



GOVERNMENT OF INDIA

**AERB SAFETY CODE**

**DESIGN OF SODIUM COOLED FAST REACTOR  
(SFR) BASED NUCLEAR POWER PLANTS**



**ATOMIC ENERGY REGULATORY BOARD**



**AERB SAFETY CODE NO. AERB/NPP-SFR/SC/D**

**DESIGN OF SODIUM COOLED FAST REACTOR (SFR) BASED  
NUCLEAR POWER PLANTS**

**Approved by the Board of AERB in December 2025**

**Atomic Energy Regulatory Board  
Mumbai-400094  
India  
December 2025**

Orders for this Code should be addressed to:

Chief Administrative Officer  
Atomic Energy Regulatory Board  
Niyamak Bhavan  
Anushaktinagar  
Mumbai-400094  
India

## FOREWORD

The Atomic Energy Regulatory Board (AERB) was constituted in 1983, to carry out certain regulatory and safety functions envisaged under Section 16, 17 and 23 of the Atomic Energy Act, 1962. AERB has powers to lay down safety standards and frame rules and regulations with regard to the regulatory and safety requirements envisaged under the Act. The Atomic Energy (Radiation Protection) Rules, 2004, provides for issue of requirements by the Competent Authority for radiation installations, sealed sources, radiation generating equipment and equipment containing radioactive sources, and transport of radioactive materials.

With a view to ensuring the protection of occupational workers, members of the public and the environment from harmful effects of ionizing radiations, AERB regulatory documents establish the requirements and guidance for all stages during the lifetime of nuclear and radiation facilities and transport of radioactive materials. These requirements and guidance are developed such that the radiation exposure of the public and the release of radioactive materials to the environment are controlled; the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation is limited, and the consequences of such events, if they were to occur are mitigated.

The Regulatory documents apply to nuclear and radiation facilities and activities giving rise to radiation risks, due to the use of radiation and radioactive sources, the transport of radioactive materials and the management of radioactive waste.



Fig. 1 Hierarchy of Regulatory Documents

Safety codes establish the objectives and set requirements that shall be fulfilled to provide adequate assurance for safety. Safety Standards provide models and methods, approaches to achieve those requirements specified in the Safety Codes. Safety Guides elaborate various requirements specified in the Safety Codes and furnish approaches for their implementation. Safety Manuals detail instructions/safety aspects relating to a particular application. The hierarchy of Regulatory Documents is depicted in Figure 1.

The recommendations of international expert bodies, notably the International Commission on Radiological Protection (ICRP) and the International Atomic Energy Agency (IAEA) are taken into account while developing the AERB Regulatory safety documents.

The principal users of AERB regulatory safety documents are the applicants, licensees, and other associated persons in nuclear and radiation facilities including members of the public. The AERB regulatory safety documents are applicable, as relevant, throughout the entire lifetime of the nuclear and radiation facilities and associated activities. The AERB regulatory safety documents also form the basis for regulation such as safety review and assessment, regulatory inspections and enforcement.

AERB had issued Safety Criteria' for Design of PFBR (Rev. 1, 1990), which was later updated as 'Safety Criteria and Guidelines' for Design of Fast Breeder Reactors (Rev. 4, 2015)' incorporating post-Fukushima design upgradation requirements and also appropriately taking into consideration Gen IV fast reactor requirements. AERB has now subsumed these Criteria and Guidelines into this Safety Code on 'Design of Sodium Cooled Fast Reactor (SFR) Based Nuclear Power Plants'. In drafting the Safety 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 (Rev.1) 2016 on 'Safety of Nuclear Power Plants: Design', AERB Safety Code No. AERB/NPP-LWR/SC/D (2015) on 'Design of Light Water Based Nuclear Power Plants' and AERB Safety Code No. AERB/NPP-PHWR/SC/D (Rev. 1) 2009 on 'Design of Pressurised Heavy Water Based Nuclear Power Plants', 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.

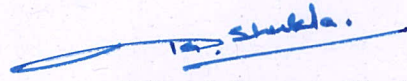
This Safety Code is effective from the date of its issue and it applies to Sodium Cooled Fast Reactor (SFR) based Nuclear Power Plants to be built after the issue of this Safety Code. In case any specific requirement(s) is/are not applicable to any particular system or feature, based on its design, then such inapplicability shall be justified.

Requirements contained in this Safety Code, to the extent practicable, shall also be applied during Periodic Safety Review (PSR) of SFR based NPPs built before issue of this Safety Code to check existing NPP design against current safety standards and identify non-conformances, if any. Adequate corrective actions (backfits or other alternate measures including administrative controls and operating procedures) shall be implemented to ensure that current safety requirements are addressed to provide equivalent level of safety.

For aspects not covered in this code, applicable national and international standards, codes and guides acceptable to AERB and applicable AERB safety directives should be followed. Non-radiological aspects of industrial safety and environmental protection are not explicitly considered in this code. Industrial safety shall be ensured by compliance with all relevant industrial safety requirements under prevailing statutes.

Safety related terms used in this Safety Code are to be understood as defined in the AERB Safety Glossary (AERB/GLO, Rev.1). The special terms which are specific to this Safety Code are included under section on 'Special Terms and Interpretation'. In addition, the terms already defined in AERB Safety Glossary AERB/GLO, Rev.1, and being used in this Safety Code with a specific context and require interpretation or explanation are also included in this section. Annexure, references and bibliography are to provide information that might be helpful to the user.

This Safety Code has been drafted by an In-House Working Group (IHWG). The draft was further reviewed by a working group with specialists drawn from technical support organisations and institutions, and other consultants. The comments obtained from the major stakeholders and member of public have been suitably incorporated. The Safety Code has been vetted by the AERB Advisory Committee on Nuclear and Radiation Safety (ACNRS). AERB wishes to thank all individuals and organizations who have contributed to the preparation, review and finalization of this Safety Code.



**(Dinesh Kumar Shukla)**  
**Chairman, AERB**





## **SPECIAL TERMS AND INTERPRETATIONS**

### **Cold Shutdown**

Shutdown state in which the temperature of the primary heat transport system at inlet is less than the specific value (e.g. 180 °C for sodium).

### **Core Disruptive Accident (CDA)**

Postulated whole core accident producing rapid power rise which leads to fuel melting, fuel vaporization and pressure build-up, and ultimate neutronic shutdown due to physical disassembly of the core.

### **Fuel Subassembly**

A group of fuel pins including blanket pins and supporting structures which is normally treated as a unit for handling and accountability purposes.

### **Non-Permanent Equipment**

The equipment (portable or mobile), provided with the aim of restoring safety functions that have been lost, but not to be the regular means to achieve these functions in accident conditions such as DBA and DEC.

### **Practically Eliminated Conditions**

Highly unlikely and physically impossible conditions eliminated by robust design and operational measures and demonstrated in the relevant DiD provisions, design practice following standards, material selection, and elimination or reduction of degradation mechanisms and their monitoring.

### **Prompt Power Coefficient of Reactivity**

The prompt reactivity change for 1 % increase in reactor power averaged over a given power range. (Only prompt feedback effects like fuel Doppler and axial fuel expansion considered).

### **Reactor Containment Building (RCB)**

The building, along with systems and components required for isolation that completely encloses the reactor, its primary coolant and cover gas system and serves to restrict the release of radioactivity to the environment within prescribed limits during all operational states and accident conditions.

### **Supplementary Control Room (SCR)**

A facility redundant to the main control room to ensure the availability of at least one among these two at all times, under all conditions of the plant.

### **Total Power Coefficient of Reactivity**

The reactivity change for 1 % increase in reactor power averaged over a given power range as measured in two steady state operations. This coefficient (sometimes referred to as power coefficient of reactivity for short) can be decomposed to its components arising from physical changes in fuel, clad, coolant and structure with power increase.

### **Total Temperature Coefficient of Reactivity**

The reactivity change for unit increase in reactor temperature. This coefficient (sometimes referred to as temperature coefficient of reactivity for short) can be decomposed to its components arising from temperature rises in fuel, clad and structure which are not uniform.



## Table of Contents

<b>FOREWORD .....</b>	<b>i</b>
<b>SPECIAL TERMS AND INTERPRETATIONS .....</b>	<b>v</b>
<b>1. INTRODUCTION .....</b>	<b>1</b>
1.1 General .....	1
1.2 Objective .....	1
1.3 Scope .....	1
<b>2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS.....</b>	<b>2</b>
2.1 General .....	2
2.2 Fundamental Safety Objective .....	2
2.3 Safety Principles .....	2
2.4 Safety Requirements.....	3
2.5 Radiation Protection .....	3
2.6 Safety in Design.....	3
2.7 Concept of Defence-in-Depth (DiD) .....	5
2.8 Maintaining the Integrity of Design of the Plant Throughout the Lifetime .....	7
2.9 Nuclear Security .....	8
2.10 Industrial Safety.....	8
<b>3. MANAGEMENT FOR SAFETY IN DESIGN .....</b>	<b>9</b>
3.1 General .....	9
3.2 Management for Safety in Design .....	9
3.3 Management System for Plant Design .....	9
3.4 Safety of the Plant Design throughout the Lifetime of the Plant .....	10
3.5 Safety Assessment and Independent Verification .....	11
<b>4. PRINCIPAL TECHNICAL REQUIREMENTS .....</b>	<b>13</b>
4.1 Fundamental Safety Functions .....	13
4.2 Design of Nuclear Power Plant .....	13
4.3 Application of Defence-in-Depth (DiD) .....	14
4.4 Design Approaches .....	15
4.5 Dose Criteria .....	16
4.6 Interfaces of Safety with Security .....	17
4.7 Proven Engineering Practices .....	17
4.8 Safety Assessment.....	18
4.9 Provision for Construction .....	18
4.10 Features to Facilitate Radioactive Waste Management and Decommissioning .....	18
<b>5. GENERAL PLANT DESIGN.....</b>	<b>19</b>
<b>5A DESIGN BASIS FOR THE PLANT.....</b>	<b>19</b>
5.1 General Design Basis.....	19
5.2 Design Basis for Items Important to Safety.....	19

5.3	Design Limits .....	20
5.4	Safety Classification and Seismic Categorization .....	20
5.5	Reliability of Items Important to Safety .....	21
5.6	Common Cause Failures (CCFs) .....	22
5.7	Independence of Safety Systems .....	23
5.8	Single Failure Criterion (SFC) .....	23
5.9	Fail-Safe Design .....	23
5.10	Support Service Systems.....	24
5.11	Equipment Outages .....	24
5.12	Materials, Coolant and Other Process Fluids Chemistry .....	25
5.13	Operational Limits and Conditions for Safe Operation .....	25
5.14	Postulated Initiating Events (PIEs) .....	26
5.15	Internal and External Hazards .....	27
5.16	Engineering Design .....	30
5.17	Design Extension Conditions (DECs) .....	31
5.18	Combinations of Events and Failures.....	33
5.19	Reactor Safe States.....	33
5B	DESIGN FOR SAFE OPERATION OVER THE LIFE TIME OF THE PLANT.....	34
5.20	Provision for Testing, Calibration, Maintenance, Inspection and Monitoring of Items Important to Safety .....	34
5.21	Ageing Management .....	35
5.22	Qualification of Items Important to Safety.....	35
5C.	HUMAN FACTORS .....	36
5.23	Design for Optimal Operator Performance .....	36
5D.	OTHER DESIGN CONSIDERATIONS .....	38
5.24	Systems Performing Both Safety and Process Functions .....	38
5.25	Sharing of Safety Systems between Multiple Units of a Nuclear Power Plant .....	39
5.26	Primary Coolant Boundary and Systems Containing Fissile Material or Radioactive Material	39
5.27	Prevention of Harmful Interactions of Systems Important to Safety .....	39
5.28	Interactions between the Electrical Power Grid and the Plant.....	40
5.29	General Considerations for Instrumentation and Control System.....	40
5.30	Use of Non-programmable digital systems or Computer-based Systems and Equipment .....	40
5.31	Design of Civil Structures .....	41
5E.	LAYOUT OF THE PLANT .....	41
5.32	Control of Access to the Plant and Systems .....	42
5.33	Escape Routes from the Plant .....	42
5.34	Communication Systems at the Plant .....	42
5F.	COMMISSIONING AND DECOMMISSIONING .....	43
5.35	Commissioning of the Plant.....	43

5.36 Decommissioning of the Plant .....	43
5G. SAFETY ANALYSIS .....	44
5.37 Safety Analysis of the Plant Design .....	44
5.38 Deterministic Approach .....	44
5.39 Source Term Evaluation.....	45
5.40 Probabilistic Approach .....	46
6. DESIGN OF SPECIFIC PLANT SYSTEMS .....	48
6A. REACTOR CORE AND REACTIVITY CONTROL .....	48
6.1 Reactor Core and Associated Systems .....	48
6.2 Performance of Fuel Elements and Assemblies .....	48
6.3 Structural Capability of the Reactor Core .....	50
6.4 Control of the Reactor Core.....	50
6.5 Reactor Assembly .....	51
6.6 Reactor Shutdown Systems .....	52
6B. REACTOR COOLANT SYSTEMS .....	54
6.7 Design of Reactor Coolant System .....	54
6.8 In-Service Inspection (ISI) of Reactor Coolant Boundary .....	56
6.9 Purification of Reactor Coolant.....	56
6.10 Heat Transport Systems .....	57
6.11 Decay Heat Removal Systems .....	58
6.12 Sodium Heating Systems .....	59
6.13 Sodium-Water Reactions.....	59
6C. CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM.....	59
6.14 Containment System.....	59
6.15 Containment Structure .....	60
6.16 Control of Radioactive Releases from the Containment.....	61
6.17 Isolation of the Containment.....	61
6.18 Access to the Containment .....	63
6.19 Control of Containment Conditions .....	63
6.20 Containment Heat Removal.....	63
6D. INSTRUMENTATION AND CONTROL SYSTEMS.....	64
6.21 Provision of Instrumentation.....	64
6.22 Reliability and Testability of Instrumentation and Control Systems .....	65
6.23 Separation of Protection Systems and Control Systems .....	66
6.24 Use of non-programmable digital systems or computer based systems or programmable equipment Important to Safety .....	66
6.25 Main Control Room (MCR) .....	67
6.26 Supplementary Control Room (SCR).....	68
6.27 Onsite Emergency Support Centre (OESC) .....	68
6.28 Severe Accident Monitoring .....	69

6E. ELECTRICAL POWER SUPPLY SYSTEM.....	69
6.29 General Requirements .....	69
6.30 Off-Site Power System .....	69
6.31 On-Site Power System .....	70
6.32 Emergency Power Supply .....	70
6.33 Station Blackout (SBO) .....	71
6F. SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS .....	72
6.34 Performance of Supporting Systems and Auxiliary Systems .....	72
6.35 Process Water Cooling System .....	72
6.36 Process Sampling Systems and Post-Accident Sampling Systems .....	72
6.37 Compressed Air Systems .....	73
6.38 Air Conditioning and Ventilation Systems.....	73
6.39 Fire Protection Systems (FPS) .....	73
6.40 Fire Protection for Sodium (Na).....	74
6.41 Lighting Systems .....	75
6.42 Overhead Lifting Equipment .....	75
6G. COMPONENT HANDLING AND STORAGE SYSTEMS .....	75
6.43 Component Handling and Storage Systems .....	75
6H. TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE .....	78
6.44 Systems for Treatment and Control of Waste .....	78
6.45 Systems for Treatment and Control of Effluents.....	79
6I. OTHER POWER CONVERSION SYSTEMS.....	79
6.46 Steam Supply System, Feed Water System and Turbine Generators .....	79
6J. RADIATION PROTECTION.....	80
6.47 Design for Radiation Protection .....	80
6.48 Radiation Monitoring .....	81
6K. ACCIDENT RESPONSE CAPABILITY FOR UNEXPECTED COMBINATION OF EVENTS	
82	
6.49 Diverse and Flexible Accident Response Capability .....	82
6.50 Use of Non-Permanent Equipment .....	82
6.51 Ultimate Heat Sink (UHS) Pathways .....	82
6L. INDICATIVE LIST OF SAFETY ENHANCEMENT IN SFR BASED NPPS .....	83
<b>ABBREVIATIONS</b> .....	84
<b>REFERENCES</b> .....	86
<b>BIBLIOGRAPHY</b> .....	87
<b>IN-HOUSE WORKING GROUP (IHWG)</b> .....	88
<b>TASK FORCE</b> .....	89
<b>ADVISORY COMMITTEE ON NUCLEAR AND RADIATION SAFETY (ACNRS)</b> .....	90

# **1. INTRODUCTION**

## **1.1 General**

- 1.1.1 This Safety Code specifies the requirements for the design of sodium cooled fast reactor based Nuclear Power Plants (NPP) and is intended to ensure “the highest level of safety that can reasonably be achieved” for the protection of people and the environment from harmful effects of ionizing radiation arising from NPP. It is recognized 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:
- (a) Design requirements for the Structures, Systems and Components (SSCs) of a Sodium Cooled Fast Reactor (SFR) based NPP for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, if they do occur, and
  - (b) Organizational processes important to safety, that are required to be met.
- 1.2.2 This Safety Code is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning of NPPs; in safety analysis, verification and review; in the provision of technical support; as well as by regulatory body.

