rules, Codes and Standards, are all met, and that due account is taken of human capabilities and limitations and of factors that could influence human performance. Adequate information on the design shall be provided for ensuring the safe operation and maintenance of the plant, and to allow subsequent plant modifications to be made. Recommended practices shall be provided for incorporation into the administrative and operational procedures for the plant (i.e. the operational limits and conditions).

4.2.2 The design shall take due account of relevant available experience that has been gained in the design, construction, operation and decommissioning of other nuclear power plants, and of the results of relevant research programmes.

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

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

4.3 Application of Defence in Depth

The design of a nuclear power plant shall incorporate the concept of defence in depth. The levels of defence in depth shall be independent as far as practicable.

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

4.3.2 Defence in depth shall be structured in five levels. Should one level fail, the subsequent level comes into play. The objective of the first level of protection is the prevention of abnormal operation and system/equipment failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third level ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level prevents escalation to severe core damage conditions by additional safety systems/features, but if that also fails, it controls (prevent or mitigate) the accident with core melt by complementary safety features as well as through accident management to limit external releases of radioactive materials. Although, severe accident sequences which may lead to early or large radioactive releases must be practically eliminated by design, the last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

4.3.3 Defence in depth level four shall include consideration of design extension conditions (DEC). The DEC are accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DEC include severe accident conditions involving significant core degradation or core melt. The severe accident sequences which may lead to early or large

radioactive releases shall be practically eliminated. A clear distinction shall be introduced in level four between means and conditions for DEC without core melt and DEC with core melt.

4.3.4 The effective dose target (ref. clause 4.5) for multiple failure events (DEC without core melt) and for postulated single initiating events (DBA under level 3) should remain the same. The design shall ensure that for DEC scenarios only protective measures that are of limited scope in terms of area and time shall be necessary.

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

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

4.4 Design Approaches

For the design of safety systems necessary within design basis conditions rigorous safety criteria and conservative engineering practices shall be followed. This includes use of adequate margins, approach of single failure criteria, rigorous quality and qualification requirement for systems required to cater for addressing design basis events or accidents.

For design extension conditions without core melt, additional safety systems/ features (other than those provided for DBA), if envisaged, should be diverse from the safety systems for design basis conditions.

In design of complementary safety features which are used to prevent or mitigate the consequences of design extension conditions with core melt or severe accident situations that involve large early releases (e.g. early containment failure), the design approach should be to prevent such sequences by significant margins.

4.4.1 The design shall:

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

(b) be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimised, that accidents are prevented as far as

practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect[3];

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

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

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

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

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

(a) Challenges to the integrity of physical barriers

(b) Failure of one or more barriers

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

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

4.5 Dose Criteria

The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational

3 A cliff edge effect, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another, following a small deviation in a design parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable during, and following, accident conditions.

4.5.1 The design shall be such as to ensure that plant states that could lead to large radioactive releases are practically eliminated and that there are no, or only minor, potential radiological consequences for all the plant states with a significant likelihood of occurrence.

4.5.2 For practical application, quantitative dose assessment shall be undertaken for the NPP designs to demonstrate that the design will meet the dose limits stipulated by AERB. Radiological assessment should be done using realistic approach to compare the results of the calculations with acceptance criteria. For a given site, the dose criteria shall be applied for a representative person of the public, considering all routes of exposure or exposure pathways. For quantitative dose criteria refer AERB safety code 'Site Evaluation of Nuclear Facilities [AERB/NF/SC/S (Rev 1)]'.

4.5.3 Normal Operation

The annual release limits for all the facilities within a particular site (taken together) shall ensure that the effective dose limit for any individual at off-site, due to normal operation (including anticipated operational occurrences) is less than the limit prescribed by AERB [3].

Sufficient dose reserve shall be ensured while apportioning the doses among nuclear facilities to factor future requirements.

4.5.4 Accident Conditions: Nuclear Power Plants

(i) Design basis accident (initiating event with consequential failure and taking credit of safety systems considering single failure criterion):

Permitted calculated off-site releases during accident conditions shall be linked to the radiological consequence targets as specified. For design basis accident (DBA) in an NPP there shall be no need for offsite countermeasures (i.e. no need for prophylaxis, food control, shelter or evacuation) involving public, beyond Exclusion Zone.

In such cases the design target for effective dose calculated using realistic methodology shall be less than acceptable limit following the event [3].

(ii) Design extension condition (DEC) without core melt (multiple failure situations and rare external events):

For accidents without core melt within design extension conditions (multiple failure situations and rare external events) there shall be

no necessity of protective measures in terms of sheltering or evacuation for people living beyond Exclusion Zone. Required control on agriculture or food banning should be limited to a small area and to one crop. However, the design target for effective dose, with such interventions considered, remains same as for DBA.

(iii) Design extension condition with core melt (severe accident)

In case of severe accident e.g. accidents with core melt within design

extension conditions, the release of radioactive materials should cause no permanent relocation of population. The need for off-site interventions should be limited in area and time.

4.6 Interfaces of Safety with Security

Safety measures, nuclear security measures and arrangements for the system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.

4.7 Proven Engineering Practices

Items important to safety for a nuclear power plant shall be designed in accordance with the applicable codes and standards.

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

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

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

4.8 Safety Assessment

Comprehensive deterministic safety assessments and probabilistic safety

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

4.8.1 The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.

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

4.9 Provision for Construction

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

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

4.10 Features to Facilitate Radioactive Waste Management and Decommissioning

Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant [4].

4.10.1 In particular, the design shall take due account of:

(a) The choice of materials, so that amount of radioactive waste will be minimised to the extent practicable and decontamination will be facilitated.

(b) The access capabilities and the means of handling that might be necessary.

(c) The facilities necessary for the treatment and storage of radioactive waste generated in operation and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.

5. GENERAL PLANT DESIGN

5A DESIGN BASIS FOR THE PLANT

All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as to prevent the occurrence of events that could lead to an uncontrolled release of radioactivity to the environment; to prevent accidental criticality and overheating; to ensure that radioactive releases of material are kept below authorised limits on discharges in normal operation; and to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated. It should be further ensured that there are no, or only minor, potential radiological consequences for all the plant states with a significant likelihood of occurrence.

5.1 General Design Basis

The plant states shall be identified and grouped into a limited number of categories according to their likelihood of occurrence. The categories typically cover normal operation, anticipated operational occurrences, design basis accidents and design extension conditions, including severe accidents with significant degradation of the reactor core.

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

5.1.2 Conservative design measures shall be applied and sound engineering practices shall be adhered to in the design bases for normal operation, anticipated operational occurrences and design basis accidents so as to provide a high degree of assurance that no significant damage will occur to the reactor core and that radiation doses will remain within prescribed limits/ acceptable limits for normal operation and accident conditions respectively and will be ALARA.

5.1.3 The design shall also address the performance of the plant during design extension conditions including severe accidents. The assumptions and methods used for these evaluations may be realistic rather than conservative. The credible additional accident scenarios under design extension conditions shall be identified and addressed in design. The practicable provisions for prevention of such accidents or mitigation of their consequences, if they do occur, should also be addressed.

5.2 Design Basis for Items Important to Safety

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

5.2.1 The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the operating organisation to operate the plant safely.

5.2.2 Proven and conservative design measures with well established engineering practices shall be adopted in safety system design for design basis accidents. Additional safety systems/features for preventing and/or mitigating the consequences of design extension conditions leading to accidents situations without core melt, shall be designed with proven engineering practice. Complementary safety features shall be provided as practical for mitigating the consequences of any core melt scenario.

5.3 Design Limits

A set of design limits consistent with the key physical parameters for each safety related structure system or component including safety systems, additional safety systems/features and complementary safety features for the nuclear power plant shall be specified for all operational states and for accident conditions.

5.3.1 The design limits shall be specified and shall be consistent with relevant regulatory requirements provided in AERB regulatory safety documents and other applicable international standards.

5.4 Safety Classification and Seismic Categorisation

All structures, systems and components (SSC) shall be identified and shall be classified on the basis of their function and their safety significance.

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

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

(b) The consequences of failure to perform a safety function.

(c) The frequency with which the item will be called upon to perform a safety function.

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

5.4.2 Items important to safety shall be designed, constructed and maintained such that their quality and reliability are commensurate with this classification.

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

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

5.4.5 The seismic categorisation of all SSC shall be aligned with the requirements specified by AERB or equivalent standards. Seismic fragility levels should be evaluated for SSC important to safety by analysis or, where possible, by testing.

5.5 Reliability of Items Important to Safety

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

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

5.5.2 The safety systems and their support systems shall be designed to ensure that the probability of a safety system failure on demand from all possible causes is lower than 10^{-3}. The reliability model for each system should use realistic failure criteria and best estimate failure rates, considering the anticipated demand on the system from PIEs. Design for reliability should include consideration of mission times for SSC important to safety.

5.5.3 To the extent possible, the design shall provide for testing to demonstrate that these reliability requirements will be met during operation.

5.6 Common Cause Failures

The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of

diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.

Such event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant or due to external or internal hazards. Common cause failures may simultaneously affect a number of items important to safety and failure of common support systems.

5.6.1 Vulnerability of the design against common cause failures initiated by credible external events shall be assessed. Capability of the design to withstand demands arising out of non availability of multiple systems that could be vulnerable to a single/correlated external phenomenon shall be assessed.

5.6.2 With respect to physical separation among safety systems or between safety system and process systems the following shall be ensured:

(a) A safety system designed to act as a redundant or a backup system shall not be located in the same space.

(b) If a safety system and a process system must share space, then it shall be demonstrated that failure of process system does not affect the safety function or the associated safety functions are also achieved by another unaffected safety system.

5.6.3 The design shall provide sufficient physical separation between redundant divisions of safety systems and support systems. This applies to equipment and to routing of the following items:

(a) Electrical cables for power and control of equipment.

(b) Piping for service water for the cooling of fuel and process equipment.

(c) Tubing and piping for compressed air or hydraulic drives for control equipment.

5.6.4 Diversity shall be applied to additional safety systems or features that act as back-up systems with respect to main safety systems that perform same safety function by incorporating different attributes into the systems or components. Such attributes shall include different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers to address common cause failure.

5.7 Independence of Safety Systems

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

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

5.8 Single Failure Criterion

The single failure criterion[4] shall be applied to each safety group or 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 design basis accidents are not exceeded.

5.8.1 Spurious action shall be considered to be one mode of failure when applying the concept to a safety group or safety system designed for anticipated operational occurrences and design basis accidents.

