



GOVERNMENT OF INDIA

**AERB SAFETY CODE**

**DESIGN OF PRESSURISED  
HEAVY WATER REACTOR BASED  
NUCLEAR POWER PLANTS**



**ATOMIC ENERGY REGULATORY BOARD**

**AERB SAFETY CODE NO. AERB/NPP-PHWR/SC/D (Rev. 1)**

**DESIGN OF PRESSURISED  
HEAVY WATER REACTOR BASED  
NUCLEAR POWER PLANTS**

**Approved by the Board on October 22, 2009**

**Atomic Energy Regulatory Board  
Mumbai-400 094  
India**

**December 2009**

Price

Order for this code should be addressed to:

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

## FOREWORD

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

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

AERB issued a safety code titled 'Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants' (AERB Code No. SC/D) in 1989, to spell out the requirements to be met during design of pressurised heavy water based nuclear power plants in India for assuring safety. This safety code is a revised version and is issued to reflect developments, which have taken place since then. Specifically, more attention is given to management of design, severe accidents, ageing, computer-based safety systems and safety assessment. In drafting the code, the relevant International Atomic Energy Agency (IAEA) documents under the nuclear safety standards (NUSS) programme, especially IAEA safety standards series No. NS-R-1 (2000) on 'Safety of Nuclear Power Plants: Design Requirements' have been used extensively. The principles and objectives stated in this code can be usefully applied to other nuclear power plants. An appendix and references are included to provide information that might be helpful to the user.

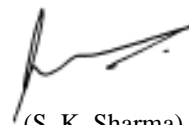
This safety code does not address all requirements for ensuring physical security of the plant or consequences arising from breach of provisions of physical security. As details of this aspect are restricted, they would be dealt with by appropriate authority.

The revised code supersedes the earlier version and applies only for nuclear power plants built after the issue of the document. However during periodic safety review, a review for applicability of the current code for existing power plants would be performed.

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 the applicable provisions of the Factories Act, 1948 and the Atomic Energy (Factories) Rules, 1996.

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

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



(S. K. Sharma)  
Chairman, AERB

## **DEFINITIONS**

### **Acceptable Limits**

Limits acceptable to the regulatory body for accident condition or potential exposure.

### **Accident**

An unplanned event resulting in (or having the potential to result in) personal injury or damage to equipment which may or may not cause release of unacceptable quantities of radioactive material or toxic/hazardous chemicals.

### **Accident Conditions**

Substantial deviations from operational states, which could lead to release of unacceptable quantities of radioactive materials. They are more severe than anticipated operational occurrences and include design basis accidents as well as beyond design basis accidents.

### **Active Component**

A component whose functioning depends on an external input, such as actuation, mechanical movement, or supply of power, and which therefore, influences the system process in an active manner, e.g. pumps, valves, fans, relays and transistors. It is emphasized that this definition is necessarily general in nature as is the corresponding definition of passive component. Certain components, such as rupture discs, check valves, injectors and some solid state electronic devices, have characteristics, which require special consideration before designation as an active or passive component.

### **ALARA**

An acronym for 'As Low As Reasonably Achievable'. A concept meaning that the design and use of sources, and the practices associated therewith, should be such as to ensure that exposures are kept as low as reasonably practicable, with economic and social factors taken into account.

### **Anticipated Operational Occurrences**

An operational process deviating from normal operation, which is expected to occur during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety, nor lead to accident conditions.

### **Atomic Energy Regulatory Board (AERB)**

A national authority designated by the Government of India having the legal authority for issuing regulatory consent for various activities related to the nuclear and radiation facilities and to perform safety and regulatory functions, including enforcement for the protection of site personnel, the public and the environment from undue radiation hazards. (Also called "Regulatory Body")

**Beyond Design Basis Accidents (BDBA)**

Accidents of very low probability of occurrence, more severe than the design basis accidents, those may cause unacceptable radiological consequences; they include severe accidents also.

**Channel (Coolant)**

The primary heat transport coolant tube and accessories through which the reactor coolant flows in a reactor.

**Channel (Instrumentation)**

An arrangement of interconnected components within a system that initiates output (s).

**Commissioning**

The process during which structures, systems and components of a nuclear or radiation facility, on being constructed, are made functional and verified in accordance with design specifications and found to have met the performance criteria.

**Common Cause Failure (CCF)**

The failure of a number of devices or components to perform their functions, as a result of a single specific event or cause.

**Computer-based System**

A system consisting of one or more computers (comprising hardware and software) collectively forming a functional unit of an instrumentation and control system.

**Computer Hardware**

Central processing unit, memory, standard peripherals, peripheral controllers, communication hardware and the power supplies for the above.

**Control System**

A system performing actions needed for maintaining plant variables within prescribed limits.

**Decommissioning**

The process by which a nuclear or radiation facility is finally taken out of operation in a manner that provides adequate protection to the health and safety of the workers, the public and the environment.

**Deflagration**

Vigorous burning with emission of large heat and intense light accompanied by subsonic flame propagation.

**Defence-in-Depth**

Provision of multiple levels of protection for ensuring safety of workers, the public or the environment.

**Design**

The process and results of developing the concept, detailed plans, supporting calculations and specifications for a nuclear or radiation facility.

**Design Basis Accidents (DBAs)**

A set of postulated accidents which are analysed to arrive at conservative limits on pressure, temperature and other parameters which are then used to set specifications to be met by plant structures, systems and components, and fission product barriers.

**Design Basis Threat (DBT)**

The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

**Design Life**

The period for which the item will perform satisfactorily meeting the criteria set forth in the design specification.

**Design Limits**

Limits on the design parameters within which the design of the structures, systems and components of a nuclear facility has been shown to be safe.

**Deterministic Method**

A method for which most of the parameters and their values are mathematically definable and may be explained by physical relationships and are not dependent on random statistical events.

**Detonation**

An exothermic chemical reaction due to combustion of a substance, which propagates through reactive material at supersonic speed.