## **1.3 Scope**

- 1.3.1 The Safety Code establishes requirements for land based stationary pool type Sodium Cooled Fast Reactor (SFR) based NPPs. The requirements specified, with judgement, can also be applied to Liquid Metal/Alloy Cooled Fast Reactor based NPPs with evolutionary or novel features with due consideration for safety implications associated with such new features. However, this Safety Code has to be seen in conjunction with other safety requirements by AERB.
- 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 NPP.
- 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 Terms and Interpretations).

## **2. APPLYING THE SAFETY PRINCIPLES AND CONCEPTS**

### **2.1 General**

This Safety Code specifies safety requirements that must be met to ensure the protection of people and the environment. These requirements are established based on the ‘Safety Fundamentals’ as enunciated in the IAEA document [1], which defines the ‘Fundamental Safety Objective’ and ‘Safety Principles’ of protection and safety of people and the environment as brought out below.

### **2.2 Fundamental Safety Objective**

Protection of people and the environment from harmful effects of ionizing radiation is the fundamental safety objective from which the safety principles and requirements for minimising the risks associated with NPPs are derived. The fundamental safety objective applies to all stages in the lifetime of an NPP, including planning, siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste.

### **2.3 Safety Principles**

- 2.3.1 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 brought out in the IAEA SF-1 [1], 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 Safety Code are derived from the following safety principles<sup>1</sup> [1]:

#### **Responsibility for Safety (Principle 1)**

The prime responsibility for safety must rest with the person or Organization 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.

#### **Optimization of Protection (Principle 5)**

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

#### **Limitation of Risks to Individuals (Principle 6)**

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

---

<sup>1</sup> 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 directly relevant to the subject of this Safety Code.



## **Protection of Present and Future Generations (Principle 7)**

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

## **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.

### **2.4 Safety Requirements**

Safety requirements which are particularly important in the design of NPPs 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

These are elaborated in Clauses 2.5 to 2.10 below

### **2.5 Radiation Protection**

- 2.5.1 In order to satisfy the safety principles, it is required to ensure that for all operational states of an NPP and for any associated activities, doses from exposure to radiation within the plant or exposure due to any planned radioactive release from the plant are kept below the 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.
- 2.5.2 To apply the safety principles, it is also required that NPPs 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 and the release of authorized amounts of radioactive substances to the environment from NPPs 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.

### **2.6 Safety in Design**

#### **2.6.1 General Design Objective**

To achieve the highest level of safety that can reasonably be achieved in the design of an NPP, 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 plant, any radiological consequences would be below the acceptable limits or other relevant regulatory criteria (refer 4.5.5 (c)) 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 DEC-B, only limited countermeasures are needed in area and time, in the public domain and sufficient time is available to implement these measures.
- (e) ensure integration of safety with security measures in design and in implementation.
- (f) limit sodium aerosol release within acceptable limits.

#### 2.6.2 *Radiation Protection Objective*

The design for safety of an NPP 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 due to an ‘early radioactive releases’<sup>2</sup> or a ‘large radioactive releases’<sup>3</sup> must be practically eliminated<sup>4</sup>; 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 2.7.2 (e) of this Safety Code]

#### 2.6.3 *Environmental Protection Objective*

The environmental protection objective is to provide all reasonably practical mitigation measures to protect the environment during the operation of an NPP and to mitigate the consequences of an accident.

The design shall include provisions to control, treat and monitor releases to the environment and shall minimize the generation of radioactive and hazardous wastes.

#### 2.6.4 *Safety Assessment*

- (a) To demonstrate that the fundamental safety objective is achieved in the design of

---

<sup>2</sup> An ‘early radioactive release’ in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time.

<sup>3</sup> A ‘large radioactive release’ is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

These ‘large’ and ‘early’ are defined w.r.t feasibility of implementation of the emergency countermeasures.

<sup>4</sup> 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.

an NPP, 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:

- i. all normal operation states,
- ii. anticipated operational occurrences (AOO),
- iii. design basis accidents (DBA), and
- iv. event sequences that may lead to Design Extension Conditions including Severe Accidents.

(b) The safety of the plant shall be assessed for:

- i. selected anticipated operational occurrences, and
- ii. accident conditions which could result due to:
  - a single Postulated Initiating Event (PIE) with consequential failures with superimposition of one failure of any of the active or passive elements of the safety systems, or one human error, in conformity with single failure criteria, which is independent of the initiating events;
  - an external or internal hazard (e.g. earthquake, flooding, fire) with consequential failures affecting one or several safety (or safety related) systems; and
  - accidents with credible multiple failures other than a postulated hazard, affecting similar equipment in the same safety (or safety related) system.

(c) On the basis of the safety analysis, the capability of the design to withstand PIEs 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 DEC's shall be envisaged and measures such as additional safety features and/or complementary safety features shall be introduced to ensure that the radiological consequences of an accident could be mitigated.

## **2.7 Concept of Defence-in-Depth (DiD)**

2.7.1 The primary means of preventing accidents in an NPP and mitigating the consequences of accidents if they do occur is the application of the concept of DiD. This concept is applied to all safety related activities, whether organizational, behavioral 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 DiD throughout design and operation provides protection against anticipated operational occurrences (AOOs) 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.

2.7.2 Application of the concept of DiD in the design of an NPP provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects of radiation on the 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 DiD 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 or reducing the effectiveness 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 accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction and in-service inspection, maintenance and testing, 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 PIEs are likely to occur over the operating lifetime of an NPP, 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 minimize 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 AOOs or postulated single initiating events including its consequential failures might not be controlled at a preceding level and that a DBA could develop. Event sequences pertaining to the third level of defence shall be categorised as Design Basis Accidents (DBA). 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 mitigate the consequences of accidents that result from failure of the third level of DiD or multiple failures, in which the design basis may be exceeded. The aim is to prevent the progression of such accidents and to mitigate the consequences of a severe accident. Event sequences pertaining to the fourth level of defence shall be categorised into two sub-categories as Design Extension Conditions (DEC) without core melt (DEC-A) and Design Extension Conditions with core melt (DEC-B) depending upon the consequences. Aim for the first kind of event sequences (i.e. DEC-A) is to limit the progression of accident and thereby avoid core melt (DEC-B). 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; (i) additional safety features for preventing extensive fuel damage or core melt at level DEC-A, and (ii) complementary safety features along with respective procedures for limiting the consequences of DEC-B. The targeted acceptable radiological consequences for these accident sequences are given in Clause 4.5 of this Safety Code.

Event sequences with radiological consequences potentially going beyond those specified for DEC-B, i.e. which can lead to large or early release are required to shall be ‘practically eliminated’.

- (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 center and Emergency Plans and emergency procedures for on-site and off-site emergency response.

- 2.7.3 A relevant aspect of the implementation of DiD is the provision in the design of a series of 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.

## **2.8 Maintaining the Integrity of Design of the Plant Throughout the Lifetime**

- 2.8.1 The design, construction and commissioning of an NPP might be shared between a number of organizations (including the research and design organizations): the architect/engineer, the designer/vendor of the reactor and its supporting systems, the Technical Support Organization (TSO) of vendor, the suppliers of major components, and the suppliers of other systems that are important to the safety of the plant.
- 2.8.2 The prime responsibility for safety rests with the Responsible Organization (RO) for operating the NPP that gives rise to radiation risks. The RO shall set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e. during the operating life and decommissioning). A formally designated entity i.e. Design Authority within the RO shall take responsibility for this process.
- 2.8.3 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.

- 2.8.4 The management system requirements that are placed on design authority shall also apply to all the entities 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 RO.

## **2.9 Nuclear Security**

- 2.9.1 The aim of the nuclear security is to minimize the risk of unauthorized removal of nuclear material and radioactive material, and to minimize sabotage on NPP. Detailed requirements are not within the scope of this Safety Code.

## **2.10 Industrial Safety**

- 2.10.1 Industrial safety is not explicitly considered in this code, however, Design shall take into account all relevant industrial safety requirements provided in Atomic Energy (Factories) Rules, 1996 and specified by AERB.
- 2.10.2 Safety measures and industrial safety measures in an NPP shall be designed and implemented in an integrated manner so that all requirements of safety are met without compromising industrial safety.

### **3. MANAGEMENT FOR SAFETY IN DESIGN**

#### **3.1 General**

Effective leadership<sup>5</sup> and management<sup>6</sup> for safety must be established and sustained in the Responsible Organization (RO). The requirements in this Safety Code integrate both leadership and management for ensuring safety in design of NPP.

#### **3.2 Management for Safety in Design**

- 3.2.1 An applicant for a license to construct and/or operate an NPP shall be responsible for ensuring that the design submitted to AERB meets safety objectives. As part of fulfilling this responsibility, the RO 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 RO 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 RO has overall responsibility for the design including the design changes effected throughout the life of the plant.
- 3.2.2 All organizations, including the Design Authority and related design organizations, engaged in activities important to the safety of the design of an NPP shall be responsible for ensuring that safety matters are given the highest priority.
- 3.2.3 Ownership of the safety case should reside with the RO 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.

#### **3.3 Management System for Plant Design**

- 3.3.1 The Design Authority within the RO 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 RO, 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 fulfill its role [2].

---

<sup>5</sup> ‘Leadership’ is the use of an individual’s capabilities and competences to give direction to individuals and groups and to influence their commitment to achieve the fundamental safety objective and apply the fundamental safety principles, by means of shared goals, values and behavior.

<sup>6</sup> ‘Management’ is a formal, authorized function for ensuring that an organization operates efficiently and that work is completed in accordance with requirements, plans and resources. Managers at all levels need to be leaders for safety.

- 3.3.2 The management system shall include provision for ensuring quality of the design of each structure, system and component, as well as of the overall design of the NPP, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.
- 3.3.3 The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled.

### **3.4 Safety of the Plant Design throughout the Lifetime of the Plant**

- 3.4.1 The Responsible Organisation (RO) 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 organization during the lifetime of the plant.
- 3.4.2 The Design Authority within the RO shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure that:
- (a) the plant design is fit for the purpose and meets the requirement for the optimization of protection and safety by keeping radiation dose and associated risks as low as reasonably achievable.
  - (b) the design verification, use of engineering codes, standards, requirements and proven engineering practices, provision for feedback of information on construction and operational experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design.
  - (c) the acceptance of new technology or systems is based on comprehensive test program, analysis, and/or operational experience with similar systems. Detailed reports containing substantiation for design, technology and functioning of systems shall be provided demonstrating reliable performance of such systems. Such systems, especially in the absence of operational experience, shall undergo extensive programme for performance testing during commissioning to the extent practicable.
  - (d) the aspects of design, having implications on operability, shall be reviewed. This should ensure the acceptance of the design by RO for ensuring proper operability, maintainability, layout, inspectability etc. in the designs.
  - (e) the knowledge of the design and the safety case that is needed for safe operation, maintenance (including appropriate intervals for testing) and modification of the



plant is available, that this knowledge is maintained up to date by the RO, and that due account is taken of past operating experience and validated research findings.

- (f) the management of design requirements and configuration control are maintained.
- (g) the necessary interfaces with original vendor designers and suppliers engaged in design work are established and controlled.
- (h) the necessary engineering expertise and scientific and technical knowledge are maintained within the RO.
- (i) all design changes to the plant are reviewed, verified, documented and approved.
- (j) adequate documentation is maintained to facilitate future decommissioning of the plant.

3.4.3 An indicative list of design capabilities required by the Design Authority within the RO 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, deterministic and probabilistic safety assessment, loads such as seismic loads, and interface requirements etc.
- (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 (structural integrity assessment, stress analysis, thermal hydraulic analysis, fracture mechanics, reactor core physics aspects including fuel management, and shielding, etc.) which demonstrates the adequacy of the design and the ability to reproduce the design calculation, if needed. Specific attention shall be paid to failure modes such as thermal striping, thermal stratification, cellular convection, fluid-elastic instability of thin shells with high added mass and others.
- (f) An understanding of the inspections, analysis, testing, computer code validation and acceptance criteria used by participating design organizations 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.

### **3.5 Safety Assessment and Independent Verification**

#### **3.5.1 *Safety Assessment***

- a) A comprehensive safety assessment shall be carried out throughout the design process to ensure that all relevant safety requirements are met by the design of the plant throughout all stages of the plant's life to confirm that the design meets requirements as delivered for fabrication, as for construction, as built, as operated and as modified.

- b) The safety assessment shall be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in the scope and level of detail as the design programme progresses.
- c) The basis for the safety assessment shall be derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice.

#### 3.5.2 *Independent Verification*

The adequacy of the plant design, including design tools and design inputs and outputs, shall be reviewed by individuals or groups separate from those who originally performed the design work. The computer codes used in the design shall be verified and validated. Verification and Validation of the computer codes and approval of the plant design shall be completed as soon as practicable in the design and construction processes.

#### 3.5.3 *Quality Assurance*

A quality assurance programme that describes the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented<sup>7</sup>. This programme shall be supported by more detailed plans for each system, structure and component so that the quality of the design is ensured at all times.

- 3.5.4 Necessary records of design, fabrication, inspection, erection, testing and maintenance of structures, systems and components shall be maintained throughout the life of the plant

---

<sup>7</sup> AERB Safety Code on Management System for Quality In Nuclear Facilities , AERB/NF/SC/MS-Q

## **4. PRINCIPAL TECHNICAL REQUIREMENTS**

### **4.1 Fundamental Safety Functions**

- 4.1.1 Fulfillment of the following fundamental safety functions for NPP 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.
- 4.1.2 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.
- 4.1.3 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 of Nuclear Power Plant**

- 4.2.1 The design of NPP 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 minimized.
- 4.2.2 The design of NPP shall be such as to ensure that the requirements of the RO, the safety requirements of AERB and the requirements of established relevant Acts, Rules, Safety Codes and Safety Standards, are all met, and that due account is taken of human capabilities and limitations and of factors that could influence human performance.
- 4.2.3 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).
- 4.2.4 The design shall take due account of relevant available experience that has been gained in the design, construction, commissioning, operation and decommissioning of other NPPs, and of the results of relevant research programmes.
- 4.2.5 The design shall take into account feasibility of construction, inspection and maintenance planned during lifetime of the plant.
- 4.2.6 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.
- 4.2.7 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 (DiD)**

- 4.3.1 The NPP shall be designed based on the concept of DiD. The levels of DiD shall be independent as far as practicable<sup>8</sup>.
- 4.3.2 The DiD concept shall be applied to provide several levels of defence that are aimed at preventing accidents that could lead to harmful effects on the public and the environment and ensuring that appropriate measures are taken for the protection of the people and the environment, and for the mitigation of consequences, in case prevention fails.

DiD 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.

DiD level four shall include consideration of design extension conditions (DEC). The DEC are accident conditions that are not considered for DBAs, but that are considered in the design process of the NPP in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DEC are classified into two sub-levels. At sub-level DEC-A, additional safety features prevent escalation to core melt conditions but if that also fails, at sub-level DEC-B, complementary safety features together with Accident Management Programmes are provided to limit the core melt and to limit external releases of radioactive materials. DEC-B includes Severe Accident conditions involving core melt. A clear distinction shall be introduced in level four between means and conditions for DEC-A and DEC-B.

The Severe Accident sequences which may lead to early or large radioactive releases shall be ‘practically eliminated’ by design.

The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases that could potentially result from accidents through on-site and off-site emergency response, which require adequately equipped emergency response facilities and preparedness with emergency plans and procedures.

- 4.3.3 The effective dose targets for various levels of events shall be as per Clause 4.5 of this Safety Code.

---

<sup>8</sup> Nevertheless, if a single safety system is envisaged to function under multiple levels of DiD, the equipment considered failed under particular mode/configuration of operation during the mitigation of a particular level of DiD (say DBA) shall not be credited as available under that same mode/configuration of operation for demonstrating the mitigating capability of the safety system in the next level of DiD (say DEC).

- 4.3.4 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 DiD shall be kept available at all times and any relaxation shall be justified for specific modes of operation and shall be only for limited duration.
- 4.3.5 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 NPP.

#### **4.4 Design Approaches**

- 4.4.1 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, application of single failure criteria, rigorous quality and qualification requirement for systems required to cater for addressing design basis events or accidents.
- 4.4.2 For DEC-A, additional safety features (other than those provided for DBA), if envisaged, should be diverse from the safety systems for DBAs.
- 4.4.3 In design of complementary safety features which are used to prevent or mitigate the consequences of DEC-B or Severe Accident situations that involve large or early releases, the design approach should be to prevent such sequences by significant margins.
- 4.4.4 Design shall also include provision to use non-permanent equipment to handle extreme events, along with unexpected failure of existing safety systems or features.
- 4.4.5 The design shall:
- (a) provide for multiple physical barriers to the release of radioactive material to the environment, adequate protection of these barriers, and assurance of their effectiveness by the use of passive or active features;
  - (b) 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;
  - (c) be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect<sup>9</sup>;
  - (d) provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;

---

<sup>9</sup>A cliff edge effect, in NPP, 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.