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

5.8.3 In designing additional safety systems/features or complementary safety features for preventing the design extension conditions and to mitigate the consequence of such scenario the possibility of application of the single failure criterion shall be explored. However, emphasis shall be to provide diversified backup systems [refer sections [2.4.2 (d) and (5.6.4)] and consideration should be given to the repair and replacement potential should a failure occur.

5.9 Fail-safe Design

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

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

5.9.2 The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power and instrument air), or postulated adverse environment (e.g. extreme conditions of heat or cold, fire, pressure, steam, water, and radiation) are experienced.

4 The single failure criterion is 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.

5.10 Support Service Systems

Safety support systems necessary to maintain a safe state of the plant include electricity, cooling water, compressed air or other gases and means of lubrication. Normally, where services are to be provided from external sources, backup sources to such services for safety support systems shall be identified. The design shall provide emergency services for safety support systems to cope with the possibility of loss of normal service and, where applicable, concurrent loss of backup services. Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.

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

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

5.10.3 The systems that provide normal services, backup services and emergency services shall have:

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

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

The emergency services support systems shall have adequate capacity and shall be capable of providing services for sufficient duration. Such systems shall have significant margin with respect to their availability during and after an external event (e.g. earth quake, flood, etc).

5.11 Equipment Outages

The time allowed for equipment outages and the actions to be taken shall be analysed and defined for each case before the start of plant operation and included in the plant operating documents.

5.12 Materials and Water Chemistry

5.12.1 To ensure satisfactory performance during normal operation and accident conditions, only approved materials for structures, components, etc. shall be selected based on considerations, among others, such as:

(a) irradiation damage,

(b) activation and corrosion,

(c) creep and fatigue,

(d) erosion,

(e) compatibility with other interacting materials,

(f) thermal effects,

(g) resistance to brittle fracture, and

(h) hydrogen pick-up.

Current state-of-art developments in material research and behaviour phenomena should form an essential input for design updates.

5.12.2 Design organisation should prescribe the range of permissible water chemistry for primary and secondary systems to avoid various degradation mechanisms such as, corrosion and flow accelerated corrosion (FAC).

5.13 Operational Limits and Conditions for Safe Operation

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

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

(a) Safety limits

(b) Limiting settings for safety systems

(c) Operational limits and conditions for operational states

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

(e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design.

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

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

The design shall ensure that on-line surveillance and testing of systems

important to safety can be conducted. The impact of anticipated surveillance test and/or repair work on the reliability of systems important to safety shall be considered in the design such that the safety function can still be achieved with the required reliability.

These requirements and limitations shall be a basis for the establishment of operational limits and conditions under which the responsible organisation will be licensed to operate the plant.

5.14 Postulated Initiating Events

A systematic approach shall be adopted during the design of the nuclear power plant to identify a comprehensive set of postulated initiating events such that all foreseeable events with a significant frequency of occurrence and all foreseeable events with the potential for significant radiological consequences are anticipated and are considered in the design basis or in the design extension condition.

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

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

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

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

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

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

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

(d) Following a postulated initiating event, the plant would be rendered safe by the actuation of additional safety systems/features or complementary safety features following specified procedures, in case the plant state reaches design extension condition.

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

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

5.14.7 Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems or additional safety systems/features, to prevent progression to more severe plant conditions.

5.14.8 Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems, or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long (15 to 30 minutes), and sufficiently detailed procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.

5.14.9 The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment. The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

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

5.15 Internal and External Hazards

All foreseeable internal hazards and external hazards [3], including the human induced events, having potential to affect the safety of the nuclear power plant directly or indirectly, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety of the plant.

5.15.1 Internal Hazards

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

(b) Some external events may initiate internal fires or floods and may also cause the generation of missiles. Such interaction of external and internal events shall also be considered in the design, wherever appropriate.

(c) SSC important to safety shall be designed and located in a manner that minimises the probability and effects of fires and explosions caused by external or internal events.

5.15.2 External Hazards

(a) The design shall consider all those natural and human induced external events (i.e. events of origin external to the plant) that have been identified through adequate conservatism in the site evaluation process. Applicable natural external hazards include events such as earthquakes, volcano eruptions, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions. Human-induced external events include those that are identified in the site evaluation, such as potential aircraft crashes, ship collisions, large area fire, and nearby hazardous industries. Loss of Ultimate Heat Sink from conditions arising out of external hazards shall also be addressed.

(b) The design of the plant shall provide for a sufficient safety margin to protect against site specific external events (earthquake, flood, extreme wind, and temperature) and to avoid cliff edge effects.

(c) A design-specific assessment of the effects on the plant of the impact of an aircraft shall be conducted using realistic analytical model and realistic assumptions about the size of the aircraft. This analysis shall be used to identify and incorporate into the design those design features and functional capabilities to show that, with reduced use of operator actions:

(i) the reactor core remains cooled, or the containment remains intact; and

(ii) spent fuel cooling or spent fuel pool integrity is maintained.

(d) The safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and water for a minimum period of seven days. The design shall take due account of site specific conditions to determine the maximum delay time, by which off-site services can be considered to be available.

(e) Flood protection of safety-related rooms shall follow the logic of defence in depth. Penetrations and the doors built under the postulated flood level of safety related buildings shall be watertight.

(f) Appropriate parameters of external events shall be specified which can act as warning indicators to operator with respect to external events following which there will be a need for operator to take necessary measures.

(g) Design shall consider that any interaction between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design does not lead to any unsafe condition.

(h) The design shall be such as to ensure that items important to safety are capable of withstanding the effects of external events considered in the design, and if not, other features such as passive barriers shall be provided to protect the plant and to ensure that the required safety function will be performed.

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

5.15.3 Applicability of Leak Before Break

Leak-before-break (LBB) analysis shall be conducted to permit removal of protective hardware such as pipe whip restraints and jet impingement barriers, redesigning pipe connected components, their supports and their internals,

and other related changes in operating plants for the piping systems that are qualified to be considered for LBB application.

Analyses should demonstrate that the probability of pipe rupture is extremely low under conditions consistent with the design basis for the piping. A deterministic evaluation of the piping system that demonstrates sufficient margins against failure, including verified design and fabrication, and an adequate in-service inspection program can be assumed to satisfy the extremely low probability criterion.

The LBB case can be used as an independent method of safety case establishment which does allow for the omission of the double ended guillotine break (DEGB) dynamic effect arrangement. Credit of such postulation shall not be extended in the design to capacity of the emergency core cooling system, internal missile effect on primary containment wall, and containment pressure build up in accident condition.

5.15.4 Fire Safety

(a) Structures, systems and components important to safety shall be designed and located, consistent with other safety requirements, so as to minimise the likelihood and effects of internal fires and explosions caused by external or internal events.

(b) Basic safety functions shall be achieved by suitable incorporation of redundant equipment, diverse systems, physical separation, fire protection systems and design for fail-safe operation such that the following objectives are achieved:

(i) Preventing fires from starting

(ii) Detecting and extinguishing quickly those fires which do start, thus limiting the damage

(iii) Preventing the spread of those fires which have not been extinguished, thus minimising their effect on essential plant functions.

The first objective requires that the design and operation of the plant be such that the probability of a fire starting is minimised. The second objective concerns the early detection and extinguishing of fires by automatic and/or manual firefighting techniques. For implementation of the third objective, particular emphasis shall be placed on the use of passive fire barriers and physical separation. This includes spatial separation and fire barriers which would be the last line of defence. The main purpose of this line of defence is to ensure that even if fire occurs or initiates and if the mitigating and suppression features fail,

the design of the plant safety systems is such that all safety functions can be successfully performed.

(c) The planning for prevention and protection against fire and explosion should be started at the plant design stage itself and carried through construction, commissioning and operation phases. A fire hazard analysis of the plant shall be carried out to determine the required rating of the fire barriers, and the required capability of fire detection and fire fighting systems shall be provided.

(d) Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety, and does not simultaneously affect redundant safety chains, thereby challenging compliance with the single failure criterion.

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

5.16 Engineering Design

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

5.16.1 Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant.

5.17 Design Basis Accidents

A set of accident conditions that are tobe considered in the design shall be derived from postulated initiating events for the purpose of establishing the bounding conditions for the nuclear power plant to withstand, without exceeding the acceptable limits of radiation protection.

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

5.17.2 The design shall be such that for design basis accident conditions, key plant parameters do not exceed the applicable design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only

minor, radiological impacts, on or off the site, and are within AERB specified limits, and do not necessitate any off-site countermeasures.

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

5.18 Design Extension Conditions

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

5.18.1 The NPP design shall identify credible design extension conditions, based on operational experience, engineering judgment, and the results of analysis and research. This shall include multiple failure events without core melt situation as well as event sequences leading to significant core degradation/ melt (severe accidents), particularly those events that may challenge the containment.

5.18.2 An analysis of design extension conditions for the plant, including assessment of radiological impact, shall be performed. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered as design basis accident conditions, or to mitigate their consequences, to the extent practicable. This might require additional safety systems/features and complementary safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. Such safety features for design extension conditions, or extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state (refer clause 5.20) and the containment function can be maintained, with the result that significant radioactive releases would be practically eliminated. The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.

5.18.3 The design extension conditions shall be used to define the design basis for additional safety systems/features and complementary safety features, and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences. Complementary safety features include design or procedural considerations, or both, and are based on a combination of phenomenological models, engineering judgments, and probabilistic methods.

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

(a) be independent, of those used in more frequent accidents,

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

(c) have reliability commensurate with the function that they are required to fulfill.

The design shall be balanced such that no particular design feature or event makes a dominant contribution to the frequency of accidents involving severe degradation of core or core melt, taking uncertainties into account.

5.18.5 If the plant state is within design extension condition without core melt, it shall be brought to and maintained under safe state within 24 hours (desirable) or within 72 hours (mandatory). Thereafter safe shutdown state (refer section 5.20) should be maintained. In the design extension condition with core melt, the containment system and its safety features shall be able to perform in extreme scenarios that include, among other things, melting of the reactor core. Containment shall maintain its role as a leak-tight barrier for a period that allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage. Containment shall also prevent uncontrolled releases of radioactivity after this period.

Severe accident management guidelines shall be prepared, taking into account the plant design features and the understanding of accident progression and associated phenomena.

5.18.6 To the extent practicable, the design shall provide biological shielding of appropriate composition and thickness to protect operational personnel during design extension conditions, including severe accidents.

5.18.7 In the case of multi-unit plants, the use of available support from other units can be considered as extra advantage but its credit shall not be taken in safety

analysis. However, such support can be relied upon only if it can be established that the safety of the other units is not compromised under any condition.