**Diversity**

The presence of two or more different components or systems to perform an identified function, where the different components or systems have different attributes, so as to reduce the possibility of common cause failure.

**Dose**

A measure of the radiation received or absorbed by a target. The quantities termed absorbed dose, organ dose, equivalent dose, effective dose, committed equivalent dose, or committed effective dose are used, depending on the context. The modifying terms are used when they are not necessary for defining the quantity of interest.

**Engineered Safety Features (ESF)**

The system or features specifically engineered, installed and commissioned in a nuclear



power plant to mitigate the consequences of accident condition and help to restore normalcy, e.g. containment atmosphere clean up system, containment depressurisation system etc..

### **Exclusion Zone**

An area extending upto a specified distance around the plant, where no public habitation is permitted. This zone is physically isolated from outside areas by plant fencing and is under the control of the plant management.

### **Explosion**

An abrupt oxidation or decomposition reaction producing an increase in temperature, or in pressure or in both simultaneously.

### **Exposure**

The act or condition of being subject to irradiation. Exposure can be either external (irradiation by sources outside the body) or internal (irradiation by sources inside the body). Exposure can be classified as either normal exposure or potential exposure; either occupational, medical or public exposure; and in intervention situations, either emergency exposure or chronic exposure. The term 'exposure' is also used in radiation dosimetry to express the amount of ions produced in air by ionising radiation.

### **Fail Safe Design**

A concept in which, if a system or a component fails, then plant/component/system will pass into a safe state without the requirement to initiate any operator action.

### **Fuel Bundle**

An assembly of fuel elements identified as a single unit (also called "Fuel Assembly")

### **Fuel Element**

A component of fuel assembly that consists primarily of the nuclear fuel and its encapsulating materials.

### **Functional Isolation**

Prevention of influences from the mode of operation or failure of one circuit or system on another.

### **Independence**

The ability of equipment, channel or system to perform its function irrespective of the normal or abnormal functioning of any other equipment, channel or system. Independence is achieved by functional isolation and physical separation.

### **Items Important to Safety (IIS)**

The items which comprise:

- those structures, systems, equipment and components whose malfunction or failure could lead to undue radiological consequences at plant site or off-site;

- those structures, systems, equipment and components which prevent anticipated operational occurrences from leading to accident conditions;
- those features which are provided to mitigate the consequences of malfunction or failure of structures, systems, equipment or components.

#### **Level 1 PSA (Nuclear Reactor)**

It evaluates core damage frequency by developing and quantifying accident sequences (event trees) with postulated initiating events together with system unavailability values derived from fault tree analyses with inputs from failure data on components, common causes and human actions.

#### **Level 2 PSA (Nuclear Reactor)**

It takes inputs from Level 1 PSA results and quantifies the magnitude and frequency of radioactive release to the environment following core damage progression and containment failure.

#### **Level 3 PSA (Nuclear Reactor)**

Taking inputs from Level 2 analysis, it evaluates frequency and magnitude of radiological consequences to the public, environment and the society considering meteorological conditions, topography, demographic data, radiological release and dispersion models.

#### **Limiting Conditions for Operation (LCO)**

Conditions that are imposed on operation which are intended to ensure safety during startup, normal operation and shutdown. They also help to avoid reaching the limiting safety system settings and ensure readiness for performing necessary functions in the event of an accident. LCO include limits of operating parameters, requirements of minimum operable equipment of various systems, minimum specified staffing as well as prescribed actions to be taken by operating staff.

#### **Monitoring**

The continuous or periodic measurement of parameters for reasons related to the determination, assessment in respect of structure, system or component in a facility or control of radiation.

#### **Normal Operation**

Operation of a plant or equipment within specified operational limits and conditions. In case of nuclear power plant, this includes start-up, power operation, shutting down, shutdown state, maintenance, testing and refuelling.

#### **Nuclear Power Plant (NPP)**

A nuclear reactor or a group of reactors together with all the associated structures, systems, equipment and components necessary for safe generation of electricity.

### **Nuclear Safety**

The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of site personnel, the public and the environment from undue radiation hazards.

### **Nuclear Security**

All preventive measures taken to minimize the residual risk of unauthorised transfer of nuclear material and/or sabotage, which could lead to release of radioactivity and/or adverse impact on the safety of the plant, plant personnel, public and environment.

### **Operating State**

The state when an entity performs a required function.

### **Physical Protection**

Measures for the protection of nuclear/radiation facility designed to prevent unauthorised access or removal of radioactive material, or sabotage.

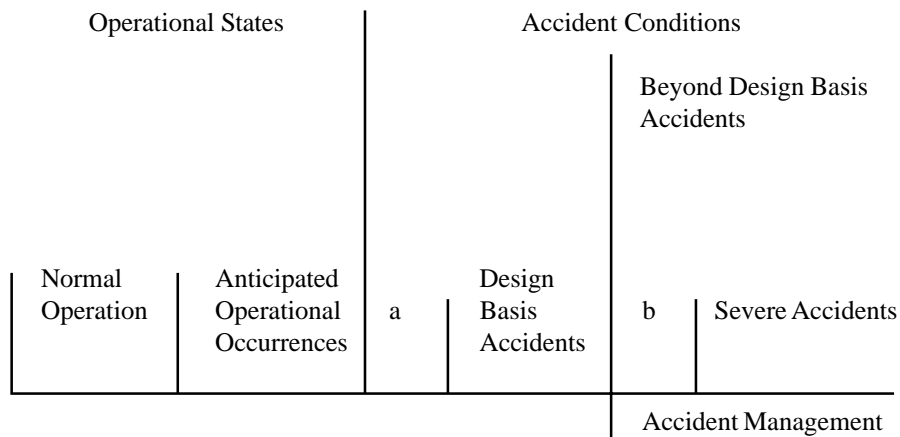
### **Physical Separation**

A means of ensuring independence of equipment through separation by geometry (distance, orientation etc.), appropriate barriers or combination of both.