- (e) provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized;
  - (f) provide for SSCs 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;
- 4.4.6 The design should also consider the benefit of implementing passive safety features for both, shutdown and decay heat removal functions.
- 4.4.7 Complementary safety features for DEC-B shall be independent of safety systems/ additional safety features as far as practicable.
- 4.4.8 To ensure that the concept of DiD is maintained, the design shall prevent, as far as practicable:
- (a) challenges to the integrity of physical barriers;
  - (b) failure of one or more barriers;
  - (c) failure of a barrier as a consequence of the failure of another barrier, and
  - (d) the possibility of harmful consequences of errors in operation and maintenance.

## **4.5 Dose Criteria**

- 4.5.1 The design of NPP shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the prescribed dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable during, and following, accident conditions.
- 4.5.2 The design shall be such as to ensure that plant states that could lead to large or early radioactive releases, beyond those that could be mitigated by emergency countermeasures, 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 (see Clause 4.5.5).
- 4.5.3 For practical application, quantitative dose assessment shall be undertaken for the NPP designs to demonstrate that the design will meet the dose criteria 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)]' [3].
- 4.5.4 *Normal Operation*
- a) The annual release limits for all the facilities within a particular site (taken together) shall ensure that the effective dose limit for a representative person of the public at

off-site, due to normal operation (including anticipated operational occurrences) is less than the limit prescribed by AERB [3].

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

#### 4.5.5 *Accident Conditions*

- a) 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 DBA in NPP, there shall be no need for off-site countermeasures (i.e. no need for prophylaxis, food control, sheltering 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 DBA [3].

- b) DEC-A:

For accidents at level DEC-A, i.e. accidents without core melt within design extension conditions, 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.

- c) DEC-B:

In case of accidents at level DEC-B, i.e. Severe Accident with core melt, 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 NPP shall be designed and implemented in an integrated manner so that they do not compromise one another.

### 4.7 **Proven Engineering Practices**

- 4.7.1 Items important to safety for NPP shall be designed in accordance with the latest applicable codes and standards.
- 4.7.2 Items important to safety for NPP 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.
- 4.7.3 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.

- 4.7.4 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**

- 4.8.1 Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out as part of the design process for NPP 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.
- 4.8.2 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 program progresses.
- 4.8.3 The safety assessments shall be documented in a form that facilitates independent evaluation.

#### **4.9 Provision for Construction**

- 4.9.1 Items important to safety for NPP 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.
- 4.9.2 In the provision for construction, due account shall be taken of relevant experience that has been gained in the construction of other similar plants and their associated SSCs. 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**

- 4.10.1 Special consideration, especially for waste minimization and dose reduction shall be given at the design stage of NPP to the incorporation of features to facilitate radioactive waste management during operational life and the future decommissioning and dismantling of the plant [4].
- 4.10.2 In particular, the design shall take due account of:
- (a) the choice of materials, so that amount of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;
  - (b) the access capabilities and the means of handling that might be necessary;
  - (c) the facilities necessary for the 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 NPP 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 are kept below authorized limits on discharges in normal operation; and to ensure that plant states that could lead to high radiation doses due to early radioactive releases 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**

- 5.1.1 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 (NO), Anticipated Operational Occurrences (AOOs), Design Basis Accidents (DBAs) and Design Extension Conditions (DECs), including Severe Accidents.
- 5.1.2 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.
- 5.1.3 Conservative design measures shall be applied and sound engineering practices shall be adhered to in the design bases for normal operation, anticipated operational occurrences and design basis accidents so as to provide a high degree of assurance that no significant damage will occur to the reactor core and that radiation doses will remain within prescribed limits/acceptable limits for normal operation and accident conditions respectively and will be ALARA (As low as reasonably achievable).
- 5.1.4 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 DECs shall be identified and addressed in design. The practicable provisions for prevention of such accidents and mitigation of their consequences should also be addressed.

#### **5.2 Design Basis for Items Important to Safety**

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

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

5.2.3 Proven and conservative design measures with well-established engineering practices shall be adopted in safety system design for DBAs. Additional safety features for preventing and/or mitigating the consequences of DEC-A, shall be designed with proven engineering practice. Complementary safety features shall be provided, as practical, for mitigating the consequences of DEC-B.

### **5.3 Design Limits**

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

5.3.2 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 Categorization**

5.4.1 All SSCs, including software for instrumentation and control (I&C), that are important to safety, shall be identified and shall be classified on the basis of their function and their safety significance. The safety classification of all SSCs shall be aligned with the approach specified by AERB.

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

- (a) 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.

5.4.3 Items important to safety shall be designed, constructed and maintained such that their quality and reliability are commensurate with their classification. The applicable codes and standards for design, manufacture, construction, inspection, testing and in-service inspection of all these SSCs shall be used.

- 5.4.4 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. If a fluid system is interconnected with another fluid system that operates at a higher pressure, then it shall be designed to withstand the higher pressure, or provisions shall be made to prevent the design pressure of the system operating at the lower design pressure from being exceeded, considering a single failure.
- 5.4.5 Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment.
- 5.4.6 The seismic categorization of all components shall be aligned with the requirements as specified by AERB or equivalent standards. Seismic fragility levels should be evaluated for component(s) important to safety by analysis or, where possible, by testing or by experience/comparisons.

## **5.5 Reliability of Items Important to Safety**

- 5.5.1 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.
- 5.5.2 In the selection of equipment, consideration shall be given to avoid 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.
- 5.5.3 The safety systems and their support systems shall be designed to ensure that the targeted probability of a safety system failure on demand from all possible causes to be lower than  $10^{-3}$  subject to meeting the overall probability targets given in clause 5.41.3 of this Safety Code. 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.
- 5.5.4 To the extent possible, the design shall have provisions for testing to demonstrate that these reliability requirements will be met during operation.

## **5.6 Common Cause Failures (CCFs)**

- 5.6.1 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 required reliability.
- 5.6.2 Common 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. CCFs may simultaneously affect a number of items important to safety and failure of common support systems.
- 5.6.3 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 and appropriately addressed.
- 5.6.4 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 location so as to minimize the vulnerability to common cause failures;
  - (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.
- 5.6.5 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;
  - (d) Oil storage and pipelines supplying oil to the safety equipment, and
  - (e) Interacting fluid chemistry.
- 5.6.6 Diversity shall be applied to additional safety feature 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.

- 5.6.7 Diversity shall be applied to Ultimate Heat Sink (UHS) as practicable considering external events having impact on UHS leading to common mode failure of redundant safety systems connected to UHS.
- 5.6.8 The design shall provide for protection against CCFs in computer based systems or programmable equipment, including Software used in safety systems (refer 6.24.2 (d) of this safety code).

## **5.7 Independence of Safety Systems**

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

- 5.8.1 The single failure criterion<sup>10</sup> 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 plant states within design basis are not exceeded. In addition, some individual systems may require to meet SFC.
- 5.8.2 Human error and spurious action shall be considered to be one mode of failure when applying the SFC concept to a safety group or safety system.
- 5.8.3 The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the PIE. Credible passive system failure shall be considered unless justified by other means such as periodic surveillance, replacement etc.
- 5.8.4 SFC need not be applied for system required for mitigating very low probability event, such as external event of low probability. Likewise, SFC need not be applied for safety feature provided for mitigating DEC-A & DEC-B. However, consideration shall be given to redundancies that can participate in meeting quantitative safety targets, especially in features provided in design for preserving integrity of containment in case of severe accident condition.

## **5.9 Fail-Safe Design**

- 5.9.1 The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.
- 5.9.2 Systems and components important to safety shall be designed for fail-safe behavior, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function.

---

<sup>10</sup> 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.

- 5.9.3 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.

## **5.10 Support Service Systems**

- 5.10.1 Safety support systems necessary to maintain a safe state of the plant include electricity, cooling water, compressed air, cover gas such as argon, insulating gas such as nitrogen 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 appropriately to meet the safety function.
- 5.10.2 The reliability, redundancy, diversity and independence of support service systems and the provision of features for their isolation and for testing their functional capability shall commensurate with the significance to safety of the system being supported.
- 5.10.3 It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions, and compromising the capability of these systems to fulfill their safety functions.
- 5.10.4 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 provide the service.
- 5.10.5 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 analyzed and defined for each configuration of the plant (depending on the outages of SSCs) before the start of plant operation and included in the plant operating documents.

## **5.12 Materials, Coolant and Other Process Fluids Chemistry**

5.12.1 To ensure satisfactory performance during normal operation and accident conditions, 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,
- (h) hydrogen pick-up, and
- (i) interacting fluid chemistry.

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

5.12.2 Design organization should prescribe the range of permissible coolant/cover gas/insulation gas/ chemistry parameters for primary/secondary/tertiary systems to avoid various degradation mechanisms such as, corrosion/oxidation, stress corrosion cracking and flow accelerated corrosion.

## **5.13 Operational Limits and Conditions for Safe Operation**

5.13.1 The design shall establish a set of operational limits and conditions for safe operation of the NPP.

5.13.2 The requirements and operational limits and conditions established in the design for the NPP shall include:

- (a) Safety Limits (SL),
- (b) Limiting Safety Systems Settings (LSSS),
- (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 SSCs 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, and
- (g) action statements, including completion times for actions in response to deviations from the operational limits and conditions.

5.13.3 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.

5.13.4 These requirements and limitations shall be a basis for the establishment of operational limits and conditions under which the RO will be authorized to operate the plant.

#### **5.14 Postulated Initiating Events (PIEs)**

5.14.1 The design of the NPP shall apply a systematic approach to identify a comprehensive set of Postulated Initiating Events (PIEs) 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 DEC.

5.14.2 The PIEs shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment including past operating experiences. A justification shall be provided, to show that all foreseeable events have been considered.

5.14.3 The PIEs shall include all foreseeable failures of SSCs of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether at full power, low power, refuelling or shutdown states.

5.14.4 An analysis of the PIEs 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.

5.14.5 The expected behaviour of the plant in any PIE shall be such that the following conditions can be achieved, in the order of priority:

- (a) A PIE 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 PIE, 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 PIE.
- (c) Following a PIE, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the PIE.
- (d) Following a PIE, the plant would be rendered safe by following specified procedures.

5.14.6 In case plant state reaches DEC (Multiple failure), safety would be achieved by actuation of additional safety features or by complementary safety features following specified procedures (Refer clause 5.18.3 of this Safety Code).

5.14.7 The PIEs 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.

- 5.14.8 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 PIEs.
- 5.14.9 Where prompt and reliable action would be necessary in response to a PIE, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems or additional safety features, to prevent progression to more severe plant conditions.
- 5.14.10 Where prompt action in response to a PIE would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems, or on other operator actions (Refer Clauses 5.24.11, 5.24.12 and 5.24.13 of this Safety Code). For such cases, 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.
- 5.14.11 The operator actions that would be necessary to diagnose the state of the plant following a PIE and to put it into a safe 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 and include 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.
- 5.14.12 Any equipment that is necessary for actions to be taken in manual response and recovery processes shall be placed at the most suitable location to ensure its availability at the time of need and to allow safe access 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 NPP directly or indirectly, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determination of the PIEs 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 including sodium 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. Sodium chemical reaction with air, water, concrete and other fluids, and associated products release shall be taken into account in the design of the plant. 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) SSCs important to safety shall be designed and located in a manner that minimizes 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, tsunamis, 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, asphyxiant and toxic gases, corrosive and radioactive gases & liquids, electromagnetic interference, explosions and nearby hazardous industries. Loss of UHS from conditions arising out of external hazards shall also be addressed. SSCs necessary to assure the capability for shutdown, residual heat removal and confinement of radioactive material shall be designed to remain functional in the event of natural and human induced external events.
- (b) The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the Site, and to avoid cliff edge effects. The design of the plant shall also provide for an adequate margin to protect items necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the Site. Such assessment of margins should include possible secondary effects due to the primary hazard.

The SSCs of NPP identified to meet basic safety functions, (i.e., immediate and long term (guaranteed) shutdown, decay heat removal from core and spent fuel, and containment) as well as SSCs identified for post-accident management shall remain functional under extreme external events.

- (c) The possibility of incorporating suitable design features including layout of buildings & equipment which would provide additional defence against aircraft crash should be investigated. Otherwise, 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 of 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;
  - ii. spent fuel cooling or spent fuel pool integrity is maintained.
- (d) The design shall include due consideration of extreme external hazards and their consequences, such as long term loss of all AC power supplies and plant instrumentation.
- (e) 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.
- (f) Flood protection of safety-related rooms shall follow the logic of defence -in-depth. The design shall avoid penetrations/doors to structures housing safety related equipment below the flood level. Penetrations and the doors built under the postulated flood level of safety related buildings shall be watertight.
- (g) 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.
- (h) Design shall consider the possibility of 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 and ensure that it does not lead to any unsafe condition.
- (i) 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.
- (j) For multiple unit plant sites, the design shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several/all units on the Site.

#### 5.15.3 *Applicability of Leak before Break (LBB)*

- (a) Wherever credit for Leak Before Break (LBB) is taken in the design, analysis shall be done to establish that leakage, if any, shall be detected by leak detection systems, and the predicted crack size has adequate margin to the critical crack size.
- (b) Analyses should demonstrate that the rupture is highly unlikely under conditions consistent with the design basis for the vessel/piping. Towards this, a deterministic evaluation of the vessel/piping system that demonstrates sufficient margins against failure, including verified design and fabrication, and an adequate In-Service Inspection (ISI) program shall be carried out.

#### 5.15.4 *Fire Safety*

- (a) SSCs important to safety shall be designed and located, consistent with other safety requirements, so as to minimize the likelihood and effects of internal fires and explosions caused by external or internal events. Special attention shall be paid to issues associated with sodium fire.
- (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, and
  - iii. Preventing the spread of those fires which have not been extinguished, thus minimizing their effect on essential plant functions.
- (c) The first objective requires that the design and operation of the plant be such that the probability of a fire starting is minimized. 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.
- (d) 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 (FHA) of the plant shall be carried out to determine the required rating of the fire barriers, and the required capability of fire detection and firefighting systems shall be provided.
- (e) Firefighting 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 SSCs important to safety, and does not simultaneously affect redundant safety chains, thereby challenging compliance with the single failure criterion.
- (f) 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**

5.16.1 The engineering design rules for SSCs important to safety at NPP 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.

5.16.2 Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of NPP.

### **5.16.3 Design Basis Accidents (DBAs)**

5.16.4 A set of accident conditions that are to be considered in the design shall be derived from PIEs for the purpose of establishing the bounding conditions for the NPP to withstand, without exceeding the acceptable limits of radiation protection.

- 5.16.5 DBAs 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.
- 5.16.6 The design shall be such that for DBAs, key plant parameters do not exceed the applicable design limits. A primary objective shall be to manage all DBAs so that they have no, or only minor, radiological impacts, on or off the site, and are within acceptable limits, and do not necessitate any off-site countermeasures.
- 5.16.7 The DBAs shall be analyzed 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.

## **5.17 Design Extension Conditions (DECs)**

- 5.17.1 A set of DECs shall be derived on the basis of engineering judgment, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the NPP, by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than DBAs or that involve additional failures. These DECs 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.
- 5.17.2 The NPP design shall identify credible DECs, based on operational experience, engineering judgment, and the results of analysis and research. The DECs 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.
- 5.17.3 An analysis of DECs for the plant, including assessment of radiological impact, shall be performed. The main technical objective of considering the DECs is to provide assurance that the design of the plant is such as to prevent accident conditions not considered as DBA conditions, or to mitigate their consequences, to the extent practicable. This might require additional safety features and complementary safety features for DECs or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for DECs, 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 an appropriate state (refer Clause 5.20 of this Safety Code) and the containment function can be maintained, with the result that significant radioactive releases, beyond those that could be mitigated by emergency countermeasures, would be practically eliminated. The effectiveness of provisions to

ensure the functionality of the containment shall be analyzed on the basis of the best estimate approach.

- 5.17.4 The DEC's shall be used to define the design specifications for additional safety 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.
- 5.17.5 The analysis undertaken shall include identification of the systems/features that are designed for use in, or that are capable of preventing or mitigating, events considered in the DEC's. 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 DEC's, including severe accidents, where appropriate; and
  - (c) have reliability commensurate with the function that they are required to fulfill.
- 5.17.6 If the plant state is within DEC-A, it shall be brought to and maintained under safe state within 72 hours. Subsequently, it is desirable to reach and maintain the safe shutdown state (refer Clause 5.20). In the DEC-B, 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.
- 5.17.7 To the extent practicable, the design shall provide biological shielding of appropriate composition and thickness to protect operational personnel during DEC's, including severe accidents.
- 5.17.8 In case of multi-unit plant Site, 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.
- 5.17.9 The design shall take into account the availability of off-site services only in the long term [refer Clause 5.15.2 (e) of this Safety Code].
- 5.17.10 The design shall be such that event sequences with DEC-B that could lead to large or early releases of radioactivity are practically eliminated. For DEC's 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.

5.17.11 In addition to above, design shall also include provision to use non-permanent equipment to handle extreme events, along with unexpected failure of existing safety systems or features.