5.18.8 The design shall take into account the availability of off-site services only in long term [refer section 5.15.2 (d)].

5.18.9 The design shall be such that design extension conditions that could lead to large or early releases of radioactivity are practically eliminated. For design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.

5.19 Combinations of Events and Failures

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

5.20 Reactor Safe States

Design should ensure that following anticipated operational occurrences or accident conditions, the fundamental safety functions are ensured and the reactor is maintained at safe states.

5.20.1 Controlled state

This is a state of the plant, following an anticipated operational occurrence or accident condition, in which the fundamental safety functions can be ensured and can be maintained for a time sufficient to implement provisions to reach a safe state /safe shutdown state. This state is characterised by:

(a) Core is subcritical

(b) Core heat is adequately removed

(c) Activity discharges are within acceptable limits.

In case of a DBA, it is mandatory to reach the safe shutdown state following a controlled state. During an accident (DBA and DEC without core melt), controlled state shall not be continued for more than 24 hours.

5.20.2 Safe Shutdown State

Safe shutdown state is the state of the plant, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and maintained continuously. This state is characterised by:

(a) Reactor under shutdown with desired margin below sub-criticality.

(b) Continuous decay heat removal up to ultimate heat sink through designed cooling chain.

(c) Availability of containment functions.

During a design basis accident, it is mandatory to reach the safe shutdown state following a controlled state.

5.20.3 Safe State

State of plant, following design extension condition without core melt, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time. This state is characterised by:

(a) Core is in long term subcritical state.

(b) Long term decay heat removal is established

(c) Containment functions are available and activity discharges are in accordance with the acceptable limits.

Design provisions shall be made to achieve and maintain safe state for 72 hours from the initiation of accident (design extension condition without core melt). Subsequently it is desirable to reach safe shutdown state.

5.20.4 Severe Accident Safe State

Severe accident safe state is a state which shall be achieved subsequent to a design extension condition with significant core damage or core melt phenomena. Severe accident safe state shall be reached at the earliest after an accident initiation. It should be possible to maintain this state indefinitely. During this state there is:

(a) No possibility of re-criticality.

(b) Fuel or debris are continuously cooled.

(c) Uncontrolled release of radioactivity to environment is arrested.

(d) Means to maintain above conditions are available for long term, including critical parameter monitoring.

(e) Monitoring of radiological releases and containment conditions.

As the plant state is in design extension condition with core melt (severe accident), the severe accident safe state should be preferably reached within about one week from accident initiation.

5B. DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT

5.21 Calibration, Testing, Maintenance, Repair, Replacement, Inspection and Monitoring of Items Important to Safety

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

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

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

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

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

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

5.21.4 Details of alternate approaches to monitor the performance of SSC, if any, shall be provided in the design documentation.

5.21.5 The design shall provide facilities for monitoring chemical conditions of fluids commensurate with the metallic and non-metallic materials used in the system design. In addition, the means for chemical addition to control or modify the chemical constituents of fluid streams shall be specified.

5.22 Ageing Management

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

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

5.22.2 Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behaviour of the plant or degradation that might occur in service. Required data shall be generated for these equipment for ageing management and estimation of their residual life.

5.22.3 In cases where the design life of equipment/component is less than the design life of the plant, and mid-term in-situ replacement of the equipment is warranted, adequate provisions shall be made in the design, particularly for the in core equipment, to facilitate such replacements.

5.23 Qualification of Items Important to Safety

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

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

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

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

5.23.4 Equipment that is credited to operate (e.g. certain instrumentation) during design extension conditions and during and after severe accidents scenario shall be shown, with reasonable confidence, to be capable of achieving the intended function under the expected environmental conditions. Severe accident management guidelines should address uncertainties arising from any shortfalls in such qualification of specific equipment/instrument.

5C. HUMAN FACTORS

5.24 Design for Optimal Operator Performance

Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process [5].

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

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

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

5.24.4 The operator shall be provided with the necessary information:

(a) to assess the general state of the plant in any condition,

(b) to operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions),

(c) to confirm that actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended, and

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

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

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

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

5.24.8 Dependence on early operator action should be avoided by design provisions as indicated below:

(a) All the required immediate responses to an abnormal situation are made automatic.

(b) All safety systems for prevention or mitigation of events within design basis shall be designed such that no operator action is necessary for first thirty minutes of any incident.

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

5.24.10 Automated response shall continue for at least a reasonable predetermined time dependent on prior assessment (Refer 5.14.8). However operator actions to enhance safety within such time can be allowed, if design envisages.

5.24.11 The need for operator intervention on a short time-scale of less than 30 minutes following a PIE should be kept to a minimum. The design should take into account that the credit for such operator intervention within 30 minutes of PIE is acceptable only if the:

(a) design can demonstrate that the operator has sufficient time to decide and to act,

(b) necessary information on which the operator must base a decision to act is simply and unambiguously presented,

(c) physical environment following the event is acceptable in the control room or in the supplementary control room/backup control points, and

(d) access route to that supplementary control room/backup control points, is available.

However, even in such cases the design shall not take credit for operator action within the first 15 minutes of PIE.

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

5D. OTHER DESIGN CONSIDERATIONS

5.25 Systems Performing Both Safety and Process Functions

5.25.1 In cases where a system performs both process functions and safety functions, the following design considerations shall apply:

(a) The process and safety functions shall not be credited at the same time.

(b) If the process function is operating, and a PIE specific to the process function is postulated, then it shall be shown that all its essential safety functions remains unaffected.

(c) The system shall be designed to the standards commensurate with the functions important to safety.

5.25.2 If the design includes sharing of instrumentation between a safety system and a non-safety system (such as a process or control system), then the following shall apply:

(a) The reliability and effectiveness of a safety system shall not be impaired by normal operation, by partial or complete failure in non-safety systems, or by any cross-link generated by the proposed sharing.

(b) Sharing shall be limited to the sensing devices and their pre-amplifiers or amplifiers as needed to get the signal to the point of processing.

(c) The signal from each sensing device shall be electrically isolated so that failures cannot propagate from one system to the other.

(d) Isolation devices between systems of different safety importance shall always be associated with the system classified as being of greater importance to safety.

5.26 Sharing of Safety Systems between Multiple Units of a Nuclear Power Plant

Safety systems and additional safety systems/features, required for DBAs and design

extension conditions without a core melt scenario, shall not be shared and interconnected between multiple units, unless this contributes to enhanced safety. Capability of complementary safety features, their support systems and onsite resource requirements for mitigating design extension condition with core melt scenario, shall be such that simultaneous handling of such events at all the reactors at a multiunit site is possible.

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

5.27 Pressure-retaining SSC and Systems Containing Fissile Material or Radioactive Material

All pressure-retaining SSC shall be protected against overpressure conditions, and shall be classified, designed, fabricated, erected, inspected, and tested in accordance with established standards.

5.27.1 All pressure-retaining SSC of the reactor coolant system and auxiliaries shall be designed with an appropriate safety margin to ensure that the pressure boundary will not be breached, and that fuel design limits will not be exceeded in normal operation, AOO, DBA or design extension conditions without core melt scenario.

5.27.2 Pressure-retaining components whose failure may affect nuclear safety shall be designed to permit inspection of their pressure boundaries throughout the design life of NPP.

5.28 Prevention of Harmful Interactions of Systems Important to Safety

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

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

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

5.29 Interactions between the Electrical Power Grid and the Plant

The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

5.29.1 NPP's mode of operation (e.g. base load unit, load follower, etc) shall be defined, and all relevant types of transients shall be analyzed. Droop characteristics as defined for that grid shall be followed. Design of SSC important to safety including fuel shall take into account the transients originating from such operation.

5.30 General Considerations for Instrumentation and Control System

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

5.30.1 Interference between protection systems and control systems shall be prevented by means of separation, by avoiding interconnection or by suitable functional independence.

5.30.2 Instrumentation and recording equipment shall be such that essential information is available to support plant procedures during and following any accident by:

(a) Indicating important plant parameters and radiological conditions.

(b) Identifying the locations of radioactive material.

(c) Facilitating decisions in accident management.

5.31 Use of Computer-based Systems or Equipment

If computer based systems or equipment are used for safety purpose, correct (with respect to specification), safe and complete implementation of the requirements shall be ensured. Software in these systems must be demonstrated to be safe and to have a high level of integrity. Diverse backup systems or hardwired based backup systems for instrumentation and control of important safety functions, especially protection function, shall be provided.

5.31.1 Integrity should be assured by developing system/software using systematic, technically appropriate, carefully controlled, fully documented and reviewable engineering process which is suitably interfaced with verification and validation activities.

5.31.2 The safety case in support of the system and in particular software safety and integrity shall be based on design and design documents produced during the system development, result of analysis of specifications, algorithms and implementation.

5.32 Design of Civil Structures

Civil structures shall be designed to meet the serviceability, strength and stability requirements for all possible load combinations due to loads arising out of normal operation, anticipated operational occurrences, DBA, and DEC including severe accident conditions, as well as from external hazards and their credible combinations with plant states.

5.32.1 External events to be considered in the design of civil structures include earthquakes, floods, high winds, tornadoes, tsunamis, extreme meteorological conditions and human induced events, as applicable. Civil structures important to safety shall also be designed and located so as to minimise the probabilities and effects of internal hazards such as fire, explosion, smoke, flooding, missile generation, pipe whip, jet impact or release of fluid due to pipe breaks.

5.32.2 The design specifications shall define all loads and load combinations, with due consideration given to probability of occurrence and loading time history. The serviceability considerations include satisfying limits on deflection, vibration, permanent deformation, cracking of concrete structural members and settlement.

5.32.3 Environmental impacts shall be considered in the design of civil structures and in the choice and selection of construction materials. Provision, wherever necessary, should be made for structural monitoring using instruments. The design shall enable implementation of periodic inspection programs for structures related to nuclear safety to verify structural conditions.

5.32.4 The design shall include provision for recording response of reactor building and another typical safety related structure in the event of an earthquake for post earthquake analysis.

5.32.5 The design shall ensure that no substantive damage to these SSC will be caused by the failure of any other SSC under safe shutdown earthquake (SSE) conditions.

5.33 Nuclear Power Plants Used for Cogeneration of Heat and Power

Nuclear power plants coupled with heat utilisation units shall be designed to preclude processes that transport radionuclides from the nuclear plant to heat utilization unit under conditions of operational states and in accident conditions.