### **Plant Management**

Members of the site personnel who have been delegated responsibility and authority by the responsible/operating organisation for directing the operation of the plant.

### **Plant States**



a = Accident conditions which are not explicitly considered as design basis accidents, but are enveloped by them.

b = Beyond design basis accidents without significant core degradation.

- Accident conditions include all non-operational states, rather than just design basis accidents and those enveloped by them (marked as 'a');
- The category, marked 'b', of beyond design basis accidents which are not classified as severe accidents because there is no significant core degradation; and
- The term accident management is applied only to beyond design basis accidents, rather than all non-operational states.

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

Identified events during design that lead to anticipated operational occurrences or accident conditions, and their consequential failure effects.

#### **Prescribed Limits**

Limits established or accepted by the regulatory body.

#### **Probabilistic Risk Assessment (PRA)/Probabilistic Safety Assessment (PSA)**

A comprehensive structured approach to identifying failure scenarios constituting a conceptual and mathematical tool for deriving numerical estimates of risk. The term PRA and PSA are interchangeably used.

#### **Protection System**

A part of safety system which encompasses all those electrical, mechanical devices and circuitry, from and (including the sensors) up to the input terminals of the safety actuation system and the safety support features, involved in generating the signals associated with the safety tasks.

#### **Quality Assurance (QA)**

Planned and systematic actions necessary to provide the confidence that an item or service will satisfy given requirements for quality.

#### **Redundancy**

Provision of alternative structures, systems, components of identical attributes, so that any one can perform the required function, regardless of the state of operation or failure of the other.

#### **Regulatory Body**

(See "Atomic Energy Regulatory Board").

#### **Reliability**

The probability that a structure, system, component or facility will perform its intended (specified) function satisfactorily for a specified period under specified conditions.

#### **Residual Heat**

The sum of the time-dependent heat loads originating from radioactive decay and

shutdown fission and heat stored in reactor-related structures and heat transport media in a nuclear reactor facility.

**Responsible Organisation**

An organisation having overall responsibility for siting, design, construction, commissioning, operation and decommissioning of a facility.

**Sabotage (Security)**

Any deliberate act directed against a nuclear/radiation facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances.

**Safety**

(See “Nuclear Safety”)

**Safety Actuation System**

A part of safety system, which encompasses all equipment, required to accomplish the required safety action when initiated by the protection system.

**Safety Analysis Report (SAR)**

A document, provided by the applicant/consentee to the regulatory body containing information concerning the nuclear or radiation facility, its design, accident analysis and provisions to minimize the risk to the public, the site personnel and the environment.

**Safety Assessment**

A review of the aspects of design and operation of a source which are relevant to the protection of persons or the safety of the source, including the analysis of the provisions for safety and protection established in the design and operation of the source and the analysis of risks associated with normal conditions and accident situations.

**Safety Culture**

The assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, the protection and safety issues receive the attention warranted by their significance.

**Safety Function**

A specific purpose that must be accomplished for safety.

**Safety Limits**

Limits upon process variables within which the operation of the facility has been shown to be safe.

**Safety Related Systems**

Systems important to safety which are not included in “Safety Systems”, and which are required for the normal functioning of the safety systems.

**Safety Support System**

Part of safety systems which encompasses all equipment that provide services such as cooling, lubrication and energy supply (pneumatic or electric) required by the protection system and safety actuation systems.

**Safety System**

Systems Important to safety and provided to assure that under anticipated operational occurrences and accident conditions, the safe shutdown of the reactor followed by heat removal from the core and containment of any radioactivity, is satisfactorily achieved. (Examples of such systems are shutdown systems, emergency core cooling system and containment isolation system).

**Safety System Settings**

The levels at which protective devices are automatically actuated in the event of anticipated operational occurrences or accident conditions, so as to prevent safety limits being exceeded.

**Severe Accidents**

Nuclear facility conditions beyond those of the design basis accidents causing significant core degradation.

**Single Failure**

A random failure, which results in the loss of capability of a component to perform its intended safety function. Consequential failures resulting from a single random occurrence are considered to be part of the single failure.

**Site**

The area containing the facility defined by a boundary and under effective control of facility management.

**Software (Computer)**

The set of instructions that make computer hardware perform certain tasks. Programs, operating systems, device drivers and macros are all different kinds of software.

**Source**

Anything that causes radiation exposure, either by emitting ionising radiation or releasing radioactive substances or materials.

**Suppression Pool**

A pool of water located at the lowermost elevation of the reactor building, into which steam resulting from loss of coolant accident /main steam line break is directly led and condensed to reduce the pressure in the primary containment.

**Surveillance**

All planned activities viz. monitoring, verifying, checking including in-service inspection, functional testing, calibration and performance testing carried out to ensure compliance with specifications established in a facility.

**Technical Specifications for Operation**

A document approved by the regulatory body, covering the operational limits and conditions, surveillance and administrative control requirements for safe operation of the nuclear or radiation facility. It is also called as 'Operational Limits and Conditions'.

**Ultimate Heat Sink**

The atmosphere or a body of water or the ground water to which a part or all of the residual heat is transferred during normal operation, anticipated operational occurrences or accident conditions.

**Validation**

The process of determining whether a product or service is adequate to perform its intended function satisfactorily.

**Validation (Computer Code)**

The evaluation of software at the end of the development process to ensure compliance with the user requirements. Validation is therefore 'end-to-end' verification .

**Verification**

The act of reviewing, inspecting, testing, checking, auditing, or otherwise determining and documenting whether items, processes, services or documents conform to specified requirements.

**Verification (Computer Code)**

The process of determining that the controlling physical and logical equations have been correctly translated into computer code.