## **5.18 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 (AOOs) or to accident conditions, such combinations of events shall be considered to be DBAs or shall be included as part of DECAs, 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 PIE.

## **5.19 Reactor Safe States**

5.19.1 Design shall ensure that following AOOs or accident conditions, the fundamental safety functions are ensured and the reactor is maintained at safe states.

### **5.19.2 *Controlled State***

This is a state of the plant, following an AOO or accident condition (DBA or DEC-A), 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 characterized by:

- (a) core is subcritical;
- (b) core heat is adequately removed;
- (c) radioactive discharges are within acceptable limits.

In case of a DBA or DEC-A, it is mandatory to reach the safe shutdown state following a controlled state. During an accident (DBA), controlled state shall not be continued for more than 24 hours.

### **5.19.3 *Safe Shutdown State***

Safe shutdown state is a state of the plant, following an AOO or DBA, in which the fundamental safety functions can be ensured and maintained continuously. This state is characterized by:

- (a) reactor is under shutdown with desired margin (1\$);
- (b) continuous decay heat removal up to UHS through designed cooling chain; and
- (c) availability of containment safety functions.

During a DBA, it is mandatory to reach the safe shutdown state following a controlled state.

### **5.19.4 *Safe State***

State of plant, following DEC-A, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time. This state is characterized by:

- (a) core is in long term subcritical state;
- (b) long term decay heat removal is established; and
- (c) containment functions are available and radioactive discharges are in accordance with the acceptable limits.

Design provisions shall be made to achieve and maintain safe state within 72 hours from the initiation of accident (DEC-A). Subsequently, it is desirable to reach safe shutdown state.

#### 5.19.5 *Severe Accident Safe State*

Severe accident safe state is a state which shall be achieved subsequent to a DEC-B 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 is 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
- (f) containment integrity is maintained.

As the plant is in DEC-B (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 LIFE TIME OF THE PLANT**

#### **5.20 Provision for Testing, Calibration, Maintenance, Inspection and Monitoring of Items Important to Safety**

- 5.20.1 Items important to safety for NPP shall be designed to facilitate testing, calibration, maintenance, inspection and monitoring as required to ensure their capability of performing their functions, and to maintain their integrity in all conditions specified in their design basis.
- 5.20.2 The plant layout shall be such that activities for calibration, testing, maintenance, 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 to radiation and harsh environment.
- 5.20.3 Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. 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. For items important to safety, full scale testing shall be demonstrated during commissioning, wherever feasible.

5.20.4 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.

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

5.20.6 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.

## **5.21 Ageing Management**

5.21.1 The design life of items important to safety at NPP shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, such as high temperature, use of sodium coolant, fast neutron irradiation, 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.

5.21.2 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, and in plant states during and following a PIE.

5.21.3 Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help identify unanticipated behavior 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.

5.21.4 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.

## **5.22 Qualification of Items Important to Safety**

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

- 5.22.2 The qualification program for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, electromagnetic interference, lightning, irradiation, humidity, corrosive environment or temperature) over the expected service life of the items important to safety.
- 5.22.3 When the items important to safety are subject to sudden changes<sup>11</sup> in the environment due to internal or external events and are required to perform a safety function during or following such an event, the qualification program shall replicate, in an accelerated manner, as far as practicable the conditions imposed on the items important to safety prior to the event as well as by the event, either by test or by analysis or by a combination of both.
- 5.22.4 Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states including during testing, such as in periodic testing of the containment, shall be included in the qualification programme.
- 5.22.5 Equipment that is credited to operate (e.g. certain instrumentation) during DEC 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**

### **5.23 Design for Optimal Operator Performance**

- 5.23.1 Systematic consideration of human factors, including the human-machine interface shall be included at an early stage in the design process for NPP and shall be continued throughout the entire design process [5].
- 5.23.2 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 operator 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, in all plant states.
- 5.23.3 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.
- 5.23.4 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

---

<sup>11</sup> Regardless of the redundancy used in the equipment designed to perform a safety function, environmentally induced common cause damage to the redundant systems is a matter of concern. A sudden change of environment could lead to loss of safety function due to simultaneous failure of all the redundant equipment/components. Examples of hazardous environmental conditions which could cause such failures are temperature, pressure, radiation field, sodium aerosols and earthquake.

organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment.

5.23.5 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.

5.23.6 The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the Main Control Room (MCR) or the Supplementary Control Room (SCR) and in locations on the access route to the SCR do not compromise the protection and safety of the operating/emergency handling personnel.

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

5.23.8 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.

5.23.9 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 30 minutes of any incident.

5.23.10 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.

5.23.11 Automated response shall continue for at least a reasonable pre-determined time dependent on prior assessment (Refer Clause 5.14.9). However, operator actions to enhance safety within such time can be allowed, if design envisages.

5.23.12 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 time available for operator actions should be considered from the first clear and unambiguous indication of the necessity for operator actions. The design shall take into account the following:

- (a) Credit for operator action shall not be considered earlier than 20 min. (if actions are taken from control room).
- (b) Credit for operator action shall not be considered earlier than 30 min. (if actions are taken from the field).

5.23.13 The credit for such operator intervention 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 MCR or in the SCR/backup control points, and
- (d) access route to that SCR/backup control points, is available.

5.23.14 In certain circumstances, which must be justified, an operator action shorter than 20 minutes for control room action might be assumed, provided that:

- (a) the operator is exclusively focused on the action in question;
- (b) the required action is unique, and does not involve choice from several options;
- (c) the required action is simple and does not involve multiple manipulations.

5.23.15 The design for NPP 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**

### **5.24 Systems Performing Both Safety and Process Functions**

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

5.24.2 If the design includes sharing of instrumentation between a safety system and a safety related 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 safety related system, 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. However, if failure of such device is cause for a PIE, the mitigating system for that PIE should not depend on the same device.
- (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.

## **5.25 Sharing of Safety Systems between Multiple Units of a Nuclear Power Plant**

- 5.25.1 Safety systems and additional safety features, required for DBAs and DEC-A 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 DEC-B scenario, shall be such that simultaneous handling of such events at all the reactors at a multi-unit plants site is possible.
- 5.25.2 Safety system support features and safety related items shall be permitted to be shared and interconnected between several units of NPP, 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.

## **5.26 Primary Coolant Boundary and Systems Containing Fissile Material or Radioactive Material**

- 5.26.1 All primary coolant boundary shall be protected against overpressure/negative pressure conditions, and shall be classified, designed, fabricated, erected, inspected, and tested in accordance with established standards. All other interfacing system, failure in which may lead to radioactivity release also need to be designed in accordance with established standards.
- 5.26.2 All primary coolant boundary 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 DEC-A scenario
- 5.26.3 All primary coolant boundary components whose failure may affect nuclear safety shall be designed to permit inspection/monitoring of their pressure boundaries throughout the design life of NPP.

## **5.27 Prevention of Harmful Interactions of Systems Important to Safety**

- 5.27.1 The potential for harmful interactions of systems important to safety at the NPP that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.
- 5.27.2 In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, 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.
- 5.27.3 If two fluid systems important to safety are interconnected and are operating at different pressures, either both the systems shall 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.

## **5.28 Interactions between the Electrical Power Grid and the Plant**

- 5.28.1 The functionality of items important to safety at the NPP shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply as well as single phase open conditions.
- 5.28.2 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, if applicable, as defined for that grid shall be followed. Design of SSCs important to safety including fuel shall take into account the transients originating from such operation.

## **5.29 General Considerations for Instrumentation and Control System**

- 5.29.1 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 NPP, 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.
- 5.29.2 Interference between protection systems and control systems shall be prevented by means of separation, by avoiding interconnection or by suitable functional independence.
- 5.29.3 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, and
  - (c) facilitating decisions in accident management.

## **5.30 Use of Non-programmable digital systems or Computer-based Systems and Equipment**

- 5.30.1 If non-programmable digital systems or computer based systems and equipment are used for safety purpose, correct (with respect to specification), safe and complete implementation of the requirements shall be ensured. Software in computer based systems and equipment 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.
- 5.30.2 Integrity should be assured by developing non-programmable digital systems or computer based systems and equipment /software (for computer based systems and equipment) using systematic, technically appropriate, carefully controlled, fully documented and reviewable engineering process which is suitably interfaced with verification and validation activities.
- 5.30.3 The safety case in support of the non-programmable digital systems or computer based systems and equipment and in particular software safety and integrity for computer based systems and equipment shall be based on design and design documents produced

during the system development, result of analysis of specifications, algorithms and implementation.

- 5.30.4 Non-programmable digital systems or computer based systems and equipment shall be designed to have the fault tolerance commensurate with the safety category of the system. It shall have self- diagnostic features. It shall have maintainability features. Security features (with administrative control) for access to computer system shall be provided.

### **5.31 Design of Civil Structures**

- 5.31.1 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, AOOs, DBA, and DEC including severe accident conditions, as well as from external hazards and their credible combinations with plant states.
- 5.31.2 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 minimize 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.
- 5.31.3 The SSCs of NPP identified to meet basic safety functions, (i.e., immediate and long term (guaranteed) shutdown, decay heat removal from core and spent fuel, and containment) as well as SSCs identified for post-accident management shall remain functional under extreme external events.
- 5.31.4 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.
- 5.31.5 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.
- 5.31.6 The design shall include provision for recording response of reactor containment building and another typical safety related structure in the event of an earthquake for post-earthquake analysis.
- 5.31.7 The design shall ensure that no substantive damage to higher seismic category SSC will be caused by the failure of any other SSC of lower seismic category.

### **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, spatial interaction with other safety and non-safety related structures, etc. Consideration shall also be given to externally and internally generated missiles (turbine missile), 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.

### **5.32 Control of Access to the Plant and Systems**

- 5.32.1 The NPP shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.
- 5.32.2 Provision shall be made in the design of the buildings and the layout of the Site for the control of access to the NPP by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.
- 5.32.3 Prevention of unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be ensured. Where access is necessary for maintenance, testing or inspection purposes, it shall be ensured in the design that the necessary activities can be performed without significantly reducing the reliability of safety related equipment.

### **5.33 Escape Routes from the Plant**

- 5.33.1 NPP 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.
- 5.33.2 Escape routes from the NPP shall meet the requirements for radiation zoning and fire protection, and the relevant AERB requirements for industrial safety and plant security and emergency handling (including off-site).
- 5.33.3 At least one escape route shall be available from workplaces and other occupied areas following an internal event or an external event or following combinations of events considered in the design.

### **5.34 Communication Systems at the Plant**

- 5.34.1 Effective means of communication shall be provided throughout the NPP to facilitate safe operation in all modes of normal operation and to be available for use following all PIEs and in accident conditions.



5.34.2 Suitable alarm systems and means of communication shall be provided so that all persons present at the NPP and on the Site can be given warnings and instructions, in operational states and in accident conditions.

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

## **5F. COMMISSIONING AND DECOMMISSIONING**

### **5.35 Commissioning of the Plant**

5.35.1 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. Such testing, if it is not possible to be carried out in the reactor, should be carried out in test facilities, to the extent practicable, towards verification of the system simulating the system characteristics and configuration, as applicable to the various systems. The design should also consider the need for related testing when specifying the commissioning requirements for the plant. The testing requirements shall consider and include the experiences gained from previous plants of similar kind. Design shall provide provisions for commissioning of systems/equipment as per their requirements. The design should also consider the need for related testing when specifying the commissioning requirements for the plant.

5.35.2 Design authority should be continuously involved during commissioning to verify and certify that SSCs perform as per design intent.

### **5.36 Decommissioning of the Plant**

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

5.36.2 The design should consider that exposures of personnel and the public during decommissioning are maintainable within the limits prescribed by Regulatory Body 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 minimized and effective decontamination is facilitated,
- (b) the layout and access capabilities that may be required for facilitation of decommissioning, and,
- (c) the facilities necessary for storing radioactive waste generated during operation and provision for managing the radioactive waste generated during decommissioning of the plant

## **5G. SAFETY ANALYSIS**

### **5.37 Safety Analysis of the Plant Design**

- 5.37.1 A safety analysis of the design for the NPP shall be conducted in which both methods deterministic and probabilistic safety analysis shall be applied to enable the challenges to safety in the various categories of plant states which are to be evaluated and assessed.
- 5.37.2 On the basis of the safety analysis, the design basis for items important to safety and their links to PIEs and event sequences shall be confirmed. It shall be demonstrated that the NPP as designed, is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.
- 5.37.3 The safety analysis shall provide assurance that DiD has been implemented in the design of the plant. Any exception should be justified.
- 5.37.4 The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff-edge effects and early radioactive releases or large radioactive releases.
- 5.37.5 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.
- 5.37.6 The computer programs, analytical methods and plant models used in the safety analysis shall be verified and validated.

### **5.38 Deterministic Approach**

- 5.38.1 The deterministic safety analysis shall mainly provide:
  - (a) establishment and confirmation of the design bases for all items important to safety;
  - (b) assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff-edge effects) will be prevented;
  - (c) characterization of the PIEs that are appropriate for the Site and the design of the plant;
  - (d) analysis and evaluation of event sequences that result from PIEs, to specify the environmental qualification requirements;
  - (e) comparison of the results of the analysis with applicable acceptance criteria;
  - (f) demonstration that the management of AOs and DBA conditions is possible by safety actions through automatic actuation of designated systems and safety systems respectively, and if necessary, in combination with prescribed actions by the operator;
  - (g) demonstration that the management of DEC is possible by the actuation of additional safety features/complementary safety features and safety features in combination with expected actions by the operator.

5.38.2 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 define clearly certain requirements for SSCs. The time span of any scenario that is analyzed should extend up to the moment when the plant reaches a safe state or safe shutdown state.

5.38.3 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.

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 DECAs, including severe accidents, best estimate methods and codes may 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.

5.38.4 It should be confirmed that operational limits and conditions are in compliance with the design assumptions and intent for the normal operation of the plant.

### **5.39 Source Term Evaluation**

5.39.1 An evaluation of the behavior of fission products, radioactive corrosion products, activation products in coolant, cover gas and impurities, and actinides following possible accidents of each type<sup>12</sup> at the NPP shall be carried out early in the design stage. This is required to identify all important phenomena that affect source term behavior and to identify the possible design features that could increase their retention in the plant.

5.39.2 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 and cover gas. Values for the effect of spiking on the activity of the primary coolant and cover gas due to relevant operational transient should be considered based on relevant operational data.

5.39.3 Different operational states and possible accident sequences could be grouped, and a bounding scenario could be 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 optimized so that requirements for radiation

---

<sup>12</sup> Each type here refers to different plant states [i.e. single failure (LOFA), multiple failures (ULOFA) etc.]

protection, including restrictions on doses, are being met.

- 5.39.4 A similar range of different types of DEC's 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.

#### **5.40 Probabilistic Approach**

- 5.40.1 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 PIE makes a disproportionately large or significantly uncertain contribution to the overall risk, and that, to the extent practicable, the levels of DiD 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 assessment 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;
- (g) calculating for multi-unit plants Sites, the associated risk for Site specific initiator. This assessment should also take into account of shared SSC;
- (h) identifying areas of design improvement or operational procedures or emergency operating procedures which would significantly enhance safety.

- 5.40.2 Level-1 PSA and Level-2 PSA shall be carried out

- (a) Level-1 PSA shall be carried out considering both internal and external events, at full power as well as shutdown state of the NPP.
- (b) Level-2 PSA shall be carried out considering internal events at full power state of NPP. Apart from reactor core, the radioactivity releases from the spent fuel storage pool also shall be considered.

5.40.3 .Probabilistic safety targets, as determined from PSA are given below:

<b>Risk Metrics</b>	<b>Target Frequency (per reactor-Year)</b>
Cumulative Core Damage Frequency (CDF) for all internal events and all external hazards including seismic, fire and flood hazards	$\leq 1.0\text{E-}05$
Core Damage Frequency (CDF) for internal events, for full power, low power and shutdown states	$\leq 1.0\text{E-}06$
Cumulative Large Early Release Frequency (LERF) for internal events at full power state	$\leq 1.0\text{E-}07$

## **6. DESIGN OF SPECIFIC PLANT SYSTEMS**

### **6A. REACTOR CORE AND REACTIVITY CONTROL**

#### **6.1 Reactor Core and Associated Systems**

- 6.1.1 The reactor core and associated coolant system, control and protection systems shall be designed with appropriate safety margins to assure that the specified design limits (refer Clause 5.3 of this Safety Code) are not exceeded in all operational states and in DBAs, with account taken of the well-established uncertainties.
- 6.1.2 The design of the reactor core, reactor assembly and the reactor internal structures shall account for the static and dynamic loadings expected under operational states and DBAs with due regard to the effects of temperature, pressure, irradiation, ageing, creep, corrosion, erosion, 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 for adequate core cooling.
- 6.1.3 The reactor core and associated coolant system, control and protection systems shall be designed so as to allow adequate inspection and test, as necessary, throughout the service life of the plant.
- 6.1.4 The design of coolant flow and core components shall be such that cavitation and local coolant boiling are avoided under all Design Basis Events (DBEs). In case local coolant boiling is unavoidable, it shall be demonstrated that net reactivity inserted is negative and there shall be no burnout at local hotspots.
- 6.1.5 Sufficient shielding shall be provided surrounding the core to limit the radiation damage and to maintain integrity of irreplaceable life limiting reactor components (e.g. grid plate, core support structure, main vessel etc.), to limit activation of the components for which maintenance may be required, and to limit activation of secondary sodium.