5E. LAYOUT OF THE PLANT

The plant layout shall take into account requirements arising out of radiation zoning, industrial safety, nuclear security, availability of unobstructed access to buildings, movement of heavy machinery, seismic isolation gap between adjacent structural parts, avoiding overlapping of foundations, etc. Consideration shall also be given to externally and internally generated missiles, including events such as aircraft impact. During development of internal structural layout, apart from structural loading aspects, consideration shall also be given to radiation shielding, effective control of personnel movement for preventing spread of radioactivity within and to outside the plant, emergency requirements arising out of industrial and nuclear safety, provision of fire protection, nuclear security, surveillance and in-service inspection (ISI), maintenance and replacement requirements of the housed systems, movement of heavy loads inside the building, ergonomics etc.

5.34 Control of Access to the Plant and Systems

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

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

5.34.2 Prevention of unauthorised access to, or interference with, items important to safety, including computer hardware and software, shall be ensured.

5.35 Escape Routes from the Plant

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

5.35.1 Escape routes from the nuclear power plant shall meet the requirements for radiation zoning and fire protection, and the relevant AERB requirements for industrial safety and plant security.

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

5.36 Communication Systems at the Plant

Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and

to be available for use following all postulated initiating events and in accident conditions.

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

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

5F. COMMISSIONING AND DECOMMISSIONING

5.37 Commissioning of the Plant

All plant systems shall be so designed that, to the extent practicable, tests of the equipment can be performed to confirm that design requirements have been achieved prior to the first criticality. The design should also consider the need for related testing when specifying the commissioning requirements for the plant.

5.38 Decommissioning of the Plant

At the design stage, appropriate consideration shall be given to the incorporation of features which will facilitate the decommissioning and dismantling of the plant.

5.38.1 The design should consider that exposures of personnel and the public during decommissioning are maintainable within the limits prescribed by AERB and adequate protection of the environment from radioactive contamination shall also be ensured. Decommissioning aspects shall be considered at the design stage itself to include inter alia:

(a) the choice of materials, such that eventual quantities of radioactive waste are minimised and effective decontamination is facilitated,

(b) the access capabilities that may be required, and

(c) the facilities necessary for storing radioactive waste generated during both operation and decommissioning of the plant.

5G. SAFETY ANALYSIS

5.39 Safety Analysis of the Plant Design

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

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

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

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

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

5.40 Deterministic Approach

The deterministic safety analysis shall mainly provide:

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

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

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

(d) Comparison of the results of the analysis with dose limits and acceptable limits, and with design limits

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

(f) Demonstration that the management of design extension conditions is possible by the actuation of additional safety systems/ features or complementary safety features in combination with expected actions by the operator.

5.40.1 Deterministic safety analyses for design purposes shall be characterized by their conservative assumptions and bounding analysis. However, best estimate analysis together with an evaluation of uncertainty could be used in some cases to better define certain requirements for structures, systems and

components. The time span of any scenario that is analysed should extend up to the moment when the plant reaches a safe state or safe shutdown state.

5.40.2 If a 'best estimate' computer code instead of a 'conservative code' is used for design purpose, it shall be ensured that conservative initial and boundary conditions along with conservative assumptions with regard to the availability of systems are adopted. All uncertainties associated with the code models and plant parameters shall be bounded.

5.40.3 Realistic analyses should be used to evaluate the evolution and consequences of accidents. The realistic input data should be used in case extensive data are available; if the data are scarce, conservative input data shall be used. For the development of emergency operating procedures and for the analysis of design extension conditions, including severe accidents, best estimate methods and codes should be used. However, when determining what actions should be taken to prevent core melt, the range of uncertainties associated with the relevant phenomena should be determined.

5.41 Source Term Evaluation

An evaluation of the behaviour of fission products, radioactive corrosion products, activation products in coolant and impurities, and actinides following possible accidents of each type at the NPP shall be carried out early in the design stage. This is required to identify all important phenomena that affect source term behaviour and to identify the possible design features that could increase their retention in the plant.

5.41.1 The evaluation, before a plant is operated, of the source terms for operational states shall include all the radionuclides that, owing to either liquid discharges or gaseous discharges, may make a significant contribution to doses. The annual release of radioactive material to the environment can be evaluated by using an average value for the activity of the primary coolant. Values for the effect of spiking on the activity of the primary coolant due to applicable operational transient should be considered based on relevant operational data.

5.41.2 Different operational states and possible accident sequences could be grouped, and a bounding scenario chosen for detailed analysis representing each group. Separate analyses of the source term should be carried out for each group for which the phenomena that would affect the source term could be different. The evaluation of source terms shall also include a comprehensive analysis of postulated accidents in which the release of radioactive material would occur outside the containment. This exercise ensures that the design is optimised so that requirements for radiation protection, including restrictions on doses, are being met.

5.41.3 A similar range of different types of design extension conditions should be considered in the evaluation of the source terms including that would result

in severe accidents involving significant core damage or core melt. This exercise will also provide a basis for the emergency preparedness that may be required to protect the public under severe accident condition.

5.42 Probabilistic Approach

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

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

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

(c) providing assurance of the probability of occurrence and consequences of external hazards, in particular those unique to the plant site;

(d) checking compliance to probabilistic targets;

(e) providing basis for Technical Specification on testing frequencies and outage duration for equipment;

(f) providing assessment of risk of early large off site releases associated with containment failures; and

(g) calculating for multi-unit sites, the associated risk for site specific initiator. This assessment should also take into account of shared SSC.

5.43 Quantitative Safety Targets

The safety analysis conducted shall be able to demonstrate that the design of the nuclear power plant is capable in meeting the quantitative safety targets.

5.43.1 Safety targets for different accidents conditions are as below:

(a) Limits on core damage frequency (CDF) should be 1E-6/reactor-year due to internal events, for power and shutdown states.

(b) The cumulative core damage frequency should be less than 1E-5/ reactor-year for all internal events and external hazards including seismic hazards.

(c) Accident sequences with core melt which would lead to early or large release have to be practically eliminated. Quantitative target for the early or large release shall be less than 1E-7 per year.

5.43.2 The deterministically established containment performance (leakage rates) objective shall be met under all plant states. The containment shall be able to withstand the loads from severe accidents as well as challenges from various external threats. Loss of containment structural integrity shall be practically eliminated.

6. DESIGN OF SPECIFIC PLANT SYSTEMS

6A. REACTOR CORE AND REACTIVITY CONTROL

6.1 Reactor Core and Associated Features

The reactor core and associated coolant/moderator system, control and protection systems shall be designed with appropriate margin to assure that the specified design limits (clauses 5.3 and 5.43) are not exceeded and that dose criteria (clause 4.5) are applied in all operational states and in design basis accidents, with account taken of the existing uncertainties.

6.1.1 The design of the reactor core, reactor pressure vessel (RPV) and the reactor internal structures shall account for the static and dynamic loadings expected under operational states and design basis accidents with due regard to the effects of temperature, pressure, irradiation, ageing, creep, corrosion, erosion, hydriding, vibrations, fatigue etc. In all operational states and accident conditions other than severe accidents, adequate integrity of the core components shall be maintained to ensure:

(a) safe shutdown of the reactor and maintaining it in subcritical state with adequate shutdown margin, and

(b) coolable geometry and adequate core cooling.

6.1.2 The reactor core and associated coolant system, control and protection systems shall be designed so as to allow adequate inspection and test capability throughout the service life of the plant.

6.2 Performance of Fuel Elements and Assemblies

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

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

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

6.2.3 Specified fuel design limits shall not be exceeded in normal operation, and conditions that could be imposed on fuel assemblies during anticipated operational occurrences shall cause no significant additional deterioration. Permissible fission product leakage shall be included in fuel design limits and kept to a minimum.

6.2.4 The design shall provide means for allowing reliable detection of fuel defects in the reactor, and subsequent removal of failed fuel from the reactor if activity levels are exceeded.

6.2.5 It shall be possible to detect fuel failure in the core during power operation. It shall be possible to detect and identify the failed fuel in shutdown state.

6.2.6 The aforementioned requirements for reactor and fuel element design shall also be maintained in the event of changes in fuel management strategy or operational conditions during the plant life.

6.2.7 In design basis accidents, the specified fuel safety limits shall not be exceeded.

6.3 Structural Capability of the Reactor Core

The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for maintaining adequate cooling and the insertion of control rods is not impeded.

6.4 Control of the Reactor Core

The reactor core and associated coolant systems shall be designed so that in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for the possible positive reactivity insertion.

Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refuelling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified fuel design limits in all operational states shall be minimised.

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

6.4.2 In the design of reactivity control devices, due account shall be taken of wear out and of the effects of irradiation, such as burnup, changes in physical properties and production of gas.

6.4.3 The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (i) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (ii) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly, the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, main steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

6.4.4 The core and its control systems shall be so designed that uncontrolled increase of power cannot occur. The negative reactivity worth and the insertion rates of the control and protection systems shall be sufficient to override reactivity changes, including those due to internal and dynamic reactivity coefficients during all plant states. Positive reactivity insertion rate shall be within permissible limits.

6.4.5 The design of the core and the fuel management scheme provided should minimise the demands made on control system for maintaining flux shapes and levels and stability within specified limits in all operational states.

6.4.6 The reactor core including the associated coolant control and protection system shall be designed to assure that power oscillations which can result in conditions exceeding specified fuel design limits do not occur, or can be readily and reliably detected and suppressed.

6.4.7 Special consideration shall be given for the detectors and monitoring requirements for the first approach to criticality of a new type of reactor.

6.5 Reactor Shutdown

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

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

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

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

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

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

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

6B. REACTOR COOLANT SYSTEMS

6.6 Design of Reactor Coolant System

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

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

6.6.2 The design shall take into consideration the behavior of pressure boundary material under operational, maintenance and testing conditions and in design basis accidents, taking into account the expected end of life properties (which are affected by erosion, creep, fatigue, the chemical environment, the radiation environment and ageing), any uncertainties in determining the initial state of the components, and the rate of possible deterioration.

6.6.3 The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could be prone to brittle failure are avoided.

6.6.4 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 consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service.

6.6.5 The materials used in the fabrication of the component parts shall be so selected as to minimise their activation.

6.6.6 If heat removal function under the accident conditions involving primary heat transport pressure boundary is likely to be adversely affected, the system (provided to cope with this situation) shall be designed assuming single failure.

6.6.7 Components which are part of reactor coolant pressure boundary shall be designed, fabricated, inspected, erected and tested to the highest quality standards.

6.6.8 The pressure retaining boundary for reactor coolant shall be so designed that flaws are very unlikely to be initiated but, if initiated, would propagate only by very small amounts. Even if significantly higher growth were to take place it will take place, in such a manner that leak occurs before break permitting timely detection of flaws. Designs and plant states, in which components of the reactor coolant pressure boundary could exhibit brittle behaviour, shall be avoided. Process of leak before break needs to be established and proved (refer clause 5.15.3). System shall be provided for early leak detection and its adequacy shall be demonstrated.