## **SPECIAL DEFINITIONS** (Specific to the Present Code)

### **Accident Management**

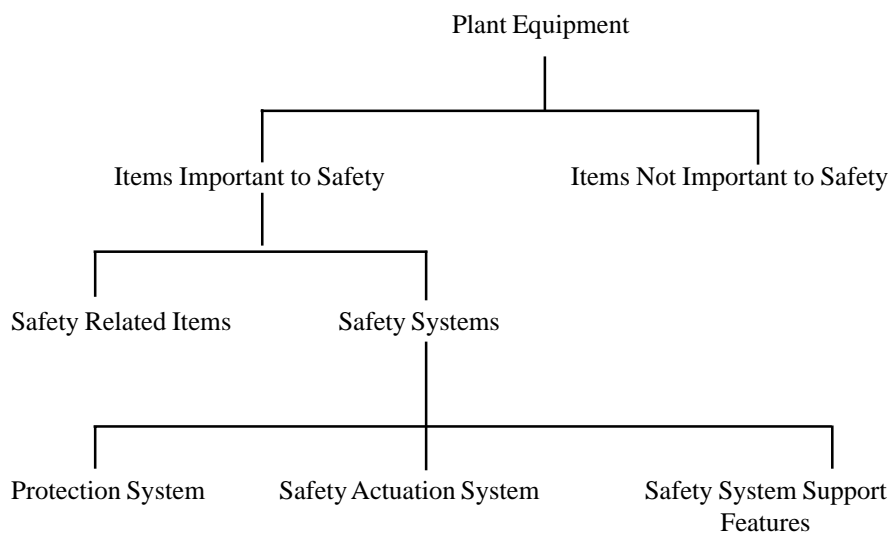
The taking of a set of actions during the evolution of a beyond design basis accident:

- to prevent the escalation of the event into a severe accident;
- to mitigate the consequences of a severe accident; and
- to achieve a long term safe stable state.

### **Passive Component**

A component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power. A component which has no moving part and only experiences a change in process parameters such as pressure, temperature, or fluid flow in performing its functions. In addition, certain components, which function with very high reliability, based on irreversible action or change, may be assigned to this category (examples of passive components are heat exchangers, pipes, vessels, electrical cables, and structures. Certain components, such as rupture discs, check valves, injectors and some solid-state electronic devices have characteristics, which require special consideration before designation as an active or passive component).

### **Plant Equipment**





**Safety Chain**

The assembly of equipment designated to perform all actions required for a particular PIE to ensure that the limits specified in the design basis for the anticipated operational occurrences and design basis accidents are not exceeded.

**Safety Group**

The assembly of equipment designated to perform all actions required for a particular postulated initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded.

## CONTENTS

FOREWORD .....	i
DEFINITIONS .....	iii
SPECIAL DEFINITIONS .....	xiii
1. INTRODUCTION .....	1
1.1 General .....	1
1.2 Objective .....	1
1.3 Scope .....	1
1.4 Structure .....	2
2. SAFETY OBJECTIVES AND CONCEPTS .....	3
2.1 Safety Objectives .....	3
2.2 Safety Analysis .....	4
2.3 Defence in Depth .....	5
3. REQUIREMENTS FOR MANAGEMENT OF SAFETY .....	8
3.1 Responsibilities in Management .....	8
3.2 Design Management .....	8
3.3 Proven Engineering Practices .....	9
3.4 Operational Experience and Safety Research .....	9
3.5 Safety Assessment and Independent Verification .....	9
3.6 Quality Assurance .....	10
4. PRINCIPAL TECHNICAL REQUIREMENTS .....	11
4.1 Defence in Depth Requirements .....	11
4.2 Safety Functions .....	12
4.3 Accident Prevention and Plant Safety Characteristics .....	12
4.4 Radiation Protection and Acceptance Criteria .....	13
5. PLANT DESIGN REQUIREMENTS .....	14
5.1 Safety Classification .....	14
5.2 General Design Basis .....	14
5.2.1 Categories of Plant States .....	15
5.2.2 Postulated Initiating Events .....	15
5.2.3 Design Limits .....	15
5.2.4 Internal Events .....	15
5.2.5 External Events .....	17
5.2.6 Site-related Characteristics .....	18
5.2.7 Combination of Events .....	18
5.2.8 Design Criteria .....	18

	5.2.9	Operational States .....	18
	5.2.10	Design Basis Accidents .....	19
	5.2.11	Severe Accidents .....	20
5.3		Design for Reliability of Structures, Systems and Components .....	20
	5.3.1	Common Cause Failures .....	21
	5.3.2	Single Failure Criterion .....	21
	5.3.3	Fail-safe Design .....	22
	5.3.4	Safety Support Systems .....	22
	5.3.5	System Storage Capacities .....	22
	5.3.6	Equipment Outages .....	22
5.4		Materials .....	23
5.5		Provision for In-Service Testing, Maintenance, Repair, Inspection and Monitoring .....	23
5.6		Equipment Qualification .....	24
5.7		Ageing .....	24
5.8		Human Factor .....	25
	5.8.1	Design for Optimised Operator Performance .....	25
5.9		Other Design Considerations .....	26
	5.9.1	Sharing of Structures, Systems and Components in Multi-reactor Nuclear Power Plants .....	26
	5.9.2	Power Plants Used for Cogeneration, Heat Generation or Desalination .....	26
	5.9.3	Fuel and Radioactive Waste Transport and Packaging .....	27
	5.9.4	Escape Routes and Means of Communication	27
	5.9.5	Control of Access .....	27
	5.9.6	System Interaction .....	28
	5.9.7	Electrical Grid-plant Interaction .....	28
	5.9.8	Decommissioning .....	28
5.10		Safety Analysis .....	28
	5.10.1	Deterministic Approach .....	29
	5.10.2	Probabilistic Approach .....	30
	5.10.3	Safety Analysis Report .....	31
6.		PLANT SYSTEM DESIGN REQUIREMENTS .....	32
	6.1	Reactor Core and Associated Features .....	32
	6.1.1	General Design .....	32
	6.1.2	Core Components .....	32
	6.1.3	Fuel Elements and Bundles .....	32
	6.1.4	Reactor Core Control .....	33
	6.1.5	Reactor Shutdown .....	34