#### **6.2 Performance of Fuel Elements and Assemblies**

- 6.2.1 Fuel elements and assemblies for the NPP shall be designed to keep the deformations less than the specified design limits, to maintain their structural integrity, and to withstand satisfactorily the anticipated irradiation and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in operational states.
- 6.2.2 The processes of deterioration to be considered shall include those arising from: differential expansion and deformation; differential pressure on the clad from the coolant pressure and internal pressure due to helium and additional build-up of fission products in fuel elements; irradiation effect on the fuel like swelling 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 (including those caused by seismic 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 the data, calculations/computational models and the manufacturing tolerances.

- 6.2.3 Fuel elements and fuel subassemblies shall be capable of withstanding the loads and stresses associated with fuel handling.
- 6.2.4 Provision shall be made in the design to prevent 'unsafe' loading of subassemblies on the grid plate causing less coolant flow than that is required to remove the heat generated. Provision shall also be made in the design to prevent 'unsafe' loading of a higher fuel enrichment subassembly in a lower enrichment zone of the core.
- 6.2.5 Specified fuel design limits shall not be exceeded in normal operation, and conditions that could be imposed on fuel subassemblies during AOOs shall cause no significant additional deterioration.
- 6.2.6 Sodium flow paths through the core subassemblies shall be such that gross blockage of flow to and within a subassembly is precluded.
- 6.2.7 Individual fuel subassembly size shall be such that it does not become critical ( $k_{eff}$  not more than 0.95) when individually immersed in water, alcohol etc.
- 6.2.8 The design shall provide means for allowing reliable detection of failed fuel in the reactor during power operation, and subsequent removal of fuel subassembly having failed fuel pin from the reactor, if coolant activity limits are exceeded.
- 6.2.9 Two diverse systems for failed fuel detection shall be provided such as monitoring system for cover gas radioactivity and delayed neutrons in sodium. Operation of the plant with failed fuel (causing gas leak) shall not interfere with detection of subsequent failed fuel.
- 6.2.10 Design Safety Limits (DSLs) shall be established for fuel, clad and coolant for all categories of DBEs (up to DBA) and compliance shall be demonstrated.
- 6.2.11 Under operational states, power to flow mismatch in a fuel subassembly shall be detected within appropriate time so that corrective safety action is initiated and DSL is not exceeded.
- 6.2.12 In case of earthquake within design basis, reactivity transients introduced due to the relative movements of absorber rods and fuel subassemblies shall not result in crossing of DSL. For beyond design basis earthquake, the reactivity transients introduced due to the relative movements of absorber rods and fuel subassemblies shall be such that core damage is prevented.
- 6.2.13 Hold down of all subassemblies shall be ensured under all DBEs.
- 6.2.14 Coolant temperatures at the exits of all fuel subassemblies shall be measured during reactor operation using two or more thermocouples.
- 6.2.15 Amenability to flow measurement of both fuel and blanket subassemblies shall be ensured during shutdown state.

- 6.2.16 The requirements of Clauses 6.1 & 6.2 for reactor and fuel element design shall also be met in the event of changes in fuel management strategy or operational conditions during the plant life.

### **6.3 Structural Capability of the Reactor Core**

The fuel elements and fuel subassemblies and their supporting structures for the NPP shall be designed so that, in operational states and accident conditions other than severe accidents, a geometry that allows for maintaining adequate cooling and the insertion of absorber elements is not impaired. For the DEC's, structural integrity of primary coolant boundary shall be ensured taking into account of mechanical energy released during a Core Disruptive Accident (CDA). The subsequent re-criticality shall be avoided simultaneously ensuring cooling of core debris.

### **6.4 Control of the Reactor Core**

- 6.4.1 The reactor core and associated coolant, core support and absorber elements (including their drive mechanisms) shall be so designed that the total power co-efficient, the prompt power co-efficient and the total temperature co-efficient of reactivity shall be negative throughout the reactor life, for all operational states and DBA conditions, taking into account all core loading configurations and irradiation effects.
- 6.4.2 Distribution of neutron flux that can arise in any state of the reactor core in the NPP, including states arising after shutdown and during or after refuelling, and states arising from AOOs and from accident conditions not involving degradation of the reactor core, shall be inherently stable.
- 6.4.3 Adequate means of monitoring the neutron flux in the reactor core and its change shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits are exceeded.
- 6.4.4 In the design of reactivity control devices, due account shall be taken of wear-out and of the effects of irradiation, such as burn-up, changes in physical properties and dimensions, and production of gas during normal operation, AOOs and accident conditions.
- 6.4.5 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 boundary greater than limited local yielding, nor (ii) sufficiently disturb the core, its support structures or other reactor assembly internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by mechanical means), changes in reactor coolant temperature etc.
- 6.4.6 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.
- 6.4.7 Global or local power oscillation shall be automatically damped by the action of the reactivity feedback mechanisms. Maximum reactivity worth of absorber rod, together with



its maximum possible withdrawal speed shall be limited such that the fuel, coolant and cladding design limits are not exceeded.

- 6.4.8 The fuel design limits shall not be violated under any shape and level of neutron flux that can exist in any state of the core including those at fresh start-up, after shutdown, during and after refuelling and those arising from AOOs.
- 6.4.9 Special consideration shall be given for the detectors and monitoring requirements for the first approach to criticality and start-up of reactor after prolonged shutdown for first of a kind reactors.
- 6.4.10 Postulated whole core accident (CDA) shall be considered in the design as DEC to address safety aspects of energy release, radioactivity release to environment and adequate cooling of core debris. To avoid significant mechanical energy release during such accident, the reactor core shall be designed to have favorable neutronic, thermal, and physical characteristics, considering all reactivity feedbacks, including sodium void worth, to mitigate the consequences of such DEC.
- 6.4.11 During shutdown state, the core shall be monitored. The minimum count rate in the neutron detectors arising from core neutrons shall be more than prescribed limits in the shutdown state.
- 6.4.12 When different neutron detector systems are used to monitor the core, in different ranges of neutron flux levels, there shall be adequate overlap between any two systems covering adjacent ranges.

## **6.5 Reactor Assembly**

- 6.5.1 The reactor assembly<sup>13</sup> shall be designed and constructed to be of the highest quality with respect to materials, design standards, capability of inspection and fabrication.
- 6.5.2 The reactor assembly components shall be designed with due account taken of the creep properties, thermal stripping, fast neutron induced changes, other ageing effects, and the material compatibility with sodium and its compounds.
- 6.5.3 There shall be no penetrations in the walls of the main vessel) or safety vessel (Pool type NPPs).
- 6.5.4 Under operational states, DBAs and accident conditions, siphoning/draining of primary sodium from the reactor vessel below a level, leading to loss of heat removal from the core shall be prevented (Loop type NPPs).
- 6.5.5 Main vessel shall be enveloped with a safety vessel to contain the sodium in case of leak from the main vessel in such a way that it is possible to maintain sufficient coolant flow through core to remove decay heat. Interspace between main vessel and safety vessel shall

---

<sup>13</sup> The “Reactor Assembly” refers to the group of components such as Main Vessel, Safety Vessel, Grid Plate, Core Support Structure, Inner Vessel and Top Shields including control plug (Pool type NPP) and Main Vessel, Safety Vessel, Grid Plate, Core Support Structure, Top Shields including control plug (Loop type NPP)

be maintained under inert gas atmosphere.

- 6.5.6 The grid plate and the core support structure shall be designed and constructed to be of the highest quality with respect to materials, design standards and fabrication. Failure of the grid plate/primary pipe causing reduction in the core coolant flow must be prevented with high reliability.
- 6.5.7 Assemblies and associated core support structure shall be designed so that the core geometry can be preserved to prevent excessive reactivity effects during operation and DBAs.
- 6.5.8 Top shield of the reactor assembly shall be designed to limit exposure for normal occupancy of operating personnel from nuclear radiation during normal operation, maintenance and component handling.
- 6.5.9 Top shield and core support structure shall ensure that the failure of a critical load bearing member does not have cascading effect leading to loss of structural integrity (in the case of stiffened box type design).
- 6.5.10 Sodium from the main vessel shall not get drained out below a prescribed safe limit due to any leak in the primary sodium circuit.
- 6.5.11 Diverse systems shall be provided for the detection of sodium leak into the space between the main and safety vessels.
- 6.5.12 Cover gas system shall be designed so as to prevent air/gas ingress into the primary sodium and leakage of radioactive gas into the Reactor Containment Building (RCB). Cover gas system shall be designed to have provision to monitor oxygen and hydrogen in the supply as a source control measure of impurity.
- 6.5.13 From structural integrity considerations of the main vessel, external/internal pressure shall be maintained within the safe limits with application of single failure criteria in pressure regulating systems.
- 6.5.14 Water and oil shall not be used as a cooling medium for the top shield of reactor assembly.
- 6.5.15 Design shall minimize sodium aerosol deposition in the clearances between different equipment on the roof of reactor.
- 6.5.16 Auxiliary cooling circuits (like reactor assembly, top shield cooling, reactor vault concrete cooling) shall be designed with sufficient capacity and redundancy to remove the heat from the sources to the UHSs without exceeding the specified limits of the associated components and structures during all the operational conditions and DBAs. Considerations shall be given for the compatibility of fluids in the two circuits.
- 6.5.17 Provision shall be made for monitoring the horizontality of the core by suitable provisions such as displacement measurement device (Loop type NPPs).
- 6.5.18 Failure of core support or complete loss of core cooling, shall be practically eliminated.

## **6.6 Reactor Shutdown Systems**

- 6.6.1 Means shall be provided to ensure that there is a capability to shut down the reactor of the

NPP 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, not involving degradation of reactor core (refer Clause 6.3).

- 6.6.2 The reactivity worth and negative reactivity insertion rate of each shutdown system shall be such that for DBA, the design safety limits of fuel, coolant and clad specified for DBA are not exceeded.
- 6.6.3 For AOOs, appropriate systems shall be initiated automatically, as necessary, including reactor shutdown systems, to ensure that design safety limits of fuel, coolant and clad for AOOs are not exceeded. For AOOs requiring reactor trip, deviation in calculated consequences, if any while assuming reactor trip with SDS-2, should be justified utilizing probabilistic inputs, however, the consequences shall be limited and shall remain well within the DBAs.
- 6.6.4 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 to insert one absorber rod with maximum worth) or that could result in a common cause failure.
- 6.6.5 The means for shutting down the reactor shall consist of at least two diverse and independent, automatic, fast acting shutdown systems<sup>14</sup>.
- 6.6.6 Each of the shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability. Each individual shutdown system shall be designed such that its failure probability is less than  $1\text{E-}03/\text{demand}$ , subject to meeting the overall probabilistic safety targets given in Clause 5.41.3.
- 6.6.7 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.
- 6.6.8 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. The design shall be such that all availability testing during reactor operation can be carried out without affecting the effectiveness of each shutdown system.
- 6.6.9 With all absorber rods inside the core, the minimum shutdown margin (SDM) shall be more than 10\$. Even with fuel loading error, there shall be sufficient shut down margins (more than 1\$). In this regard all possible errors shall be considered. This includes:
  - (a) the replacement of absorber rod of maximum worth with a fresh fuel subassembly of maximum enrichment; and
  - (b) withdrawal of two absorber rods of maximum total worth including anti-shadowing effects.
- 6.6.10 Minimum SDM taking into account failure of any one shut down system and failure of maximum worth rod of working shut down system shall be more than 1\$ at cold shutdown

---

<sup>14</sup> Refer Section 6L.

state for all PIEs. Maximum reactivity worth of an absorber rod with its maximum withdrawal speed shall be designed such that DSL limits of fuel, coolant and clad are not exceeded in case of its withdrawal.

- 6.6.11 The design of the mechanism for withdrawal of absorber rods shall ensure prevention of unintended or uncontrolled withdrawal.
- 6.6.12 The reactivity worth, speed of action and delay in actuation of each shutdown system shall be such that during all operational states and DBA of the reactor, the reactor is rendered sufficiently sub-critical and maintained sub-critical. If a shutdown system or its subgroup is used for reactivity control, its functional capability to shut down the reactor shall not be jeopardized.
- 6.6.13 At least one of the shutdown systems shall be dedicated only for shutdown function and shall have the capability to bring the reactor to shutdown state and shall be so designed that it meets all functional requirements even in the case of postulated core deformation scenarios considered within the design basis.
- 6.6.14 Provision shall be available to monitor performance of the shutdown system (e.g. drop time measurement).
- 6.6.15 All equipment in shut down system shall be designed such that its failure modes will not result in an unsafe condition.
- 6.6.16 The shutdown system mechanisms including drive systems shall be designed for appropriate seismic category and qualified by tests. Results of tests done for identical system may be credited.
- 6.6.17 The design shall be such that each shutdown system can be actuated manually from the MCR and SCR.
- 6.6.18 The design shall be such that it is not possible for an operator to prevent a safe automatic action from taking place.
- 6.6.19 Any AOO or DBA, which require fast reactor trip for its mitigation, shall have two independent trip parameters for each shutdown system, one backed by the other.
- 6.6.20 Design shall provide automatic reactor trip in case of a seismic event beyond the specified threshold limit.

## **6B. REACTOR COOLANT SYSTEMS**

### **6.7 Design of Reactor Coolant System**

- 6.7.1 The components of the reactor coolant systems for the NPP shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.
- 6.7.2 The design shall take into consideration the behavior of primary coolant boundary material under operational, maintenance and testing conditions and in DBAs, taking into account the expected end of life properties (which are affected by creep properties, erosion, thermal

striping, fast neutron fluence, and other ageing effects, as well as its compatibility with sodium, and with thermal stress and dynamic load on thin-walled structures used under low pressure and high temperature conditions), any uncertainties in determining the initial state of material of the components, and the rate of possible deterioration.

- 6.7.3 The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant boundary could exhibit embrittlement are avoided.
- 6.7.4 The design of the components contained inside the reactor coolant boundary, such as pump impellers and receptacles, shall be such as to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in DBAs, with due allowance made for deterioration that might occur in service.
- 6.7.5 The materials used in the fabrication of the component parts shall be so selected as to minimize their activation by neutrons and carburization and decarburization effects.
- 6.7.6 If heat removal function under the accident conditions involving primary heat transport boundary is likely to be adversely affected, the system (provided to cope with this situation) shall be designed assuming single failure.
- 6.7.7 Components which are part of reactor coolant boundary shall be designed, fabricated, inspected, erected and tested to the highest quality standards.
- 6.7.8 The design of the reactor coolant boundary shall be such that flaws are very unlikely to be initiated, and any flaws that are initiated will propagate in such a manner that it results in leaks well before the time flaws would grow to an unstable size, thereby permitting the timely detection of coolant leakage. LBB philosophy needs to be established and proved. System shall be provided for early leak detection and its adequacy shall be demonstrated.
- 6.7.9 Inert gas shall be used as a cover gas in sodium filled components to prevent chemical reaction at the free surface of sodium. The boundaries of cover gas should be leak resistant such that the radioactivity levels in RCB remain within the permissible limits.
- 6.7.10 Adequate provisions for the removal of radioactive substances from the reactor coolant, including activated corrosion products and fission products leaking from the fuel shall be made available. The capacity of the necessary systems shall be based on the specified fuel design limit on operation with postulated number of fuel failures (gas leakers) with a conservative margin to ensure that the plant can be operated with a level of circuit activity, which is as low as reasonably practicable, and that radioactive releases meet the prescribed limits.
- 6.7.11 Provisions shall be made to detect sodium leaks and to mitigate the consequence of sodium chemical reaction in case of postulated sodium leaks from the reactor coolant systems. The reactor safety functions shall be maintained under severe sodium leak events considered in the DECAs.
- 6.7.12 The design shall consider the potential for flow and thermal disturbances, such as flow induced vibrations, and shall reduce or eliminate such effects to maintain the structural

integrity of the components of the reactor coolant systems.

- 6.7.13 The opaqueness of the sodium coolant shall be taken into consideration in the design of the components contained inside the reactor coolant system.
- 6.7.14 Provision shall be made for maintaining the level of the reactor coolant to ensure that specified design limits are not exceeded in operational states and that the cooling of fuel is maintained in accident conditions, with taking due account of volumetric changes to ensure heat removal by coolant circulation.
- 6.7.15 Components, which constitute the reactor coolant boundary, shall be designed to maintain the boundary function in case of Anticipated Transients without Scram (ATWS).
- 6.7.16 Thermowells or instrumentation lines, which penetrate or are connected to the boundary of the reactor coolant systems, shall be designed so that sodium leaks and the consequences caused by their failure are prevented and/or mitigated. Response time and integrity of thermowells under the flow condition shall be commensurate with assumptions in safety analysis.
- 6.7.17 Safety Vessel and guard pipes shall be designed so as to maintain the sodium surface of the primary coolant system at a level necessary for decay heat removal in the case of a sodium leak accident in the primary coolant system (Loop type NPPs).
- 6.7.18 The primary sodium piping shall be provided with guard pipe or an equivalent arrangement (Loop type NPPs).