6.6.9 Postulating break of the primary coolant system boundary shall be part of the design basis events. If the design envisages the complete guillotine break of a main coolant line as 'excluded from break postulates', it shall ensure:

(a) accessibility and the inspectability of each point of these lines throughout the life of NPP,

(b) provisions to allow access for a 100 % volumetric inspection of all the welds of the main coolant lines and of the parts of the large connecting pipes with a potential of degrading effects,

(c) provision to allow the use of two volumetric inspection methods for the dissimilar welds, and

(d) combination of different methods available to monitor primary leaks.

In such case, the break size should be limited to complete guillotine rupture of the largest pipe connected to a main coolant line (e.g. surge line for pressurizer). In practice, the designer has to assume that any pipe connected to a main coolant line might separate from its connecting nozzle. In these conditions, the flow area through which the primary water might escape is equal to the internal cross section of the nozzle, and no flow limiter can be taken into account in the corresponding calculations. Moreover to be in-line with LBB requirements (clause 5.15.3), the exclusion of guillotine break of main coolant pipe should be applicable for the loads:

(a) to be considered for the design of reactor core assembly and the internal structures of the reactor pressure vessel;

(b) to be considered for the design of the structures inside the containment building;

(c) considered for the spent fuel pool structure design (if internal to reactor building); and

(d) on supports of the SSC and additional safety systems/features and their environmental qualification requirement.

However, double ended guillotine rupture of a main coolant line (2A-opening) shall be assumed for the design of the emergency core cooling function (coolant mass flow requirement) and of the containment pressure boundary (design pressure, temperature and withstanding pipe whip or associated internal missiles) so as to ensure safety margins. The 2A-opening of main coolant pipes also have to be assumed for designing complementary safety features.

6.7 In-service Inspection of the Reactor Coolant Pressure Boundary

6.7.1 The components of the reactor coolant pressure boundary shall be designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the boundary.

6.7.2 Provision shall be made to implement a material surveillance programme for the reactor pressure vessel, particularly in high irradiation locations, and other important components as appropriate for determining the effect of environment on material properties.

6.7.3 Monitoring of soundness of the reactor coolant pressure boundary shall include ability to detect flaws, distortion, leakage and reduction in thickness at location prone to erosion.

6.8 Overpressure Protection of the Reactor Coolant Pressure Boundary

Provision shall be made to ensure that the operation of pressure relief devices will protect the pressure boundary of the reactor coolant systems against overpressure, and will not lead to the release of radioactive material from the nuclear power plant directly into the environment.

6.8.1 The reactor coolant system, its associated auxiliary systems, and the pressure control/over pressure protection systems shall be so designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during anticipated operational occurrences, and that at the same time the relief system is not actuated frequently.

6.9 Inventory of Reactor Coolant

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

6.9.1 A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to ensure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss, due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components that are part of the boundary. The system shall be designed to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available), the system safety function can be accomplished with the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

6.10 Cleanup of Reactor Coolant

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

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

6.11 Removal of Residual Heat from the Reactor Core

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

6.11.1 Suitable redundancy shall be provided in the design of the system to meet its functional requirements with sufficient reliability, assuming single failure.

6.11.2 Main coolant system coast down characteristics coupled with suitable layout of the system, to ensure cooling by thermosiphon, may be considered as part of residual heat removal system.

6.12 Emergency Cooling of the Reactor Core

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

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

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

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

(c) the effectiveness of the means of cooling the reactor core is maintained in presence of possible changes in the fuel and in the internal geometry of the reactor core; and

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

6.12.2 Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfill the requirements of leak before break (clause 6.6.8) with adequate reliability for each postulated initiating event.

6.12.3 Emergency cooling provisions shall be extended to remove heat from damaged/molten core following a DEC. Adequate consideration shall be given to extending the capability of system to remove heat from the core following a severe accident.

6.12.4 An emergency cool down system of high reliability for steam generator shall be provided to ensure that process parameters of the reactor coolant system during specified operational state and accident conditions are maintained within stipulated limits. To ensure this:

(a) emergency cool down system shall be independent of the steam generator main feed water system;

(b) the system shall be designed with sufficient reliability assuming a single failure; and

(c) in case the steam generator is used as only means for decay heat removal during design extension condition, additional diverse system shall be provided for steam generator cooling (e.g. fire water injection and passive heat removal system).

6.13 Heat Transfer to Ultimate Heat Sink

The system's safety function shall be to transfer combined heat load of the structures, systems and components under all operational states and design basis accidents, at a rate such that specified fuel design limits and specified design limits of the reactor coolant pressure boundary are not exceeded. All systems that contribute to the transport of heat, by supplying fluids to the heat transport systems, by conveying heat, or by providing power, shall be designed to achieve reliability commensurate with importance to their contribution to the overall heat transfer function.

6.13.1 Systems shall be provided to transfer residual heat from items important to safety at the nuclear power plant to an ultimate heat sink. This function shall be carried out with high levels of reliability.

6.13.2 Provisions shall be made for transfer of residual heat from damaged / molten core to an ultimate heat sink to ensure that acceptable temperatures can be maintained in structures, systems and components important to the safety function of confinement of radioactive materials in the event of a severe accident.

6.13.3 Suitable redundancy in components and systems, suitable interconnections, leak detection and isolation capabilities shall be provided to assure that the system safety functions can be accomplished assuming a single failure.

6.13.4 Natural phenomena and human induced events shall be taken into account in the design of systems, in the possible choice of diversity in the ultimate heat sinks and in the storage systems from which heat transfer fluids are supplied. Availability of heat sink should be ensured under the condition of non availability of off-site and on-site power for an extended period.

6.13.5 Seismically qualified onsite storage of adequate quantity of water shall be available for decay heat removal from core and spent fuel stored under water under all plant states for at least 7 days. In addition, provisions should be available for ensuring continued availability of heat sink beyond 7 days by alternate means. The minimum period of 7 days may be revised to a higher value depending on site/plant characteristics.

6C. CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM

6.14 Containment System for the Reactor

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

In addition to the enclosing building, containment system shall include:

(a) leak tight features and structures,

(b) associated systems for the control of pressure and temperature,

(c) features for isolation, and

(d) features for management and removal of fission products, hydrogen, oxygen, and other substances that may be released into the containment atmosphere.

6.14.1 The design of the containment system shall take into account all identified design basis accidents and design extension conditions.

6.14.2 The design shall consider containment response for pressure and temperature build-up expected during postulated design extension conditions with core melt. Consideration shall be given to: potential for generation and behaviour of inflammable gases like hydrogen.

6.15 Strength of the Containment Structure

The strength of the containment structure, including access openings, penetrations and isolation valves shall be based on the internal pressures and temperatures and dynamic effects such as missiles and reaction forces resulting from the design basis accidents and design extension conditions. An assessment shall be made of ultimate load bearing capacity of the primary containment structure. Design provision shall be made to prevent the loss of the containment structural integrity in all plant states. The use of this provision shall not lead to early or to large radioactive releases.

6.15.1 The effects of other potential energy sources, including for example, possible chemical and radiolytic reactions, shall also be considered. Calculation of the required strength of the containment structure shall include consideration of natural phenomena.

6.15.2 Provisions shall be included in the design to monitor the condition of the containment and associated features following a PIE.

6.15.3 The layout of the containment shall be such that sufficient testing, and repair if necessary, can be conducted at any time during the life of the plant. If a secondary containment structure is envisaged, the annular space between the primary and secondary containment shall have purging arrangement to maintain a negative pressure in the intervening space.

6.15.4 The containment structure and internal systems shall be designed and constructed in such a way that it is possible to perform a pressure test at a specified pressure to demonstrate its structural integrity.

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

6.16 Control of Radioactive Releases from the Containment

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

6.16.1 The containment structure and the systems and components affecting the leak tightness of the containment system shall be designed and constructed so that the leak rate can be tested during commissioning and subsequently during the operating lifetime of the plant at the containment design pressure.

6.16.2 The radioactive liquids accumulated in the reactor containment building following loss of coolant accident should not escape to the environment through seepage.

6.16.3 If a secondary containment is envisaged then design shall be such that secondary containment does not get over pressurized in the event of rupture of steam and feed water pipes passing through secondary containment.

6.16.4 If resilient seals or expansion bellows are used with penetrations, they shall be designed to have leak testing capabilities, at containment design pressure, independent of the overall leak rate determination of the containment, to demonstrate their continuing integrity throughout the life of the plant.

6.17 Isolation of the Containment

6.17.1 Piping Systems Penetrating Containment

Piping systems penetrating primary reactor containment shall be provided with leak detection, isolation, and containment capabilities having redundancy, reliability, and performance capabilities which reflect the importance of isolating these piping systems towards safety. Such piping systems shall be designed with a capability to test periodically the operability of the isolation valves and associated apparatus and to determine if valve leakage is within design limits.

6.17.2 Primary Containment Isolation

Each line that connects directly to the containment atmosphere and penetrates primary reactor containment shall be provided with containment isolation

valves[5] as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

(a) One locked closed isolation valve inside and one locked closed isolation valve outside containment; or

(b) One automatic isolation valve inside and one locked closed isolation valve outside containment; or

(c) One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve should not be used as the automatic isolation valve outside containment; or

(d) One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve should not be used as the automatic isolation valve outside containment.

Isolation valves outside containment shall be located as close to the containment as practical, and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

6.17.3 Reactor Coolant Pressure Boundary Penetrating Containment

Each line that is part of the reactor coolant pressure boundary and that penetrates primary reactor containment shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis:

(a) One locked closed isolation valve inside and one locked closed isolation valve outside containment; or

(b) One automatic isolation valve inside and one locked closed isolation valve outside containment; or

(c) One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve should not be used as the automatic isolation valve outside containment; or

(d) One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve should not be used as the automatic isolation valve outside containment.

5 In most cases, one containment isolation valve or check valve is inside the containment and the other isolation valve is outside the containment. Other arrangements might be acceptable, however, depending on the design.

Isolation valves outside containment shall be located as close to containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.

Other appropriate requirements such as higher quality in design, fabrication/ construction, and inspection and testing, additional provisions for in-service inspection, protection against more severe natural phenomena and additional isolation valves shall be provided to minimise the probability or consequences of an accidental rupture of these lines or of lines connected to them.