6.2	Moderator System .....	35
6.3	Reactor Coolant System .....	36
	6.3.1 Design .....	36
	6.3.2 In-service Inspection of the Reactor Coolant Pressure Boundary .....	37
	6.3.3 Reactor Coolant Inventory .....	38
	6.3.4 Clean-up of the Reactor Coolant .....	38
	6.3.5 Residual Heat Removal from the Core .....	39
	6.3.6 Emergency Core Cooling .....	39
	6.3.7 Inspection and Testing of the Emergency Core Cooling System .....	39
	6.3.8 Auxiliary Feed Water System .....	40
	6.3.9 Fuelling System .....	40
6.4	Ultimate Heat Sink and Associated Systems .....	41
	6.4.1 Heat Transfer to an Ultimate Heat Sink .....	41
	6.4.2 Inspection and Testing .....	41
6.5	Civil Structures and Containment System .....	42
	6.5.1 Design .....	42
	6.5.2 Strength of the Containment Structure .....	43
	6.5.3 Containment Proof Tests .....	43
	6.5.4 Containment Leakage .....	43
	6.5.5 Containment Penetrations .....	44
	6.5.6 Containment Isolation .....	44
	6.5.7 Containment Testing and Inspection .....	45
	6.5.8 Containment Airlocks .....	45
	6.5.9 Pressure Suppression System .....	45
	6.5.10 Internal Structures of the Containment .....	45
	6.5.11 Containment Heat Removal .....	46
	6.5.12 Control and Clean-up of the Containment Atmosphere .....	46
	6.5.13 Coverings and Coatings .....	47
6.6	Instrumentation and Control .....	47
	6.6.1 General Requirements for Instrumentation and Control (I&C) Systems Important to Safety .....	47
	6.6.2 Periodic Testing and Maintenance .....	47
	6.6.3 Instrument Power Supply System .....	48
	6.6.4 Control Room .....	48
	6.6.5 Backup Control Room .....	48
	6.6.6 Use of Computer in Systems Important to Safety .....	49
	6.6.7 Automatic Control .....	49
	6.6.8 Protection System Functions .....	49

6.7	Emergency Control Centre .....	51
6.8	Electrical Power System .....	52
6.8.1	General Requirements .....	52
6.8.2	Off-site Power System .....	52
6.8.3	Emergency Power Supply System .....	52
6.8.4	Inspection of Emergency Power Supply Systems .....	52
6.9	Radioactive Waste Treatment and Controls Systems ...	53
6.9.1	Radioactive Waste Treatment .....	53
6.9.2	Control of Release of Radioactive Liquid Effluents to the Environment .....	53
6.9.3	Control of Airborne Radioactive Substances .	54
6.10	Fuel Handling and Storage Systems .....	54
6.10.1	New Fuel Handling and Storage .....	54
6.10.2	Spent Fuel Handling .....	54
6.11	Radiation Protection .....	55
6.11.1	General Requirements .....	55
6.11.2	Design for Radiation Protection .....	55
6.11.3	Radiation Monitoring .....	57
APPENDIX:	LIST OF SAFETY FUNCTIONS .....	58
REFERENCES	.....	60
LIST OF PARTICIPANTS	.....	61
WORKING GROUP	.....	61
ADVISORY COMMITTEE ON CODES, GUIDES AND ASSOCIATED MANUALS FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD) .....		62
ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS) .....		63
PROVISIONAL LIST OF SAFETY CODES, GUIDES AND MANUALS ON DESIGN OF PRESSURISED HEAVY WATER REACTOR BASED NUCLEAR POWER PLANTS .....		64

# 1. INTRODUCTION

## 1.1 General

1.1.1 The design safety code describes design requirements for structures, systems and components important to safety that shall be met for safe operation, and for the prevention or mitigation of the consequences of events that could jeopardise safety.

1.1.2 In order to supplement mandatory and recommendatory requirements for safety outlined in this design safety code, a series of guides on design for safety, which elaborate ways and means to achieve safety have been prepared<sup>1</sup>.

## 1.2 Objective

1.2.1 The safety code lays down mandatory nuclear safety requirements that define the elements necessary to ensure safety. These requirements are applicable to safety functions and the associated structures, systems and components (SSC), as well as to procedures important to safety in nuclear power plants.

1.2.2 This safety code is expected to aid organisations responsible for design and regulation.

## 1.3 Scope

1.3.1 The safety code establishes requirements for structures, systems and components important to safety that must be met for safe operation of nuclear power plants and for preventing or mitigating the consequences of events that could jeopardise safety. It also establishes requirements for a comprehensive safety assessment, which is carried out in order to identify the potential hazards that may arise from the operation of the plant, under various plant operational states and accident conditions. The safety assessment process includes the complementary techniques of deterministic safety analysis and probabilistic safety analysis (PSA). These analyses necessitate consideration of postulated initiating events (PIEs), which include many factors that, singly or in combination, may affect safety and which may:

- (i) originate in the operation of the nuclear power plant itself,
- (ii) be caused by human action, and
- (iii) be directly related to nuclear power plant and its environment.

---

<sup>1</sup> Reference to these safety guides is made as footnotes to applicable paragraphs of this safety code.

- 1.3.2 This safety code also addresses other events that are very unlikely to occur, such as severe accidents that may result in large radioactive releases, and for which it may be appropriate and practicable to provide preventive and/or mitigating measures by way of design features and complementary procedures.
- 1.3.3 This safety code does not address:
- (i) certain natural or man induced events which are extremely unlikely such as impact of meteorite or artificial satellite;
  - (ii) accidents of a conventional industrial safety nature that under no circumstances could affect the safety of the nuclear power plant;
  - (iii) the non-radiological effects of nuclear power plants on the environment, which may be subject to separate regulatory requirements.