## **6.8 In-Service Inspection (ISI) of Reactor Coolant Boundary**

- 6.8.1 The components of the reactor coolant 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.
- 6.8.2 Provision shall be made to implement a material surveillance programme for the reactor assembly components, particularly in high irradiation locations, and other important components as appropriate for determining the effect of environment on material properties.
- 6.8.3 Monitoring of healthiness of the reactor coolant boundary shall be provided by detection of leakage during reactor operation and by detection of flaws, tilt and elongation under shutdown condition.
- 6.8.4 Where the safety analysis of the NPP indicates that particular failures in the secondary cooling system may result in serious consequences, it shall be ensured that inspection of relevant parts of the secondary cooling system is possible.
- 6.8.5 Pre-Service Inspection (PSI) of the reactor coolant boundary shall be carried out prior to start of operation to establish the baseline data for future ISI.

## **6.9 Purification of Reactor Coolant**

- 6.9.1 Systems shall be provided to monitor and maintain purity of coolant and cover gas within allowable limits, which shall be based on consideration of air leak into the cover gas, build-

up sodium aerosol, corrosion, fouling, plugging of passages, radioactivity concentration, detection of sodium-water/steam reaction, etc. Reactor cover gas shall be provided with monitors to detect entry of air or oil ingress from sodium pump auxiliaries (mechanical seals and bearing) into sodium.

- 6.9.2 Entrainment of argon in sodium from cover gas used in surge tank shall be monitored.

## **6.10 Heat Transport Systems**

- 6.10.1 The various coolant systems and associated control, protection and auxiliary systems shall be designed to have sufficient capacity with adequate margins and redundancy to remove the heat from the core and transport it to the UHS, without exceeding the specified limits for fuel coolant and structures, under all operational states of the reactor and design basis events.
- 6.10.2 System containing sodium shall be protected against the consequences of design basis events of other components and systems. All the sodium circuits shall be protected against failure from accidental dropping of objects and other missiles by suitable designs.
- 6.10.3 Reduction of coolant flow (primary and secondary) below a threshold shall lead to automatic reactor shutdown early enough to prevent the applicable DSL being crossed.
- 6.10.4 In the event of failure of primary piping within the design basis (Double Ended Guillotine Rupture of a single pipe), crossing of design safety limits shall be prevented by the reactor shutdown systems and by adequate decay heat removal.
- 6.10.5 The primary coolant circuit shall be designed to prevent ingress of oil or gas into it. In case of ingress of gas or oil, the likelihood of which shall be remote, the resulting reactivity change shall be within the capabilities of the shutdown systems.
- 6.10.6 Design shall prevent carry over of hydrogenous materials and reaction products (hydrogen, sodium hydroxide etc.) into the core in case of a sodium-water/steam reaction in steam generators.
- 6.10.7 Heat transport system shall be designed such that radioactivity shall not spread over from primary reactor coolant system to secondary system, in case of breach in interface boundary.
- 6.10.8 The heat transport items important to safety shall be independent, redundant and physically separate from each other to prevent common cause and cross-linked failures.
- 6.10.9 Provisions shall be made for all sodium containing systems to automatically detect leaks at an early stage by diverse means. Automatic provision shall also be made for identifying the location of the leaks to the extent practicable.
- 6.10.10 Provisions shall be made in the design of sodium and its auxiliary circuits and their components to prevent entry of harmful fluids into the sodium, such as oil and air/gas.
- 6.10.11 Adequate arrangements shall be provided for transferring and storing coolant, particularly sodium, to and from equipment/components when required.
- 6.10.12 The boundaries of the sodium systems shall be designed so as to have an extremely low

probability of leakage, rapidly propagating failure and gross rupture under the static and dynamic loads expected during all operational states and all other postulated initiating events. The design for the above shall include considerations of degradation of material properties (e.g. effect of sodium, temperature, irradiation), and other phenomena such as flow induced vibrations, transients, residual stresses, and flaw size.

6.10.13 Provision shall be made for ISI of steam generator tubes, and bimetallic welds in shell nozzles. Baseline data shall be established as PSI.

## **6.11 Decay Heat Removal Systems**

6.11.1 Diverse means shall be provided for the removal of decay heat from the reactor core to an UHS, in auto mode, after shutdown of the reactor in operational states and in accident conditions.

6.11.2 The decay heat removal systems for cooling of the reactor core shall be such as to ensure that:

- (a) the design limits for fuel, the reactor coolant boundary and structures important to safety are not exceeded,
- (b) the cooling of the fuel is restored and maintained under accident conditions even if the integrity of the reactor coolant boundary is not maintained, and
- (c) function to transfer decay heat from items important to safety to an UHS is carried out with high levels of reliability for all plant states.

6.11.3 The decay heat removal system shall be designed to:

- (a) provide redundancy and diversity to the extent practicable, for reducing failures due to CCFs, including external events.
- (b) prevent freezing of the sodium coolant to avoid blockage of coolant circulation, and
- (c) provide detection and mitigation measures against postulated leakage of residual heat removal fluid.

6.11.4 Means shall be provided for the capability of core cooling under postulated plant conditions with core degradation. In DECAs, means for residual heat transfer shall be provided, in addition to a decay heat removal system for AOOs, and DBAs (refer Clause 5.18.3), with the conditions as listed below:

- (a) The cooling of the reactor core is possible even under extreme external events and their consequences (viz., long-term loss of all AC power supplies),
- (b) Passive mechanisms are used to the extent practicable, and
- (c) Residual heat removal system has diversity to the extent practicable.

6.11.5 Provision shall be made for transfer of decay heat from damaged/molten core to an UHS to ensure that acceptable temperatures can be maintained in SSCs important to the safety function of confinement of radioactive materials in the event of a severe accident.

6.11.6 For UHS as air, the design shall take into account the effect of cyclonic and severe weather conditions.



6.11.7 Provision shall be made in the design for periodic testing of decay heat removal systems to ensure their performance at their designed capacities.

## **6.12 Sodium Heating Systems**

6.12.1 The sodium heating systems and their controls shall be appropriately designed with suitable redundancy to assure that the temperature distribution and rate of change of temperature of the items are maintained within design limits, assuming a single failure.

6.12.2 The effect of non-availability of heating power shall be considered in analysis for all states of the reactor even when there is no core decay heat.

## **6.13 Sodium-Water Reactions**

6.13.1 Steam Generators and associated circuits shall be designed, constructed and operated so as to minimize the probability of water/steam leakages, and to limit the consequences resulting from sodium-water/steam reactions.

6.13.2 Flow instability in steam generators shall be avoided, with sufficient margin, by suitable design provisions.

6.13.3 Systems shall be provided to detect at an early stage at all temperatures, rapidly and reliably, the presence of small water leakages into sodium and to initiate actions to stop further progression of the sodium-water reactions. Appropriate pressure relieving systems (preferably passive systems) shall be provided to minimize the consequences of large sodium-water reactions.

6.13.4 In the design of secondary sodium and its auxiliary circuits and their components, maximum credible transient pressures and associated forces generated due to events such as sodium-water/steam reaction in steam generator, valve closure, shall be considered. Possibility of any effect propagating to primary side (e.g. through IHX) shall be investigated and precluded.

6.13.5 Spreading of corrosive substances in the secondary circuit and the water/steam system, following a leak, shall be minimized.

6.13.6 Release of sodium-water reaction products shall not endanger parts of the plant having a safety function.

# **6C. CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM**

## **6.14 Containment System**

6.14.1 A containment system shall be provided to ensure, or to contribute to, the fulfillment of the following safety functions at the NPP:

- (a) confinement of radioactive substances in operational states and in accident conditions,
- (b) protection of the reactor against natural and human induced events, and
- (c) radiation shielding in operational states and in accident conditions.

6.14.2 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, argon, nitrogen and other substances that may be released into the containment atmosphere.

6.14.3 The design of the containment system shall take into account all identified DBAs and DECAs.

## **6.15 Containment Structure**

6.15.1 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 hazards. Loss of containment structural integrity shall be practically eliminated.

6.15.2 The design 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 DBAs and DECAs<sup>15</sup>. Design provision shall be made to prevent the loss of the containment structural integrity in all plant states so that early or large radioactive releases are practically eliminated.

If assessment of containment pressure management strategies brings out the need, then provision for filtered venting of containment should be considered to avoid containment failure<sup>16</sup>. If provided, it should not be designed as the principal means of removing energy from the containment. Venting should not be done as a near term measure and this system should be used under extreme exigency. The use of this provision shall not lead to early or to large radioactive releases.

6.15.3 The effects of other potential energy sources, including for example, possible chemical and radiolytic reactions, shall also be considered.

6.15.4 Design basis of the containment shall include postulated core melting accident resulting in at least one credible scenario imposing highest loads on the containment. In calculating the necessary strength of the containment structure, natural phenomena and human induced events shall be taken into consideration (refer Clause 5.15.2), and provision shall be made to monitor the condition of the containment and its associated features. The structural design of the containment shall consider the thermal stresses arising from the calculated temperature transients and spatial temperature profiles within the structure during postulated accident conditions, as well as during normal operation.

6.15.5 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. The design shall provide for ample flow routes between separate compartments (if existing) inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in design basis

---

<sup>15</sup>An assessment of Ultimate Load Bearing Capacity (ULBC) of the containment structure which is normally required for water cooled reactors, is not needed for SFR based NPPs as the design pressure of the containment is the pressure resulting from the severe accident (Design Extension Condition- CDA).

<sup>16</sup>The provision of containment filtered venting shall not be credited for demonstration of containment safety.

events do not result in damage to the pressure bearing structure or to other systems of importance in limiting the effects of accident conditions.

- 6.15.6 The containment structure and the 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 the structural integrity and the required level of leak tightness.
- 6.15.7 Provisions shall be included in the design to monitor the condition of the containment and associated features following a PIE.
- 6.15.8 The number of penetrations through the containment should be optimized 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.
- 6.15.9 The containment shall provide sufficient shielding to permit post-accident Site occupancy requirements especially MCR and SCR habitability.
- 6.15.10 The containment shall be maintained under negative pressure during all operational states of the reactor except during special operations like transportation of IHX from RCB in reactor shutdown state.

## **6.16 Control of Radioactive Releases from the Containment**

- 6.16.1 The design of the containment shall be such as to ensure that any release of radioactive material from the NPP to the environment is as low as reasonably achievable, below the authorized limits for discharges in operational states and below acceptable limits in accident conditions.
- 6.16.2 The containment structure and the systems and components affecting the leak tightness of the containment system shall be designed and constructed so that the integrated leak rate test can be conducted during commissioning and subsequently during the operating lifetime of the plant at specified intervals.
- 6.16.3 If resilient seals (such as elastomeric seals or electrical cable penetrations) or expansion bellows are used with penetrations, they shall be designed to have leak testing capabilities as part of local leak rate tests independent of the overall leak rate determination of the containment, to demonstrate their continuing integrity throughout the life of the plant.
- 6.16.4 The number of penetrations through the containment shall be kept to a practical minimum.
- 6.16.5 Penetrations through the containment through which pipes containing fluids at high temperature pass shall have suitable cooling provision such that concrete temperatures are maintained within allowed limits under all DBE.

## **6.17 Isolation of the Containment**

- 6.17.1 Piping systems penetrating 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, dampers and associated apparatus and to determine if leakage is within design limits.

6.17.2 At least two adequately diverse parameters shall be provided for generating containment isolation signal.

6.17.3 Containment atmosphere isolation valves

- (a) Each line that connects directly to the containment atmosphere and penetrates primary reactor containment shall be provided with containment isolation valves<sup>17</sup> 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:
  - i. one locked closed isolation valve inside and one locked closed isolation valve outside containment; or
  - ii. one automatic isolation valve inside and one locked closed isolation valve outside containment; or
  - iii. 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
  - iv. 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.
- (b) 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.

6.17.4 *Closed System Isolation Valves*

- (a) Each line that penetrates primary reactor containment and is neither part of the reactor coolant 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.
- (b) The design shall recognize the conflict arising between the requirements for containment isolation provisions and the requirements for necessary safety systems that penetrate the containment envelope. In such cases, consideration of the isolation provisions shall be balanced by the required availability of the necessary safety systems and the need to avoid the escalation of the accident condition. For those pipelines penetrating the containment and which shall not be isolated during containment box up signal in view of their safety functions, it shall be ensured during design that such of these system boundaries are qualified for containment pressure boundary. It shall also

---

<sup>17</sup> 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.

be ensured by other design provisions such that uncontrolled radioactive release to the environment resulting from potential pipe failure is practically eliminated.

#### **6.18 Access to the Containment**

- 6.18.1 Access by operating personnel to the containment at NPP 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.
- 6.18.2 Where provision is made for entry of operating personnel for surveillance purposes, provision for ensuring protection and safety for operating personnel shall be specified in the design. At least one route of egress shall be available for emergency evacuation.
- 6.18.3 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**

- 6.19.1 Provision shall be made to control the pressure and temperature in the containment at NPP, 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.
- 6.19.2 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.
- 6.19.3 The coverings and coatings for components and structures within the containment system shall be carefully selected, and their methods of application specified, to ensure fulfillment of their safety functions and to minimize interference with other safety functions in the event of deterioration of coverings and coatings. They shall be qualified for the environment which they will experience, including radiation effects, for applicable length of time.

#### **6.20 Containment Heat Removal**

- 6.20.1 Adequate consideration shall be given to the capability to remove heat from the reactor containment in the event of postulated accident including severe accident. Any active system provided for this shall have adequate reliability.
- 6.20.2 The capability to remove the heat from the reactor containment shall be ensured. The safety function shall be fulfilled by reducing the pressure and temperature in the containment, and maintaining them at acceptably low levels, after an accidental release of high energy fluids into it in a DBA. If an active system is provided for performing the function of heat removal from containment, then that system shall have adequate reliability

and redundancy to ensure that this can be fulfilled, on the assumption of a single failure. These systems shall be designed to permit appropriate inspection and testing during service.

## **6D. INSTRUMENTATION AND CONTROL SYSTEMS**

### **6.21 Provision of Instrumentation**

6.21.1 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 NPP.

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

6.21.3 Instrumentation shall be environmentally qualified for the relevant plant states covering all DBE.

#### *6.21.4 Control Systems*

Appropriate and reliable control systems shall be provided to maintain and limit the relevant process variables within the specified operational ranges while safety related variables shall be maintained within prescribed ranges. Annunciation shall be provided if any of the parameters/safety related variables exceed their set limits. While determining the set points, parameters such as inertia of the system, response time and errors associated with instrumentation and control system etc. shall be taken into account.

#### *6.21.5 Protection Systems*

(a) A protection system shall be provided at the NPP 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.

(b) The protection system shall be designed:

- i. to be capable of overriding unsafe actions of the control systems,
- ii. with fail safe characteristics to achieve safe plant conditions in the event of failure of the protection system, and
- iii. to ensure that safety action once initiated by protection system is sealed-in (latched).

6.21.6 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 AOOs 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.

## **6.22 Reliability and Testability of Instrumentation and Control Systems**

- 6.22.1 Instrumentation and control systems for items important to safety at the NPP 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 protection system channel do not result in loss of the protection system function.
- 6.22.2 Safety related systems shall be designed with redundancy and self-diagnostic capability.
- 6.22.3 Design techniques such as testability, including self-checking capability where necessary, functional diversity, diversity in component design and in concepts of operation shall be used in the safety system to the extent practicable to prevent loss of a safety function.
- 6.22.4 Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and 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.
- 6.22.5 When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of bypass of any protection system that is necessary for the duration of the testing or maintenance activities. Such bypass conditions shall be justified and duly authorized.
- 6.22.6 Design and layout of instrumentation system shall be such as to permit periodic testing, calibration and preventive maintenance in order to detect and rectify faults and failures of instruments and their components. Wherever necessary, calibration, testing and preventive maintenance shall be made possible without affecting the operating state of reactor and without jeopardizing safety.
- 6.22.7 Power supply for instrumentation of safety systems and safety related instrumentation – both pneumatic and electrical - shall be designed to ensure redundancy with physical separation, adequate availability and reliability commensurate with safety functions. Power supplies to redundant channels of instrument systems shall be from independent

divisions of power supplies.

### **6.23 Separation of Protection Systems and Control Systems**

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

6.23.2 Wherever interconnection is unavoidable, adequate physical isolation shall be provided.

6.23.3 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.

### **6.24 Use of non-programmable digital systems or computer based systems or programmable equipment Important to Safety**

6.24.1 If a system important to safety at the nuclear power plant is dependent upon non-programmable digital systems or computer based systems or programmable equipment, appropriate standards and practices for the development and testing of hardware and software, as appropriate, 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.

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

- (a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety.
- (b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable.
- (c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team, to provide assurance of its high reliability. Where high reliability of such systems 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) Consequences of Common cause failures deriving from software in Safety Systems shall be addressed.
- (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 processors 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.

- (i) analysis with respect to computer security should be done and device should not compromise plant computer security.