6.17.4 Closed System Isolation Valves

Each line that penetrates 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 which shall be either automatic, or locked closed, or capable of remote manual operation. This valve shall be outside containment and located as close to the containment as practical. A simple check valve should not be used as the automatic isolation valve.

6.17.5 The containment and associated systems shall be designed to permit appropriate inspection and testing to ensure functionally correct and reliable actuation of the containment isolation valves and dampers and their leak tightness during the design life of the plant.

6.18 Access to the Containment

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

6.18.1 Where provision is made for entry of operating personnel for surveillance purposes, provision for ensuring protection and safety for operating personnel shall be specified in the design.

6.18.2 Containment openings for the movement of equipment or material through the containment shall be designed to be closed reliably and quickly, commensurate with progression of postulated accidents in shutdown state, in the event that isolation of the containment is required.

6.19 Control of Containment Conditions

Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant, and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment, and that could affect the operation of systems important to safety.

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

6.19.2 The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels after an accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled in DBA and DEC.

6.19.3 The containment cooling should be maintainable even in the case of extended station black out (SBO) subsequent to loss of coolant accident. The containment design should be such that it is able to withstand expected pressure and temperature till reactor reaches safe shutdown state.

6.19.4 Necessary design features shall be provided to:

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

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

6.19.5 Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfillment of their safety functions, and to minimise interference with other safety functions (such as core cooling) in the event of deterioration of the coverings, thermal insulations and coatings.

6D. INSTRUMENTATION AND CONTROL SYSTEMS

6.20 Provision of Instrumentation

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

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

6.20.1 Control Systems

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

6.20.2 Protection System

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

The protection system shall be designed:

(a) to be capable of overriding unsafe actions of the control systems,

(b) with fail safe characteristics to achieve safe plant conditions in the event of failure of the protection system, and

(c) to ensure that safety action once initiated by protection system is sealed-in (latched).

6.20.3 The protection system design shall:

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

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

(c) make relevant information available to the operator for monitoring the effects of automatic actions; and

(d) provide manual initiation as backup of automatic safety actions.

6.21 Reliability and Testability of Instrumentation and Control Systems

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

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;

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

(c) effects of natural phenomena and postulated accident conditions on any channel do not result in loss of the protection system function.

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

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

6.21.3 When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of bypass of any protection system that is necessary for the duration of the testing or maintenance activities.

6.22 Separation of Protection Systems and Control Systems

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

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

6.23 Use of Computer Based Equipment in Systems Important to Safety

If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.

6.23.1 For computer based equipment in safety systems or safety related systems:

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

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

(c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team, to provide assurance of its high reliability. Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means (e.g. hardwired backup) of ensuring fulfillment of the safety functions shall be provided.

(d) Common cause failures deriving from software shall be taken into consideration.

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

(f) Functions not essential to safety shall be separate from and shown not to impact the safety function.

(g) The safety function shall normally be executed in processors separate from software that implements other functions, such as control, monitoring, and display.

(h) The design shall provide for effective detection, location, and diagnosis of failures in order to facilitate timely repair or replacement of equipment or software.

6.24 Main Control Room (MCR)

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

6.24.1 Displays in the control room shall provide the operator with adequate and comprehensive information on the state and performance of the plant. The layout and design of the safety related instrumentation, in particular, shall ensure prompt attention of the operator and provide him with accurate, complete and timely information on the status of all safety systems during all operational states and accident conditions. Also, if any part of the safety

systems has been temporarily rendered inoperative for testing, it should be done under administrative control and the bypass shall be displayed in the control room.

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

6.24.3 Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, and explosive or toxic gases. Such measures should ensure the habitability of MCR for a minimum period of 72 hours.

6.24.4 The safety functions initiated by automatic control logic in response to an accident should also be possible to be initiated manually from the main control room.

6.24.5 The layout of the controls and instrumentation, and the mode and format used to present information, shall provide operating personnel with an adequate overall picture of the status and performance of the plant and provide the necessary information to support operator actions.

6.24.6 The design of the MCR shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels are minimised to applicable standards and codes. Human Engineering aspects shall be taken into consideration in MCR design (refer clause 5.24.6)

6.24.7 Cable lay out for the instrumentation and control equipment in the MCR shall be arranged such that a fire in the supplementary control room cannot disable the equipment in the MCR.

6.24.8 The MCR shall be provided with secure communication channels to the on-site emergency support centre and to off-site emergency response organisations, and to allow for extended operating periods.

6.24.9 The design of MCR and supplementary control room (SCR) shall be such that no internal PIE can affect them simultaneously.

6.25 Supplementary Control Room (SCR)

Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the main control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor

can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored, if there is a loss of ability to perform these essential safety functions from the main control room.

6.25.1 The requirements of clause 6.24.3 for MCR for taking appropriate measures and providing adequate information for the protection of occupants against hazards also apply for the supplementary control room at the nuclear power plant.

6.25.2 The design of the SCR shall ensure that appropriate lighting levels and thermal environment are maintained, and noise levels are in line with applicable standards and codes.

6.25.3 The SCR shall be provided with secure communication channels to the onsite emergency support centre and to off-site emergency response organisations. The SCR shall allow for extended operating periods.

6.26 Onsite Emergency Support Centre (ESC)

An on-site emergency support centre, separate from both the main control room and the supplementary control room, shall be provided from which the emergency response can be directed at the nuclear power plant. The facility shall have adequate radiation shielding and shall be qualified for external events with sufficient margin.

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

6.26.2 The emergency support centre shall include display system indicating important parameters which are required for taking necessary actions during severe accidents.

6.26.3 Information about the radiological conditions in the plant and its immediate surroundings, and about meteorological conditions in the vicinity of the plant, shall be accessible from the emergency support centre.

6.27 Severe Accident Monitoring Instrumentation and Control

For the purpose of severe accident monitoring and management, appropriate means shall be considered for the plant, by which the operating personnel obtain information for event assessment, and for the planning and implementation of mitigating actions.

It shall be possible to assess the information about the following:

(a) Condition of core or debris

(b) Condition of reactor pressure vessel

(c) Condition of containment

(d) Condition of spent fuel storage pool

(e) Radiological situation in the plant, site and its immediate surroundings

(f) Status of implemented accident management measures.

The measurement systems/instrument shall be capable of measuring over the entire range within which the measured parameters are expected to vary during accident conditions.

6E. ELECTRICAL POWER SUPPLY SYSTEM

6.28 General Requirements for Electrical Systems

Electric power system shall comprise off-site and on-site supplies including emergency power supply system. The systems shall be designed, installed, tested, operated and maintained to permit functioning of structures, systems and components important to safety during all plant states.

6.28.1 Functional adequacy of both off-site and on-site systems shall be assured by having adequate capacity, redundancy, independence and testability.

6.28.2 Consideration shall be given for emergency power supply system for design extension conditions including severe accident.

6.29 Off-site Power System

Electric power from the transmission network to the on-site electric distribution system shall be supplied by two physically independent circuits. These shall be designed and located so as to minimise the probability of their simultaneous failure during normal operation and under accident conditions. Each of these circuits shall be designed to be available on a long-term basis following a loss of plant generation and loss of other circuit, to ensure continued availability of off-site power.

6.30 Emergency Power Supply

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

6.30.1 In the design basis for the emergency power supply at the nuclear power plant, due account shall be taken of the postulated initiating events and the associated safety functions to be performed, to determine the requirements for capability, availability, duration of the required power supply, capacity and continuity. Emergency power supply systems shall be capable of withstanding internal and external hazards with significant margin.

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

6.30.3 The emergency power supply shall be able to supply the necessary power during any PIE assuming the coincidental loss of off-site power. Emergency power supply system shall have sufficient redundancy, independence (including physical separation between independent systems), and testability to perform their safety functions, with high reliability assuming single failure.

6.30.4 Various means of supplying emergency power shall be available. Power may be supplied directly to the driven equipment (prime mover) or through an emergency electric power system.

6.30.5 The emergency electrical loads, the safety functions to be performed and the type of electric power for each safety load shall be identified. The quality, availability and reliability of power supply shall be commensurate with safety function.

6.30.6 Inspection of Emergency Power Supply System

The system shall be designed with a provision to test periodically:

(a) the operability and functional performance of the components of the on-site power system, and

(b) operability of the system as a whole and the full operational sequence that brings the system into operation.

6.30.7 Continuity of DC power shall be ensured such that any short term actions necessary to mitigate the consequences of design extension conditions can be completed despite the loss of the AC power sources and the event that triggered it.

6.30.8 The design basis for any diesel engine or other prime mover [6] that provides an emergency power supply to items important to safety shall include:

(a) The capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period [not less than 7 days, refer clause 5.15.2 (d) and 6.13.5]

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

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

6.30.9 The design shall also include a dedicated power source adequately protected from external hazards, to supply the necessary power in design extension conditions.

6.30.10 The dedicated power source shall be independent and physically separated from the emergency power source for design basis accidents. The dedicated back-up power system connection time shall be consistent with battery autonomy

6.30.11 The dedicated power source shall be capable of supplying the necessary power to prevent significant core and spent fuel degradation in the event of the loss of the off-site power combined with the failure of the emergency power source, for design basis accidents.

6.30.12 The dedicated power source shall be capable of supplying power to the equipment necessary to mitigate the consequences of design extension conditions involving a loss of the off-site power combined with the failure of the emergency power source, for design basis accidents.

6.30.13 Equipment necessary to mitigate the consequences of a core melt accident shall be capable of being supplied by any of the power sources.

6F. SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS

6.31 Performance of Supporting Systems and Auxiliary Systems

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

[6] A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.

6.32 Component Cooling Water System

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

6.32.1 The design of component cooling water system shall be such as to ensure that non-essential parts of the systems can be isolated.

6.33 Process Sampling Systems and Post-accident Sampling Systems

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

6.33.1 Appropriate means shall be provided for the monitoring of radioactivity in fluid systems that have the potential for significant contamination (primary and secondary coolant systems, component cooling system, etc.), and for the collection of process fluid samples.

6.34 Compressed Air Systems

The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanliness of the air to be provided.

6.34.1 Compressed air systems shall be designed such that non-essential parts of the systems can be isolated.

6.34.2 Consideration should be given for avoiding use of compressed air driven devices inside the containment for continued use, during accident management.

6.35 Air Conditioning Systems and Ventilation Systems

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

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

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

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

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

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

(e) control release of gaseous radioactive material to the environment below the authorised limits for discharges and to keep them as low as reasonably achievable.

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

6.36 Fire Protection Systems

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

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

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

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

6.36.4 Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fire that starts.

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

6.36.6 Consideration shall be given to personnel safety while designing fire protection system.

6.37 Lighting Systems

Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.