#### **1.4 Structure**

- 1.4.1 There is a hierarchical relationship between safety objectives, safety criteria and safety requirements. This code follows this relationship.

Section 2 covers the safety philosophy which should be applied in the design of the plant and establishes the basis, in terms of objectives and concepts, for deriving the requirements to be applied.

Section 3 covers the principal requirements to be followed by the design organisation in the management of the design process. It also includes requirements for safety assessment, quality assurance and the use of proven engineering practices and operational experience.

Section 4 provides the principal and more general technical requirements for implementation of defence in depth and radiation protection.

Section 5 provides general plant design requirements which supplement the principal requirements to assure that the safety objectives and principles are met.

Section 6 provides the plant system design requirements that are applicable to specific plant systems, such as the reactor core, coolant systems and containment systems.

## 2. SAFETY OBJECTIVES AND CONCEPTS

### 2.1 Safety Objectives

2.1.1 There are four fundamental safety objectives, from which the safety principles and requirements for minimising the risks associated with nuclear power plants are derived. They are:

(a) General nuclear safety objective

To protect individual, society and the environment from harmful radiological hazards due to nuclear installations by establishing and maintaining effective defences against these hazards.

This general nuclear safety objective is supported by two complementary safety objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionising radiation.

(b) Radiation protection objective

To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable (ALARA), and to ensure mitigation of the radiological consequences of any accidents.

(c) Technical safety objective

To take all reasonably practicable measures to:

- (i) prevent accidents in nuclear installations and mitigate their consequences, should they occur;
- (ii) ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be below prescribed limits; and
- (iii) ensure that the likelihood of accidents with serious radiological consequences is extremely low and below acceptable limits.

(d) Nuclear security objective

- (i) To minimise the risk of unauthorised removal of radioactive material and nuclear material,
- (ii) To minimise sabotage on nuclear power plants, and
- (iii) To minimise the risk of adverse impact during the above acts.



- 2.1.2 Safety objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. However, the radiation protection objective does not preclude limited exposure of people or the release of permitted quantities of radioactive materials to the environment from reactor installations. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards<sup>2</sup>.
- 2.1.3 Meeting these four safety objectives requires that, in the design of a nuclear installation, all actual and potential sources of radiation exposure be identified and properly considered, and provision be made to ensure that sources are kept under strict technical and administrative control.

## **2.2 Safety Analysis**

- 2.2.1 It is essential in designing a nuclear power plant, that a comprehensive safety analysis is carried out to evaluate the radiation doses that could be received by workers at the installation and the public, as well as the potential effects on the environment.

The safety analysis shall, therefore, be carried out for all plant states which cover:

- (i) all planned normal operations;
  - (ii) plant performance under anticipated operational occurrences;
  - (iii) design basis accidents (DBA); and
  - (iv) event sequences that may lead to severe accidents.
- 2.2.2 From this analysis, the robustness of the engineering design to withstand postulated initiating events and accidents can be established, the effectiveness of the safety systems and safety related items or systems demonstrated, and requirements for emergency response prepared.
- 2.2.3 Although measures are taken to control radiation exposure in all operational states to levels as low as reasonably achievable (ALARA) and to minimise the likelihood of an accident that might lead to the loss of normal control of the source of radiation, there is a residual probability that an accident may happen. Measures are, therefore, required to ensure that the radiological consequences are mitigated. Such measures include engineered safety features; on-site accident management procedures established by the operating

---

<sup>2</sup> Refer AERB safety guide on 'Radiation Protection Aspects in Design for Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/NPP-PHWR/SG/D-12).

organisation; and off-site intervention measures, when required, as established by appropriate authorities in order to mitigate radiation exposure when an accident occurs.

- 2.2.4 Safe design of a nuclear power plant should follow the principle that plant conditions resulting in high radiation doses or radioactive releases are of very low probability (likelihood) of occurrence and plant conditions with significant probability (likelihood) of occurrence have only minor or no radiological consequences<sup>2</sup>. An essential objective is that external intervention measures required may be limited or even eliminated from a technical point of view, although such measures may still be required by national authorities.
- 2.2.5 Off-site services, upon which safety of the plant and protection of the public may depend, shall be planned and co-ordinated with public authorities. This may include among others, supply of cooling water for ultimate heat sink, fire fighting, means of communication and transport, emergency preparedness, etc..

### **2.3 Defence in Depth**

- 2.3.1 The concept of defence in depth is applied to all safety activities, whether organisational, behavioural or design related, to ensure that they are subject to overlapping provisions, so that if failure should occur, it would be detected and then compensated for or corrected by appropriate measures. The implementation of defence in depth, throughout design and operation, provides a graded protection under various plant states, including those resulting from equipment failures or human action within the plant, and events that originate outside the plant.
- 2.3.2 A relevant aspect of defence in depth is the provision in the design of a series of physical barriers to confine the radioactive material within specified locations. The number of physical barriers required is a function of the potential internal and external hazards, and the potential consequences of failures. The barriers are in the form of the fuel matrix, the fuel cladding, the reactor coolant system pressure boundary and the containment.
- 2.3.3 The application of the concept of defence in depth to the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. For the sake of completeness, each level is described in the following paragraphs:
  - (i) The aim of the first level of defence is to prevent deviation from normal operation, and prevent system failures. This requires that the plant be robustly and conservatively designed, constructed, maintained and operated in accordance with appropriate safety classification and engineering practices, such as the use of redundancy, independence

and diversity. To meet this objective, careful attention is paid to the selection of appropriate design codes and materials, to the control of construction including manufacture of components and to the plant construction. Design options that can contribute to reduce the potential for internal hazards<sup>3</sup>, reduce the consequences of a given PIE, or reduce the likely release source term following an accident sequence contribute at this level of defence. Attention is also given to procedures involved during the design, construction including manufacture and in-service plant inspection, maintenance and testing, to the ease of access for these activities, to the way the plant is operated and to how operational experience is utilised. This whole process is supported by a detailed analysis, which determines the operational and maintenance requirements for the plant.