## **6.25 Main Control Room (MCR)**

- 6.25.1 A main control room shall be provided at the NPP 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 AOOs and accident conditions.
- 6.25.2 Displays in the MCR 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 MCR.
- 6.25.3 Special attention shall be paid to identifying those events, both internal and external to the MCR, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events.
- 6.25.4 Appropriate measures shall be taken, including the provision of barriers between the MCR at the NPP and the external environment, and adequate information shall be provided for the protection of occupants of the MCR 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.
- 6.25.5 The safety functions initiated by automatic control logic in response to an accident should also be possible to be initiated manually from the MCR.
- 6.25.6 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.
- 6.25.7 The design of the MCR shall be such that appropriate lighting levels and thermal environment are maintained, and noise levels are minimized to applicable standards and codes. Human engineering aspects shall be taken into consideration in MCR design (refer Clause 5.24.7)
- 6.25.8 Cable lay out for the instrumentation and control equipment in the MCR shall be arranged such that a fire in the Supplementary Control Room (SCR) cannot disable the equipment in the MCR.
- 6.25.9 The MCR shall be provided with secure communication channels to the On-Site Emergency Support Centre (OESC) and to off-site emergency response organizations, and

to allow for extended operating periods.

- 6.25.10 The design of MCR and SCR shall be such that no internal PIE can affect them simultaneously.
- 6.25.11 The MCR design shall provide appropriate measures to enable prevention of unauthorized access to items important to safety, located there.
- 6.25.12 Safety Parameter Display System panel shall be provided distinct from other control panels to enhance operator performance.
- 6.25.13 Two intakes should be provided for the air conditioning of MCR to ensure habitability under certain extreme conditions. Separate air conditioning should be provided for MCR and SCR.

## **6.26 Supplementary Control Room (SCR)**

- 6.26.1 Instrumentation and control equipment shall be kept available, preferably at a single location (in SCR) that is physically, electrically and functionally separate from the MCR at the NPP. The SCR 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 MCR.
- 6.26.2 Appropriate measures shall be taken in SCR, including the provision of barriers between the SCR at the NPP and the external environment, and adequate information shall be provided for the protection of occupants of the SCR 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 safe stay of operators.
- 6.26.3 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.
- 6.26.4 The SCR shall be provided with secure communication channels to the OESC and to off-site emergency response organizations. The SCR shall allow for extended operating periods.

## **6.27 Onsite Emergency Support Centre (OESC)**

- 6.27.1 An onsite emergency support centre, separate from both the MCR and the SCR, shall be provided from which the emergency response can be directed at the NPP during certain extreme external events and/or DEC's. The facility shall have adequate radiation shielding and shall be qualified for external events with sufficient margin. The layout and services of the facility shall be designed considering multiple NPPs and nuclear facilities at that Site.
- 6.27.2 Information about important plant parameters and radiological conditions at the NPP and in its immediate surroundings shall be provided in the OESC. The OESC shall provide means of communication with the MCR, the SCR and other important locations at the plant, and with on-site and off-site emergency response organizations. Appropriate

measures shall be taken to protect the occupants of the OESC for a protracted time against hazards resulting from accident conditions. The OESC shall include the necessary systems and services to permit extended periods of occupation and operation by emergency response personnel. The OESC shall have its own dedicated power supply system.

6.27.3 The OESC shall include display system indicating important parameters which are required for taking necessary actions during severe accidents.

6.27.4 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 OESC.

6.27.5 OESC shall be provided with means of communication with MCR, SCR and important locations in the plant.

## **6.28 Severe Accident Monitoring**

6.28.1 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.

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

- (a) condition of core or debris;
- (b) condition of reactor assembly;
- (c) condition of containment and its atmosphere;
- (d) condition of spent fuel storage pool (radiation level, water level & temperature of pool);
- (e) radiological situation in the plant, Site and its immediate surroundings ; and
- (f) status of implementation of accident management measures.

6.28.3 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**

### **6.29 General Requirements**

6.29.1 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 SSCs important to safety during all plant states.

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

6.29.3 Consideration shall be given for emergency power supply system for DEC's including severe accident.

### **6.30 Off-Site Power System**

6.30.1 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 minimize 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.

- 6.30.2 An independent auxiliary standby circuit including auxiliary standby transformer (AST) shall be provided to cater to safety and non-safety loads of the plant.

### **6.31 On-Site Power System**

On-site power system is composed of distribution systems and power supplies within NPP and shall have AC and DC power supplies necessary to bring NPP to a controlled state following AOOs or accident conditions and to maintain it in a controlled state, or a safe state or severe accident safe state, in the event of the loss of off-site power. The on-site power shall include emergency power supply and DEC power source. Design shall have provisions for use of non-permanent equipment to handle unexpected failure.

### **6.32 Emergency Power Supply**

- 6.32.1 The emergency power supply at the NPP shall be capable of supplying the necessary power in AOOs and accident conditions, in the event of LOOP.
- 6.32.2 In the design basis for the emergency power supply at the NPP, due account shall be taken of the PIEs 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.
- 6.32.3 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.
- 6.32.4 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.
- 6.32.5 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.
- 6.32.6 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.
- 6.32.7 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.
- 6.32.8 The design basis for any diesel engine ) or other prime mover<sup>18</sup> 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(e)];
  - (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.
- 6.32.9 The capacity of the batteries shall be such as to ensure power supply to - MCR panel indications, instrumentation and control related to safety systems, and emergency lighting for the period of station black out (SBO).
- 6.32.10 Continuity of power shall be ensured such that any short-term actions necessary to mitigate the consequences of DEC's can be completed despite the loss of the AC power sources and the event that triggered it.
- 6.32.11 The design shall also include a DEC power source adequately protected from external hazards, to supply the necessary power in design extension conditions.
- 6.32.12 The DEC power source shall be independent diverse and physically separated from the emergency power source provided for DBAs. The dedicated back-up power (from the DEC power source) system connection time shall be consistent with Emergency power supply battery autonomy.
- 6.32.13 The DEC 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 provided for design basis accidents.
- 6.32.14 The DEC power source shall be capable of supplying power to the equipment necessary to mitigate the consequences of DEC's involving a loss of the off-site power combined with the failure of the emergency power source provided for DBAs
- 6.32.15 The design shall have provisions to mitigate simultaneous occurrence of SBO and loss of UHS due to Extreme External Events (EEE), such that the fundamental safety functions are ensured at all units on a Site, including core cooling, containment, and Spent Fuel Pool cooling capabilities. Such provisions shall be ensured for survivability during an EEE.
- 6.32.16 Equipment necessary to mitigate the consequences of a core melt accident shall be capable of being supplied by any of the power sources.

### **6.33 Station Blackout (SBO)**

- 6.33.1 The probability of combined failure of all off-site power supply and on-site AC power

---

<sup>18</sup> 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.

supply (station blackout) shall be highly unlikely. It shall however, be demonstrated by analysis that batteries and other built-in design and operating provisions shall ensure that specified fuel, cladding, coolant, component design limits and containment integrity are maintained during SBO.

6.33.2 Provisions to mitigate Extended SBO should include:

- (a) SBO coping capability of at least twenty four (24) hours using installed equipment
- (b) establish the equipment, procedures, and training necessary to implement an “Extended SBO coping time of at least seven (7) days for core and spent fuel pool cooling as needed ensuring essential lighting and instrumentation needs, with the use of dedicated power sources & other resources available at the Site as required and
- (c) arrangement for availing off-site resources to support uninterrupted core and spent fuel pool cooling as needed, including the ability to deliver the equipment to the Site in the time period allowed for extended coping, under conditions involving significant degradation of off-site transportation infrastructure associated with significant natural disasters.

## **6F. SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS**

### **6.34 Performance of Supporting Systems and Auxiliary Systems**

6.34.1 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 NPP.

### **6.35 Process Water Cooling System**

6.35.1 Process water cooling system shall be provided as appropriate to remove heat from systems and components at the NPP that are required to function in operational states and in accident conditions.

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

6.35.3 Within the containment, use of water shall be minimized. In case water is used, multiple barriers to contain the leak and monitoring provisions to detect the leak shall be available. Water lines shall be physically separated from the sodium lines. Protection shall also be made to prevent leaks under postulated accident conditions. Number of flanged joints shall be minimized and shall have provision for leakage detection, collection, monitoring and drainage to a safe location. The use of oils shall also be minimized.

### **6.36 Process Sampling Systems and Post-Accident Sampling Systems**

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

6.36.2 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.

### **6.37 Compressed Air Systems**

- 6.37.1 The design basis for any compressed air system that serves an item important to safety at the NPP shall specify the quality, flow rate and cleanliness of the air to be provided.
- 6.37.2 Compressed air systems shall be designed such that non-essential parts of the systems can be isolated.
- 6.37.3 Consideration should be given for avoiding use of compressed air driven devices inside the containment for continued use, during accident management.

### **6.38 Air Conditioning and Ventilation Systems**

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

The system shall have provisions to detect the need for isolation and capabilities to isolate in time the portions of the system with required reliability.

- 6.38.2 Systems shall be provided for the ventilation of buildings at the NPP 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 authorized limits and as low as reasonably achievable;
  - (d) ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents; and
  - (e) control release of gaseous radioactive material to the environment below the authorized limits for discharges and to keep them as low as reasonably achievable.
- 6.38.3 Areas of higher contamination at the plant shall be maintained at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas.

### **6.39 Fire Protection Systems (FPS)**

- 6.39.1 Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the NPP, with due account taken of the results of the fire hazard analysis (FHA).
  - (a) 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.
  - (b) the fire protection systems installed at the NPP shall be capable of dealing safely

with fire events of the various types that are postulated.

- (c) 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.
- (d) fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start.
- (e) fire detection systems and fire extinguishing systems that are necessary to protect against a possible fire following a PIE shall be appropriately qualified to resist the effects of the PIE.
- (f) consideration shall be given to personnel safety while designing fire protection system.

#### **6.40 Fire Protection for Sodium (Na)**

- 6.40.1 Fire protection arrangements shall be in place before the arrival of sodium at Site.
- 6.40.2 Primary sodium circuits shall be designed to prevent initiation of sodium fire in the event of leakage during any PIE.
- 6.40.3 Diverse sodium fire detection systems shall be provided in the plant with high sensitivity and reliability. These systems shall be designed to survive the sodium fire. Provisions shall be made for testability and replaceability of this system.
- 6.40.4 Design shall provide for draining or fast dumping of the sodium from the circuits in case of leaks, to limit the amount of sodium that can leak.
- 6.40.5 In order to limit the sodium fire, barriers shall be provided to prevent fire from spreading.
- 6.40.6 Effects of possible interaction between sodium and concrete (its moisture) and hence hydrogen generation due to this reaction shall be considered in the design. Sodium resistant concrete or steel liners shall be provided on concrete as appropriate.
- 6.40.7 Adequate storage of appropriate extinguishers shall be provided at appropriate locations, considering the layout of sodium circuits. Provision shall be made for remote-manual/manual operation of fire extinguishing systems depending on accessibility for firefighting, location of equipment, ventilation etc.
- 6.40.8 Release of sodium aerosols at Site boundary air shall be less than the prescribed limits for all design basis sodium leaks.
- 6.40.9 Design analysis of design basis sodium fires shall take into account mechanical, thermal and chemical effects on items important to safety. Items identified to survive sodium fire shall be qualified against the effect of sodium fire.
- 6.40.10 Re-qualification/replacement of items important to safety, after sodium fire shall be considered in the design.
- 6.40.11 Conventional firefighting strategies shall take into consideration of the presence of sodium bearing components.



## **6.41 Lighting Systems**

- 6.41.1 Adequate lighting shall be provided in all operational areas of the NPP in operational states and in accident conditions.

## **6.42 Overhead Lifting Equipment**

- 6.42.1 The overhead lifting equipment provided for lifting and lowering items important to safety and for lifting and lowering other items in the proximity of items important to safety at the NPP 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; and
  - (f) parking for overhead crane shall be provided in such a way that any safety related item is not coming under it. Safety related cranes shall be provided with locking arrangement such that during seismic event the crane remains parked safely.

## **6G. COMPONENT HANDLING AND STORAGE SYSTEMS**

### **6.43 Component Handling and Storage Systems**

- 6.43.1 Core component handling and storage systems provided at the NPP shall be designed to ensure that the integrity of the core components are maintained at all times during core component handling and storage.
- 6.43.2 The design of the plant shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel.
- 6.43.3 Provision shall be made to verify by suitable means absence of physical connection between control plug & core subassemblies prior to the start of subassembly handling inside reactor vessel to ensure that there is no obstruction to rotatable plug movement.
- 6.43.4 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.
- 6.43.5 Core loading errors during handling of core components shall be prevented by design and administrative procedures. The core loading errors shall give alarms. There shall be a provision to detect the sub-critical reactivity margin of the core and any unacceptable reduction in sub-critical margin against reference assessed values shall lead to stopping of subsequent operations manually.
- 6.43.6 Criticality in fresh and irradiated fuel assembly storage shall be prevented by physical systems or processes, preferably by use of geometrically safe configurations, under all

normal and accident conditions e.g. operator error, flooding, earthquake. The ' $k_{eff}$ ' under worst conditions shall not exceed 0.90. If the design relies on presence of neutron absorbers to ensure sub-criticality, the absorbers shall be fixed permanently in position.

- 6.43.7 Storage capacity of Spent Fuel Storage Bay (SFSB) shall be such that during the life of the plant there shall be enough unused capacity to permit full discharge of one reactor core (i.e. all fuel & other subassemblies that require cooling). In case of common SFSB for a multi-unit plants Site, there shall be enough unused capacity to permit full discharge of at least one reactor core.
- 6.43.8 Sufficient administrative controls shall be planned and counter checking arrangements made, e.g. computer surveillance of the entire handling and storage system. Proper arrangements shall be made in the handling procedures for accounting of various types of subassemblies
- 6.43.9 Provisions shall be made for handling and storage of failed fuel subassembly considering release of radioactivity, fuel-coolant compatibility and decay heat removal. Means for encapsulating failed fuel subassemblies shall be provided outside the reactor vessel in order to limit the spread of radioactive materials. This encapsulation shall allow adequate cooling.
- 6.43.10 The hoisting mechanisms of equipment (such as transfer arm etc.) which handle fuel subassembly shall be single failure proof.
- 6.43.11 Cooling medium shall be compatible with the cladding and fuel. In case of non-compatibility, adequate barrier shall be provided.
- 6.43.12 The component handling and storage systems for non-irradiated fuel subassembly 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 pins/ fuel subassemblies;
  - (e) prevent the dropping of fuel subassemblies in transit;
  - (f) have provision for identification of individual fuel subassembly;
  - (g) provide proper means for meeting the relevant requirements for radiation protection;
  - (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; and
  - (i) all fuel handling machines and storage facilities shall have sufficient shielding to limit radiation exposure of the operating personnel.
- 6.43.13 The component handling and storage systems for irradiated fuel subassembly shall be designed to:

- (a) permit adequate heat removal under all operational states and DBAs and monitoring/assessment of its status in operational states and in accident conditions, including during long term loss of all AC power supplies;
- (b) prevent the damage due to dropping of spent fuel subassembly in transit;
- (c) prevent causing unacceptable handling stresses on fuel elements or fuel subassemblies;;
- (d) prevent the dropping of heavy objects or other potentially damaging objects on the fuel subassemblies;
- (e) permit safe handling and storing of suspected or damaged fuel elements or fuel subassemblies;
- (f) control absorber levels if used for criticality safety;
- (g) facilitate maintenance and decommissioning of the fuel storage and handling facilities;
- (h) facilitate decontamination of fuel handling and storage areas and equipment when necessary;
- (i) accommodate, with adequate margins, all the fuel subassemblies removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel subassemblies of the full reactor core;
- (j) facilitate the removal of fuel from storage and its preparation for off-site transport.
- (k) detect (by radiation monitoring) fuel subassemblies, which exceed allowable decay heat limit during their discharge from main vessel
- (l) permit inspection of irradiated FSA;
- (m) ensure all fuel handling machines and storage facilities shall have sufficient shielding to limit radiation exposure of the operating personnel; and
- (n) prevent sodium aerosol deposits in critical areas of components, that can affect their functioning.

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

- (a) cooling medium shall be compatible with the cladding and fuel. In case of non-compatibility, adequate barrier shall be provided.
- (b) means for controlling the temperature, water chemistry and activity of water in which irradiated fuel is handled or stored.
- (c) means for monitoring and controlling the water level in the SFSB and means for detecting leakage.
- (d) means for preventing draining of water from the pool in the event of a pipe break in cooling/cleaning systems (i.e. anti-siphon measures).
- (e) means for removal and inactivation of sodium sticking to the fuel pins during the transport from a sodium environment to a water pool, in order to prevent fuel damage and for keeping water quality in the pool.
- (f) means for monitoring radiation levels and the air activity concentrations in the SFSB area.
- (g) special provision shall be made for handling and storing of absorber subassemblies having vented type pins and also special subassemblies having vented pins.