6.38 Overhead Lifting Equipment

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

6.38.1 The overhead lifting equipment shall be designed so that:

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

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

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

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

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

6G. OTHER POWER CONVERSION SYSTEMS

6.39 Steam Supply System, Feed Water System and Turbine Generators

The design of the steam supply system, feed water system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states and in accident conditions.

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

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

6.39.3 The turbine generators shall be provided with appropriate protection such as over speed protection and vibration protection, and measures shall be taken to minimise the possible effects of turbine generated missiles on items important to safety.

6.39.4 The secondary system design should envisage house load operation of turbine generator for an adequate time.

6H. TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE

6.40 Systems for Treatment and Control of Waste

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

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

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

6.40.3 Adequate systems shall be provided for the handling of radioactive solid or concentrated wastes and safely storing them for a reasonable period of time on the site. Adequate consideration should be given to make provision for handling waste generated during severe accident scenarios.

6.41 Systems for Treatment and Control of Effluents

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

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

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

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

6I. FUEL HANDLING AND STORAGE SYSTEMS

6.42 Fuel Handling and Storage Systems

Fuel handling and storage systems provided at the nuclear power plant shall be designed to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.

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

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

6.42.3 The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed to:

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

(b) permit inspection of the fuel;

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

(d) prevent damage to the fuel;

(e) prevent the dropping of fuel in transit;

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

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

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

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

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

(b) prevent the damage due to dropping of spent fuel in transit;

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

(d) prevent the potentially damaging dropping on the fuel of heavy objects such as spent fuel casks, cranes or other objects;

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

(f) control levels of soluble absorber if used for criticality safety;

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

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

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

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

6.42.5 For reactors using a water pool system for fuel storage, the design of the plant shall include the following:

(a) Means for controlling the temperature, water chemistry and activity of water in which irradiated fuel is handled or stored

(b) Means for monitoring and controlling the water level in the fuel storage pool and means for detecting leakage

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

(d) Means for monitoring radiation levels and the air activity concentrations in the spent fuel storage pool area.

6J. RADIATION PROTECTION

6.43 Design for Radiation Protection

Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the prescribed limits and will be kept as low as reasonably achievable.

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

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

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

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

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

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

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

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

6.43.9 Access control provisions (interlocks, turnstiles, and locked gates) and procedures shall exist for entering into areas where activity levels are expected to be high. Areas requiring personnel occupation shall be easily accessible (with mobile shielding, if required), and shall have adequate control of atmosphere and/or shall have provisions for fresh air supply.

6.44 Means of Radiation Monitoring

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

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

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

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

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

6.44.5 Stationary equipment shall be provided for monitoring radioactive effluents and effluents with possible contamination, prior to or during discharges from the plant to the environment. On-line monitoring and recording of the release of radioactive liquids and gases to the environment shall include an integrated monitoring and recording system for the stack effluent for identified radionuclides.

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

6.44.7 Facilities shall be provided for monitoring the internal and external exposures and contamination of operating personnel. Processes shall be put in place for assessing and for recording the cumulative doses to workers over a period of time.

6.44.8 Means shall be provided for monitoring the reactor containment atmosphere, spaces containing components for recirculation of loss-of-coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and under accident conditions.

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

(a) exposure pathways to people, including the food chain,

(b) radiological impacts, if any, on the local environment,

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

(d) the possibility of there being any unauthorised routes for radioactive releases.

7. REINFORCING AND ENHANCING SAFETY FURTHER

7.1 General

The safety requirements for design of nuclear power plants prescribe all-risk approach, with appropriate consideration of probability of occurrence, associated uncertainties, and potential consequences, including cliff edge effects. This also addresses a broad range of challenges to safety of nuclear reactors and spent fuel facilities, including internal hazards, external hazards, and security threats during all modes of plant operation.

7.1.1 The design requirements prescribed in previous sections should also address in a risk-informed manner both design basis accidents and design extension conditions. But, the capability to predict and control an event becomes increasingly more difficult as the frequency of occurrence of the event decreases. The design of nuclear power plant should address this by providing sufficient safety margins.

7.1.2 The purpose of this section is to foresee additional provisions supporting the accident management infrastructure that might be needed to handle extreme events, along with unexpected failure of existing safety features/systems. This section provides the minimum requirements for such additional supports.

7.2 Safety Approach in case of Unexpected Events

Pre-planned and well-executed human actions constitute an important management feature to prevent and mitigate the consequences of failure of engineered systems. Reliance on established procedures, controls and processes, coupled with rigorous training cannot completely preclude collateral events or errors, particularly when the events are far beyond those previously considered, e.g., extreme external initiating events.

7.2.1 The approach is to provide a diverse and flexible accident response capability that would provide a backup to permanently installed plant equipment, that might be unavailable following certain extreme conditions (e.g. extreme natural phenomena such as earthquakes, flooding and high winds), and would supplement the equipment already available for responding to severe accidents. The approach shall include design measures to provide multiple means of obtaining power and water needed to fulfil the key safety functions of maintaining core cooling, containment integrity, and spent fuel pool cooling.

7.3 Requirements for Additional Facilities

The above approach shall include development of accident management techniques that improve the capability of a plant to survive an extended loss of all AC power, loss of normal heat sinks and loss of normal access to plant

site, etc., as a result of extreme events. It shall include equipment to respond to such challenges; procedures and guidance; equipment readiness, storage, and transportation; and training. The increased equipment capability will consist of installed equipment, portable equipment stored onsite, and portable equipment in nearby establishments and other national facilities.

7.3.1 The provisions described in the following paragraphs address requirements considering the possibility of an event that could be more severe than known historical events.

7.3.2 The design should recognise the need to provide accident management capabilities when the onsite and the offsite infrastructure are severely damaged. The approach should be phased, to consider the immediate need to maintain core cooling, spent fuel cooling and containment integrity, and the potential need to maintain these capabilities for an extended period.

7.3.3 The means for core and spent fuel cooling should be such as to cope with prolonged loss of all AC power sources. The design should consider alternative core cooling paths, alternative power connections and alternative pumping capability and water supply. Such safety provisions should not get damaged due to effect of combined external events such as earthquake and tsunami or earthquake and large area fire.

7.3.4 Other similar measures should include enhanced command and control, improved emergency data acquisition and transmission, hardened filtered containment vents or comparable measures and capability. Procedures giving consideration to possibility of handling large amount of contaminated water storage should also be in place.

7.3.5 Provisions should be so placed as to remain functional in case of extreme external hazards affecting the rest of the plant. For design, operation and storing of such provisions or mechanisms, the following principles should be adopted:

(a) Survivability in extreme external events

(b) Easy serviceability by available staff (without specialisation)

(c) Maintainability as these remain mainly on standby

(d) Compatibility with plant design

(e) Adaptability for different needs

(f) Mobility to reach different sections of the plant

(g) Manoeuvrability

(h) Diversity to increase availability in unforeseen situations.

7.4 Specific Provisions and Means

The specific design requirements with respect to additional means/provisions will depend on location (site) as well as design of the plant. However, the minimum requirements that should be fulfilled are given in the following paragraphs:

7.4.1 Enhanced Off-site Power Supply Systems

The diversity and reliability of off-site power sources and associated systems should be maintained by such means as multiple power transmission lines from diverse routes and sources (clause 6.29), improved seismic resistance of the switchyard and substations, and additional high voltage and temporary cables along with backup electrical equipment compatible with existing switchyard and substations. The responsible organisation should implement administrative arrangements (including staff availability, training, etc.) to guarantee that nuclear power plants are the priority 'consumers' to have electrical supply restored from the national or regional grid.

7.4.2 On-site Power Supply Systems

Design should ensure functional capability of existing electrical equipment under extreme environmental conditions caused by external hazards and provide procedures and training on the use of electrical equipment including usage under harsh environmental conditions during severe accidents.

The design shall enhance the capability to connect electrical power supplies to essential equipment and instrumentation upon the loss of fixed equipment.

Means shall be provided to cope with a prolonged SBO by portable (battery recharging, instrumentation and controls supplies, etc.) spot power and mobile generators (for larger electricity demands) for enhancing electrical supplies. Design shall ensure increased capacity (24 hours / 72 hours as envisaged in specific design) and discharge times for batteries, with the capability to recharge the batteries.

7.4.3 Cooling Systems

Robustness of ultimate heat sinks shall be maintained and it shall be able to demonstrate long-term heat removal capability in the event of extended SBO. The means for enhancement in decay heat removal from the core or cooling the spent fuel should:

(a) reinforce systems capable of removing decay heat over the long term, such as systems and components being able to maintain the capacity of the steam generators (in pressurised water reactors) to remove heat to the atmosphere (alternate means to feed water and relief valves);

(b) use alternate paths and means to supply water to cool the reactor core, spent fuel or molten core catcher as applicable; and

(c) use sprinkler systems as an alternative for cooling in the spent fuel pool, especially for situations with large losses of pool water inventory.

The reactor core, spent fuel pool and containment cooling shall be enhanced by:

(a) protecting existing equipment by providing barriers for flooding, placing the pumps at higher elevations within the plant;

(b) increasing capability and mission time of existing fixed equipment;

(c) using mobile pumping equipment (e.g. fire trucks and diesel driven pumps) for alternative sources of water and diversifying backup in case the existing fixed equipment fails; and

(d) using easily accessible quick-connection equipment (piping, hoses, etc.) to provide alternative sources of cooling water to the core, the spent fuel pool and the containment, without the need to enter areas where personnel would be endangered by radiation, debris, high temperatures or steam.

7.4.4 Alternatives to the Ultimate Heat Sink

The design should implement alternative pathways to the existing ultimate heat sinks and preferably have a diverse heat sink. Use of other heat sinks, such as alternative sources of water bodies should be explored. Design should explore the possibility of using air cooling systems as an alternative to the existing ultimate heat sink.

7.4.5 Containment Systems

Protection of containment under severe accident conditions shall be ensured under any extreme situation due to external events. Alternate means of containment cooling and heat management, including features to enable the safe use of non-permanent equipment, shall be provided which shall be available under prolonged station blackout condition. As an extreme exigency, venting of containment should be undertaken to avoid containment failure. However, in such cases, filtered containment vent shall be adopted. Venting shall not be done as a near term measure.

7.4.6 Communication, I and C Systems and Emergency Response

I and C systems design enhancement shall ensure equipment functionality to remain capable of monitoring plant conditions (essential plant parameters)

under extreme environmental conditions associated with severe accident. Provision of alternative power supplies for essential instrumentation (supplies and connection capability) shall be ensured. The design shall provide alternative motive force for equipment (valves and dampers) to implement actions in response to severe accidents.