- (ii) The aim of the second level of defence is to detect and intercept deviations from normal operating conditions in order to prevent anticipated operational occurrences from escalating to accident conditions. This is in recognition of the fact that some PIEs are likely to occur during the service life of a nuclear power plant, despite the care taken to prevent them. This level requires the provision of specific systems identified in the safety analysis and the definition of operating procedures to prevent or minimize damage from such PIEs.
- (iii) The third level of defence is provided to control the consequences of design basis accident should they occur. It is assumed that although very unlikely, the escalation of certain anticipated operational occurrences or PIEs may not be arrested by a preceding level and a more serious event may develop. These unlikely events are anticipated in the design basis for the plant, and inherent safety features, fail-safe design, additional equipment and procedures are provided to control their consequences and to achieve stable and acceptable conditions following such accidents. This requires provision of engineered safety features that are capable of leading the plant first to a controlled state, and subsequently to a safe shutdown state, and maintaining at least one barrier for the confinement of radioactive material.
- (iv) The aim of the fourth level of defence is to address consequences of severe accidents<sup>4</sup>, should they occur, in which the design basis event may have been exceeded and to ensure that radioactive releases are

---

3 e.g. controlling the response during and following a PIE.

4 e.g. loss of coolant accident (LOCA) plus failure emergency core cooling system (ECCS) plus loss of moderator.

kept as low as practicable. The most important objective of this level is the protection of the confinement function. This may be achieved by the application of best estimate approaches, by complementary measures and procedures to prevent accident progression, and by mitigation of the consequences of severe accidents, in addition to accident management procedures.

- (v) The fifth level of defence is aimed at mitigation of the radiological consequences of potential releases of radioactive materials to the environment that may result from accident conditions and severe accidents<sup>5</sup>. This requires the provision of an adequately equipped emergency control centre, and plans for the on-site and off-site emergency response.

---

5 e.g. LOCA plus ECCS failure and failure of one set of containment isolation dampers to close.

### **3. REQUIREMENTS FOR MANAGEMENT OF SAFETY**

#### **3.1 Responsibilities in Management**

- 3.1.1 The responsible organisation shall ensure that safety is given highest priority and the current state-of-art for safety is taken into account. It shall also ensure fulfillment of regulatory requirements and requirements of quality assurance programme. Also, implication of any design change on safety shall be considered. In order to achieve these, the design organisation shall:
- (i) implement all regulatory safety policies;
  - (ii) have a clear division of responsibilities with corresponding lines of authority and communication;
  - (iii) ensure that it has sufficient technically qualified and appropriately trained staff at all levels;
  - (iv) establish clear interfaces between the groups engaged in different parts of the design, and between designers, utilities, suppliers, constructors and contractors as appropriate;
  - (v) develop and strictly adhere to sound procedures;
  - (vi) review, monitor and audit all safety related design aspects on a regular basis;
  - (vii) ensure that a safety culture is maintained;
  - (viii) consider operational and other feedback into design; and
  - (ix) design verification.

#### **3.2 Design Management**

- 3.2.1 The design management shall ensure that the requirements of the responsible organisation are met, and that due consideration is given to the human performance, capabilities and limitations of personnel, who will eventually operate the plant. The design organisation shall supply adequate safety design information to ensure safe operation and maintenance of the plant and to allow subsequent plant modifications to be made, and recommend practices for incorporation into the plant administrative and operational procedures (i.e. operational limits and conditions).
- 3.2.2 The design management shall take account of the results of the deterministic and complementary probabilistic safety analyses, as appropriate; so that an iterative process takes place which ensures that due consideration has been given to the prevention of accidents and mitigation of their consequences.
- 3.2.3 The design management shall ensure that the generation of radioactive waste is kept to the minimum practicable, in terms of both activity and volume, by appropriate design measures and operational and decommissioning practices.

### **3.3 Proven Engineering Practices**

- 3.3.1 Wherever feasible, structures, systems and components important to safety shall be designed according to the latest or currently applicable standards and current international practices acceptable to regulatory body; shall be of a design proven in previous equivalent applications; and shall be selected to be consistent with the plant reliability goals required for safety. Where codes and standards are used as design rules, they shall be identified and evaluated to determine their applicability, adequacy and sufficiency and shall be supplemented or modified as necessary to ensure that the final quality is commensurate with the required safety function.
- 3.3.2 Where a first-of-its-kind design or feature<sup>6</sup>, is introduced or there is a departure from an established engineering practice, safety shall be demonstrated to be adequate by appropriate supporting research programmes, or by examining operational experience from other relevant applications. The development shall also be adequately tested before being brought into service and monitored during service, to verify that the expected behaviour is achieved.
- 3.3.3 In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes<sup>7</sup>. Where failure of a system or component has to be expected and accommodated by the design, preference shall be given to equipment that exhibits a predictable and revealed mode of failure and facilitates repair or replacement.

### **3.4 Operational Experience and Safety Research**

- 3.4.1 The design shall take due account of relevant operational experience that has been gained in operating plants in the country and outside and of the results of relevant research programmes.

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

- 3.5.1 A comprehensive safety assessment shall be carried out to confirm that the design, as used for construction and as built, meets the safety requirements set out at the beginning of the design process.
- 3.5.2 The safety assessment shall be part of the design process, with iteration between the design and confirmatory analytical activities, and increasing in the scope and level of detail as the design programme progresses.
- 3.5.3 The basis for the safety assessment shall be data derived from the safety analysis, previous operational experience, results of supporting research and proven engineering practice.

---

6 e.g. computer-based systems and liquid zone control system (LZCS).

7 e.g. failure to trip when required.