6.43.15 For reactors using a sodium vessel for ex-vessel fuel storage, the design shall include the following:

- (a) means for monitoring and controlling the temperature, chemistry and activity of sodium & cover gas in which irradiated fuel is handled or stored.
- (b) means for monitoring and controlling the sodium level in the fuel storage tank and for detecting leakage.
- (c) means for preventing the uncovering of fuel assemblies in the tank in the event of a leakage.
- (d) means for providing adequate heat removal from the fuel and for monitoring its status in operational states and in accident conditions, including during long term loss of all AC power supplies.
- (e) means for preventing sodium freezing to avoid blockage of coolant circulation.

6.43.16 For reactors using a dry storage system for ex-vessel fuel storage, the design shall include the following:

- (a) means to ensure that the spent fuel will remain in a configuration which has been determined to be sub-critical during loading, transfer and storage.
- (b) exclusion of the introduction of a moderator such that consequences likely to result from it (like criticality, effect of sodium-water reaction) due to an internal or external event are eliminated.
- (c) provision to ensure adequate cooling of the subassemblies
- (d) means to facilitate monitoring of the spent fuel containment and detection of containment failures.
- (e) incorporation of containment barriers to prevent the release of radionuclides.
- (f) provision to detect any increase in the radiation field due to degradation of containment or shielding.
- (g) keeping the storage system either below atmospheric pressure to prevent the spread of airborne radionuclides to other areas of the facility or ventilated and filtered in order to maintain concentrations of airborne radionuclides below acceptable levels.

6.43.17 Seismically qualified onsite storage of adequate quantity of water shall be available for decay heat removal from spent fuel stored under water during 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.

## **6H. TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE**

### **6.44 Systems for Treatment and Control of Waste**

6.44.1 Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the NPP to keep the amounts and concentrations of radioactive releases below the authorized limits for discharges and as low as reasonably achievable.

6.44.2 Systems and facilities shall be provided for the management and storage of radioactive waste on the NPP Site for a period of time consistent with the availability of the relevant

disposal option.

- 6.44.3 The design of the plant shall incorporate appropriate features to facilitate the movement, transport and handling of radioactive waste. Consideration shall be given to the provision of access to facilities, and to capabilities for lifting and for packaging.
- 6.44.4 Adequate systems shall be provided for the handling of radioactive solid or concentrated wastes and safely storing them for a reasonable period of time at the Site. Adequate consideration should be given to make provision for handling waste generated during severe accident scenarios.

#### **6.45 Systems for Treatment and Control of Effluents**

- 6.45.1 Systems shall be provided at the NPP for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.
- 6.45.2 Liquid and gaseous radioactive effluents shall be treated at the plant so that exposure to the members of the public due to discharges to the environment is kept within the authorized limits and is as low as reasonably achievable.
- 6.45.3 The design of the plant shall incorporate suitable means to keep the release of radioactive liquids to the environment as low as reasonably achievable and to ensure that radioactive releases remain below the authorized limits.
- 6.45.4 The cleanup equipment for the gaseous radioactive substances shall provide the necessary retention factor to keep radioactive releases below the authorized limits on discharges. Filter systems shall be designed so that their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air.

### **6I. OTHER POWER CONVERSION SYSTEMS**

#### **6.46 Steam Supply System, Feed Water System and Turbine Generators**

- 6.46.1 The design of the steam supply system, feed water system and turbine generators for the NPP 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.
- 6.46.2 The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions.
- 6.46.3 The steam supply system and the feed water systems shall be of sufficient capacity and shall be designed to prevent AOOs from escalating to accident conditions.
- 6.46.4 The turbine generators shall be provided with appropriate protection such as over speed protection and vibration protection, and measures shall be taken to minimize the possible effects of turbine generated missiles including secondary effects on items important to safety.
- 6.46.5 The steam water system design should envisage house load operation of turbine generator

for adequate time.

## **6J. RADIATION PROTECTION**

### **6.47 Design for Radiation Protection**

- 6.47.1 Provision shall be made for ensuring that doses to operating personnel at NPP will be maintained below the prescribed limits and will be kept as low as reasonably achievable.
- 6.47.2 Radiation sources throughout the plant shall be comprehensively identified, and exposures and radiation risks associated with them shall be kept as low as reasonably achievable.
- 6.47.3 The integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.
- 6.47.4 Materials used in the manufacture of SSCs shall be selected to minimize neutron activation of the material as far as is reasonably practicable.
- 6.47.5 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.
- 6.47.6 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 reduced by means of access control and by means of ventilation systems.
- 6.47.7 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 minimized.
- 6.47.8 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.
- 6.47.9 Plant equipment subject to frequent maintenance or manual operation shall be located in areas of low dose rate to reduce the exposure of workers.
- 6.47.10 Facilities shall be provided for the decontamination of operating personnel and plant equipment.
- 6.47.11 Access control provisions (interlocks, turnstiles, and locked gates) and radiation protection 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.
- 6.47.12 In areas where inert gas bearing circuits (argon/nitrogen) are present, provision for monitoring of reduction of oxygen level shall be available to facilitate safety of personnel

entering these areas.

#### **6.48 Radiation Monitoring**

- 6.48.1 Equipment shall be provided at the NPP to ensure that there is adequate radiation monitoring in operational states and DBAs and, as far as is practicable, in DEC's.
- 6.48.2 Fixed area radiation monitors 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.
- 6.48.3 Fixed area monitors shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. These monitors shall provide sufficient information in the control rooms or in the appropriate control position, so that operating personnel can initiate corrective action if necessary.
- 6.48.4 Fixed 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 rooms 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.
- 6.48.5 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.
- 6.48.6 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.
- 6.48.7 Instruments shall be provided for measuring the surface contamination. Radiation monitors (e.g. portable 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.
- 6.48.8 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.
- 6.48.9 Means shall be provided for monitoring the reactor containment atmosphere, primary cover gas, primary coolant leak in interspace between main vessel and safety vessel, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including AOOs, and under accident conditions.

6.48.10 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) possibility of there being any unauthorized routes for radioactive releases.

## **6K. ACCIDENT RESPONSE CAPABILITY FOR UNEXPECTED COMBINATION OF EVENTS**

### **6.49 Diverse and Flexible Accident Response Capability**

6.49.1 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 SFSB cooling.

6.49.2 A diverse and flexible accident response capability, as a part of severe accident management programme shall be maintained with the following strategy:

- (a) use of installed equipment in early phase of accident;
- (b) augment or transition from installed equipment to on-site equipment (mobile or fixed) and consumables to maintain or restore key safety functions, at least up to 7 days.
- (c) obtain off-site support, as needed, until the stable heat removal from the core melt is achieved and maintained by the on-site installed equipment.

### **6.50 Use of Non-Permanent Equipment**

6.50.1 To aid above objective of diverse and flexible accident response capability, the design should also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply, to ensure sufficient water/sodium inventory for long term cooling of fuel (stored in SFSB), ensuring the containment integrity and monitoring essential plant parameters.

6.50.2 No credit for these non-permanent equipment shall be taken in safety assessment of DBAs.

6.50.3 Maintenance and testing programme shall be in place for non-permanent equipment, if located on-site, to ensure their availability.

### **6.51 Ultimate Heat Sink (UHS) Pathways**

Design should aim to ensure survivability of existing pathways to remove decay heat under severe conditions caused by extreme natural events (more severe than those



considered for design, derived from the hazard evaluation for the Site) through diverse and redundant provisions. If the design depends on a single UHS, failure of all the pathways leading to UHS shall be shown to be practically eliminated when subjected to loadings under all possible DEC's, including beyond design basis external events.

#### **6L. INDICATIVE LIST OF SAFETY ENHANCEMENT IN SFR BASED NPPS**

Based on application of minimum requirements, the following provisions may be made in design of SFR based NPPs for safety enhancement. The intention is to push these foreseeable DEC-B scenarios to the realm of "Practically Eliminated Events":

In order to prevent the possibility of Unprotected Loss of Flow Accident (ULOFA) or Unprotected Transient Over Power Accident (UTOPA), the design should envisage incorporation of an additional active feature to prevent uncontrolled withdrawal of absorber rod; and incorporation of a passive shutdown system such as passive drop of hydraulically suspended absorber rod, actuated by loss of flow.

- (a) Due consideration should be given to avoid CCF of main vessel and safety vessel. The design features include separation of support structures for main vessel and safety vessel, and design of safety vessel with leaked sodium against earthquake.

## **ABBREVIATIONS**

AC	Alternating Current
AERB	Atomic Energy Regulatory Board
ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operational Occurrence
AST	Auxiliary Standby Transformer
ATWS	Anticipated Transients Without Scram
CCF	Common Cause Failure
CDA	Core Disruptive Accident
CDF	Core Damage Frequency
DBA	Design Basis Accident
DC	Direct Current
DEC	Design Extension Condition
DEC-A	Design Extension Conditions without core melt
DEC-B	Design Extension Conditions with core melt
DiD	Defence-in- Depth
DSL	Design Safety Limit
EEE	Extreme External Events
EPR	Emergency Plans and Response
FHA	Fire Hazard Analysis
FSA	Fuel Sub-Assembly
IAEA	International Atomic Energy Agency
I & C	Instrumentation and Control
IHX	Intermediate Heat Exchanger
ISI	In Service Inspection
LBB	Leak Before Break
LERF	Large Early Release Frequency
LMFR	Liquid Metal Cooled Fast Reactor
LOOP	Loss of Power
LOFA	Loss of Flow Accident

MCR	Main Control Room
NPP	Nuclear Power Plant
OESC	On-Site Emergency Support Centre
PSA	Probabilistic Safety Assessment
PSI	Pre-Service Inspection
PIE	Postulated Initiating Event
RCB	Reactor Containment Building
RO	Responsible Organisation
SBO	Station Black Out
SCR	Supplementary Control Room
SDS	Shut Down System
SDM	Shutdown Margin
SFC	Single Failure Criterion
SFR	Sodium Cooled Fast Reactor
SFSB	Spent Fuel Storage Bay
SSC	Structures, Systems and Components
TSO	Technical Support Organisation
UHS	Ultimate Heat Sink
ULBC	Ultimate Load Bearing Capacity
ULOFA	Unprotected Loss of Flow Accident
UTOPA	Unprotected Transient Over Power Accident

## REFERENCES

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

## BIBLIOGRAPHY

1. ATOMIC ENERGY REGULATORY BOARD, 'Safety Criteria for Design of Prototype Fast Breeder Reactor', Rev. 4, Mumbai, 2015.
2. COMMISSION OF THE EUROPEAN COMMUNITIES, 'LMFBR Safety Criteria and Guidelines for Consideration in the Design of Future Plants, Report EUR 12669 EN, 1990.
3. ATOMIC ENERGY REGULATORY BOARD, 'Glossary of Terms for Nuclear and Radiation Safety', AERB Safety Glossary, AERB/SG/GLO, AERB, Mumbai, India, 2018.
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standard Series, 'Safety Fundamentals' SF-1, Vienna, 2006
5. ATOMIC ENERGY REGULATORY BOARD, Safety Code on 'Design of Pressurized Heavy Water Based Nuclear Power Plants', AERB/NPP-PHWR/SC/D (Rev.1), Mumbai, 2009.
6. AERB Committee on Severe Accident Management, 'Proposed AERB Design Requirements for Addressing Beyond Design Basis Accidents in Nuclear Power Plants', Report, Mumbai, 2009.
7. ATOMIC ENERGY REGULATORY BOARD, Safety Code on 'Quality Assurance in Nuclear Power Plants', AERB/SG/QA, Mumbai, 2009
8. AERB Committee to Review Safety of Indian Nuclear Power Plants Against External Events of Natural Origin, Report, Mumbai, 2011.
9. AERB-ACNS Committee and Task Force Comments and NPSD Report, 'Safety Criteria for Design of Future Fast Breeder Reactors', Mumbai, 2011.
10. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Standard, Specific Safety Requirements, 'Safety of Nuclear Power Plants: Design', SSR-2/1, 2016
11. CEA- 4th Generation Sodium-Cooled Fast Reactors The Astrid Technological Demonstrator, December, 2012
12. Safety Design Criteria for Generation-IV Sodium-cooled Fast Reactor System, SDC-TF/2013/01, May 1, 2013
13. ATOMIC ENERGY REGULATORY BOARD, Code on 'Site Evaluation of Nuclear Facilities', AERB/NF/SC/S (Rev.1), Mumbai, 2014.
14. ATOMIC ENERGY REGULATORY BOARD, 'Policies Governing Regulation of Nuclear and Radiation Safety', Mumbai, 2014
15. ATOMIC ENERGY REGULATORY BOARD, Safety Code on 'Design of Light Water Reactor Based Nuclear Power Plants', AERB/NPP-LWR/SC/D, Mumbai, 2015.

## **IN-HOUSE WORKING GROUP (IHWG)**

**Dates of Meeting:**      **April 12 - June 2, 2017**

### **Members of IHWG**

Shri S. Harikumar (Convener)	NPSD, AERB
Shri Hemant Kulkarni, Member	NPSD, AERB
Shri Animesh Biswas, Member	NPSD, AERB
Shri Rajnish Kumar, Member	NPSD, AERB
Shri Surendra Jain, Member	NPSD, AERB
Smt. Ananya Mohanty, Member	NPSD, AERB
Shri Suvadip Roy, Member	NPSD, AERB
Shri Rahul Shukla (Member-Secretary)	NPSD, AERB

## TASK FORCE

### Dates of meeting:

August 22, 2017

September 8, 2017

October 4, 2017

October 30 & 31, 2017

November 20, 2017

February 22 & 23, 2018

March 12, 2018

April 19 & 20, 2018

May 29, 2018

May 2 & 3, 2019

July 1, 2022

### Members of Task Force:

Shri K. K. Vaze, Former, BARC	-	Convener
Shri V. Balasubramanian, AERB	-	Co-Convener
Dr. P. Mohanakrishnan, Former, IGCAR	-	Member
Shri S. Raghupathy, IGCAR	-	Member
Shri C. S. Vargese, AERB	-	Member
Shri Sameer Hajela, NPCIL	-	Member
Shri S. Harikumar, AERB	-	Member
Shri Allu Ananth, BHAVINI	-	Member
Shri Y. S. Ramaswamy, BHAVINI	-	Member
Smt. T. Jayanthi, IGCAR	-	Member
Shri K. Devan, IGCAR	-	Member
Shri Hemant Kulkarni, AERB	-	Member
Shri U. K. Paul, AERB	-	Member
Dr. K. Natesan, IGCAR	-	Member
Dr. R. B. Solanki, AERB	-	Member-Secretary

## ADVISORY COMMITTEE ON NUCLEAR AND RADIATION SAFETY (ACNRS)

### Dates of Meetings:

June 9, 2018	February 03, 2022	July 30, 2024
July 14, 2018	March 08, 2022	October 27, 2024
November 17, 2018	July 21, 2022	January 07, 2025
December 29, 2018	September 14, 2023	July 27, 2025
January 20, 2022		October 16, 2025

### Members of ACNRS

Shri S.S.Bajaj (Chairman)	- AERB (Former)
Shri D.K. Shukla	- AERB (Former)
Shri S.B.Chafle	- AERB
Shri Rajesh V. , Director (T), NPCIL	- NPCIL
Shri Jayakrishnan S., Director (T-LWR), NPCIL	- NPCIL
Shri K.V. Suresh Kumar	- BHAVINI
Shri C. S. Varghese	- AERB (Former)
Shri Sanjay Kumar	- NPCIL (Former)
Shri U.C.Muktibodh	- NPCIL (Former)
Dr. M.R.Iyer	- BARC (Former)
Prof. C.V.R.Murthy	- IIT Chennai
Shri S.C.Chetal	- IGCAR (Former)
Shri H.S.Kushwaha	- BARC (Former)
Shri S.K.Ghosh	- BARC (Former)
Shri K.K.Vaze	- BARC (Former)
Dr. N. Ramamoorthy	- BRIT (Former)
Shri A.R. Sundararajan	- AERB (Former)
Shri Atul Bhandakkar	- NPCIL (Former)
Dr. A.N. Nandakumar	- AERB (Former)
Shri A. K Balasubrahmanian	- NPCIL (Former)
Shri V.Rajan Babu	- BHAVINI (Former)
Shri A. Jyothishkumar	- BHAVINI (Former)
Dr. Kallol Roy	- BHAVINI(Former)
Dr. L.R. Bishnoi	- AERB (Former)
Dr. (Smt.) Sadhana Mohan	- BARC (Former)
Shri S.T. Swamy, Member Secretary (Till Jan 2020)	- AERB (Former)
Shri S. Harikumar, Member Secretary (Till Oct 2021)	- AERB(Former)
Shri H.Ansari, Member Secretary(Till Feb 2024)	- AERB(Former)
Shri R.B Solanki, Member Secretary	- AERB



### **TECHNICAL EDITING**

Shri Rajan Babu, Former Director (T), BHAVINI

### **COPY EDITING**

Shri S.T Swamy, Former, Head, DRP&E, AERB

**AERB SAFETY CODE NO. AERB/NPP-SFR/SC/D**

*Published by:* Atomic Energy Regulatory Board,  
Niyamak Bhavan, Anushaktinagar.  
Mumbai – 400 094