Also, additional or improved (over the existing) radiation monitoring equipment for monitoring on-site conditions during severe accidents shall be provided. The responsible organisation shall develop operator training to address plant monitoring during degraded plant conditions with questionable instrumentation or readings.

REFERENCES

1. INTERNATIONAL ATOMIC ENERGY AGENCY, 'Safety Fundamentals, Fundamental Safety Principles', IAEA SF-1, IAEA, Vienna (2006).
2. ATOMIC ENERGY REGULATORY BOARD, 'Quality Assurance in Nuclear Power Plants', AERB/NPP/SC/QA (Rev-1) AERB, Mumbai, (2009).
3. ATOMIC ENERGY REGULATORY BOARD, 'Site Evaluation of Nuclear facilities', AERB/NF/SC/S (Rev-1) AERB, Mumbai, (2014).
4. ATOMIC ENERGY REGULATORY BOARD, 'Management of Radioactive Waste', AERB/NRF/SC/RW AERB, Mumbai, (2007).
5. ATOMIC ENERGY REGULATORY BOARD, 'Nuclear Power Plant Operation', AERB/NPP/SC/O (Rev 1) AERB, Mumbai, (2008).

BIBLIOGRAPHY

1. ATOMIC ENERGY REGULATORY BOARD, 'Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants', AERB/NPP-PHWR/SC/D (Rev-1) AERB, Mumbai, (2009).

2. ATOMIC ENERGY REGULATORY BOARD, 'Draft Safety Criteria and Guidelines for Design of Fast Breeder Reactors', AERB, Mumbai August 2011.

3. ATOMIC ENERGY REGULATORY BOARD, 'Glossary of Terms for Nuclear and Radiation Safety', AERB Safety Glossary, AERB/SG/GLO, AERB, Mumbai, India, (2005).

4. ATOMIC ENERGY REGULATORY BOARD, Kudankulam NPP Units 1&2, Safety Review Experience, Recommendation on Requirements for Future Imported Nuclear Power Plants, AERB, Mumbai, India, (2010).

5. ATOMIC ENERGY REGULATORY BOARD, 'Operability Determination and Audit Checks during Design and Construction of Nuclear Power Plants', AERB, Mumbai, India, (2010).

6. ATOMIC ENERGY REGULATORY BOARD, 'Proposed AERB design requirements for addressing beyond design basis accidents in Nuclear Power Plants' Report of the committee for severe accident management, (2009).

7. ATOMIC ENERGY REGULATORY BOARD, Report of the Task Group for Preliminary Study of Reactors of External Origin, AERB, (2008).

8. CANADIAN NUCLEAR SAFETY COMMISSION, Regulatory Document on Design of New Nuclear Power Plants, RD–337, CNSC, (2008).

9. FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY, Safety criteria for design of nuclear power plants, YVL1-0E, (1996).

10. INTERNATIONAL ATOMIC ENERGY AGENCY, 'Basic Safety Principles for Nuclear Power Plants' INSAG-12, IAEA, Vienna (1999).

11. INTERNATIONAL ATOMIC ENERGY AGENCY, 'Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life' INSAG-19, IAEA, Vienna (2003).

12. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design Specific Safety Requirements: IAEA SS-R-2.1, IAEA, Vienna (2012).

13. INTERNATIONAL ATOMIC ENERGY AGENCY, 'The Chernobyl Accident Updating of INSAG 1 & INSAG-7', IAEA, Vienna (1992).

14. INTERNATIONAL ATOMIC ENERGY AGENCY, 'The safety of nuclear power' INSAG-5, IAEA, Vienna (1992).

15. Technical Guidelines for design and construction of the next generation nuclear power plants with pressurized water reactors' adopted during GPR/ German Experts during plenary meeting held on October 19 and 26, 2000.

16. THE OAK RIDGE NATIONAL LABORATORY, A note on 'An evolution of alternate safety criteria for nuclear power plants' prepared for The Oak Ridge National Laboratory, N-1806- ORNL, USA, (1982).

17. UNITED STATES NUCLEAR REGULATORY COMMISSION, Annexure A to 10 CFR Part 50 General Design Criteria (GDC) for Nuclear Power Plant, USNRC (2012).

18. UNITED STATES NUCLEAR REGULATORY COMMISSION, Feasibility study for a risk-informed and performance-based regulatory structure for future plant licensing, NUREG 1860 Vol. 1, USNRC, (2007).

19. UNITED STATES NUCLEAR REGULATORY COMMISSION, Policy Issue (Notation Vote) on Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced light water reactor (ALWR) Designs, SECY-93-087, (1993).

20. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Harmonization of Reactor Safety in WENRA Countries, report by WENRA Reactor Harmonization Working Group, (2006).

21. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Progress towards Harmonisation of Safety for Existing Reactors in WENRA Countries study by WENRA Reactor Harmonization Working Group, (2011).

22. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, 'Safety of New NPP Designs' study by WENRA Reactor Harmonization Working Group, (2013).

23. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, WENRA Statement on Safety Objective for New Nuclear Power Plants, WENRA, (2010).

24. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, 'WENRA Reactor Safety Reference Levels' published by WENRA Reactor Harmonization Working Group, (2006)

LIST OF PARTICIPANTS

EXPERT COMMITTEE FOR DEVELOPMENT OF SAFETY CODE FOR DESIGN OF LIGHT WATER BASED NUCLEAR POWER PLANTS

Dates of meeting:	November 1, 2012	January 28, 2013
	March 5, 2013	March 12, 2013
	March 28, 2013	April 1, 2013
	April 5, 2013	April 12, 2013
	April 18, 2013	April 26, 2013
	May 2, 2013	August 14, 2013
	August 28, 2013	September 10, 2013
	September 13, 2013	

Members and Expert Committee:

Shri S.A. Bhardwaj (Chairman)	:	NPCIL (Former)
Shri V.K. Raina	:	BARC (Former)
Shri K.K. Vaze	:	BARC (Former)
Shri M.K. Balaji	:	NPCIL (Former)
Shri A.K. Balasubramanian	:	NPCIL
Shri R.I. Gujrathi	:	AERB (Former)
Shri Fredric Lall	:	AERB
Shri L.R. Bishnoi	:	AERB
Shri A.D. Roshan	:	AERB
Shri J. Koley (Member Secretary)	:	AERB
Dr. S. Saha	:	NPCIL (Co-opted)
Shri D. Bhatacharya	:	AERB (Co-opted)
Shri P. Krishnakumar	:	NPCIL (Co-opted)
Shri P. Bansal	:	AERB (Co-opted)

ADDITIONAL SPECIALISTS CONTRIBUTED FOR PREPARATION OF DRAFT CODE

The specialists worked during the period November 17, 2012 to March 2, 2013 for drafting and May 6, 2013 to August 9, 2013 for reviewing.

Specialists in Working Group:

Dr. H.G. Lele	:	BARC
Shri D.K. Shukla	:	BARC
Shri D. Mukhopadhyay	:	BARC
Shri K.R. Anilkumar	:	NPCIL
Shri G. Biswas	:	NPCIL
Shri H.P. Rammohan	:	NPCIL
Shri Abhijit Harshan	:	NPCIL
Shri Neeraj Agrawal	:	NPCIL
Shri Sandeep Saxena	:	NPCIL
Shri H. Kalra	:	NPCIL
Shri Priyanka Nathani	:	NPCIL
Shri S.K. Yadav	:	NPCIL

ADVISORY COMMITTEE ON CODES, GUIDES, AND ASSOCIATED MANUAL FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD)

Dates of meeting:	January 9, 2014	January 24, 2014
	April 10, 2014	June 12, 2014
	June 27, 2014	July 10,2014
	July 25, 2014	August 01, 2014
	August 08, 2014	August 14, 2014
	August 22, 2014	September 15, 2014
	October 27, 2014	

Chairman and Members of ACCGD:

Shri K.K. Vaze (Chairman)	:	BARC (Former)
Shri S.G. Ghadge	:	NPCIL
Dr. P. Chellapandi	:	IGCAR
Dr. P.K. Vijayan	:	BARC
Shri Y.S. Mayya	:	BARC
Shri A.J. Gaikwad	:	AERB
Shri K. Srivasista	:	AERB
Shri S.K. Ghosh	:	AERB
Shri P. Bansal	:	AERB
Shri G.M. Behera (Member Secretary)	:	AERB

SUB COMMITTEE OF ADVISORY COMMITTEE ON CODES, GUIDES, AND ASSOCIATED MANUAL FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD)

Dates of meeting:	July 10, 2014	July 18, 2014
	July 25, 2014	July 30, 2014
	August 08, 2014	August 14, 2014
	August 19, 2014	August 22, 2014
	August 25, 2014	September 30, 2014

Convener and Members of the Sub-committee:

Shri S.K. Ghosh (Convener)	:	AERB
Dr. S. Saha (Alternate Convener)	:	NPCIL
Shri J. Koley	:	AERB
Shri A.D. Roshan	:	AERB
Shri G.M. Behera	:	AERB
Shri P. Krishnakumar	:	NPCIL
Shri D. Bhattacharya (Member Secretary)	:	AERB
Shri P. Bansal (Alternate Member Secretary)	:	AERB

ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS)

Dates of meeting:	March 6, 2014	June 30, 2014
	July 4, 2014	December 4, 2014

Members and Invitees of ACNS :

Dr. Baldev Raj (Chairman)	:	IGCAR (Former)
Shri S.A. Bhardwaj	:	NPCIL (Former)
Shri K.K. Vaze	:	BARC (Former)
Shri S.G. Ghadge	:	NPCIL
Shri Rajnish Prakash	:	HWB
Dr. P. Chellapandi	:	IGCAR
Dr. D.N. Sharma	:	BARC
Prof. J.B. Doshi	:	IIT, Bombay (Former)
Shri R. Bhattacharya	:	AERB
Shri A.J. Gaikwad	:	AERB
Shri S.A. Hussain	:	AERB (Former)
Shri K. Srivasista (Member-Secretary)	:	AERB

LIST OF SAFETY CODE ON DESIGN OF LIGHT WATER REACTOR BASED NUCLEAR POWER PLANTS

S. No.	Safety Series No.	Title
1	AERB/NPP-LWR/SC/D	Design of Light Water Reactor Based Nuclear Power Plants

AERB SAFETY CODE NO. AERB/NPP-LWR/SC/D

Published by **:** Atomic Energy Regulatory Board
Niyamak Bhavan, Anushaktinagar
Mumbai - 400 094
INDIA.

BCS