- 3.5.4 The responsible organisation shall ensure that an independent verification of design and the safety assessment is performed by an independent group, separate from that carrying out the design, before it is submitted to the regulatory body.
- 3.5.5 Aspects of design, having implications on operability, shall be reviewed by the responsible organisation. The merits in developing such a methodology include acceptance of the design by responsible organisation for ensuring proper operation, maintainability, layout, inspectability etc. in the new designs. An agreed methodology must be arrived at for implementing this clause.
- 3.6 Quality Assurance**
- 3.6.1 A quality assurance programme that describes the overall arrangements for the management, performance and assessment of the plant design shall be prepared and implemented. 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. Further details are given in AERB safety code 'Quality Assurance in Nuclear Power Plants' (AERB/SC/QA, Rev. 1)<sup>8</sup> [6].
- 3.6.2 Design, including subsequent changes or safety improvements, shall be carried out in accordance with established procedures that call on appropriate engineering codes and standards, and shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled.
- 3.6.3 The adequacy of design, including design tools and design inputs and outputs, shall be verified or validated by individuals or groups separate from those who originally performed the work. Verification, validation and approval shall be completed before implementation of the detailed design.
- 3.6.4 Necessary records of design, fabrication, inspection, erection, testing and maintenance of structures, systems and components shall be maintained throughout the life of the plant as per procedures outlined in the AERB quality assurance code [6] at the plant site by the plant management of the operating organisation/responsible organisation.

---

<sup>8</sup> Also refer AERB safety guide on 'Quality Assurance in the Design of Nuclear Power Plants' (AERB/SG/QA-1).

## 4. PRINCIPAL TECHNICAL REQUIREMENTS

### 4.1 Defence in Depth Requirements

- 4.1.1 The design process shall incorporate defence in depth as described in section 2. The design shall comply with the requirements so as to ensure that during normal operation prescribed limits and during accident conditions acceptable limits are not exceeded. The design therefore shall provide:
- (i) multiple physical barriers to the uncontrolled release of radioactive materials to the environment;
  - (ii) conservatism and high construction quality, so as to provide confidence that plant failures and deviations from normal operations are minimised and accidents prevented;
  - (iii) for control of the plant behaviour during and following a PIE, using inherent and engineered features, i.e. uncontrolled transients shall be minimised or excluded by design to the extent possible;
  - (iv) for supplementing control of the plant by the use of automatic actuation of safety systems in order to minimise operator actions in the early phase of PIEs. However, operator action in early phase of PIE may be permitted provided enough information is available for operator actions;
  - (v) for equipment and procedures to control the course and limit the consequences of accidents as far as practicable; and
  - (vi) multiple means for ensuring that each of the fundamental safety functions, i.e. control of the reactivity, adequate heat removal and confinement of radioactive materials is performed, thereby ensuring the effectiveness of the barriers or mitigating the consequences of any PIEs.
- 4.1.2 To ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable:
- (i) challenges to the integrity of physical barriers;
  - (ii) failure of a barrier when challenged; and
  - (iii) failure of a barrier as a consequence of failure of another barrier.
- 4.1.3 The design shall be such that the first, or at most the second, level of defence is capable of preventing accident conditions for all but the most improbable PIEs.
- 4.1.4 The design shall take into account the fact that the existence of multiple levels of defence is not sufficient basis for continued power operation in the absence



of one level of defence. All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.

## **4.2 Safety Functions**

4.2.1 The objective of the safety approach shall be to provide adequate means to maintain the plant in a normal operational state, to ensure proper short term response immediately following a PIE and to facilitate the management of the plant, during and following any design basis accident, and following the plant conditions beyond the design basis that are considered.

4.2.2 To ensure safety, the following fundamental safety functions<sup>9</sup> shall be performed in all operational states, during and following design basis accidents and, to the extent practicable, on occurrence of the selected beyond design basis accidents (BDBAs)<sup>10</sup> also:

- (i) control of the reactivity;
- (ii) adequate heat removal from the core; and
- (iii) confinement of radioactive materials and control of operational discharges within prescribed limit, as well as to limit accidental releases within acceptable limits.

An example of a detailed subdivision of these three fundamental safety functions<sup>9</sup> is given in the appendix.

4.2.3 A systematic approach shall be followed to identify the systems, structures and components that are required to fulfill the safety functions at various times following a PIE.

## **4.3 Accident Prevention and Plant Safety Characteristics**

4.3.1 The plant design shall be such that its sensitivity to PIEs is minimised. The expected plant response to any PIE shall be those of the following that can reasonably be achieved in following order of importance:

- (i) A PIE produces no significant safety related effect or produces only a change in the plant towards a safe condition by inherent characteristics; or
- (ii) Following a PIE, the plant is rendered safe by passive features or by the action of safety-related systems that are continuously operational in the state required to control the effect of PIE; or

---

<sup>9</sup> Refer AERB safety guide on 'Safety Classifications and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-1).

<sup>10</sup> Analysis is required for BDBAs within the frequency range of  $10^{-6}$  to  $10^{-7}$ /reactor-year.

- (iii) Following a PIE, the plant is rendered safe by the action of safety systems that need to be brought into service in response to the PIE;  
or
- (iv) Following a PIE, the plant is rendered safe by specified procedural actions.

#### **4.4 Radiation Protection and Acceptance Criteria**

- 4.4.1 Measures shall be provided to ensure that radiation protection and technical safety objectives, as given in paras 2.1.1, are achieved; and that radiation doses to the public and to site personnel during all operational states, including maintenance and decommissioning, do not exceed prescribed limits and are as low as reasonably achievable.
- 4.4.2 The design shall have as an objective the prevention of accidents and, if this fails, the mitigation of radiation exposures from accident conditions. Design provisions shall be made to ensure that potential radiation doses to the public and the site personnel do not exceed acceptable limits and are as low as reasonably achievable.
- 4.4.3 Events shall be categorised based on likelihood of occurrence<sup>11</sup>. All events belonging to a category having higher likelihood of occurrence shall have lower permissible consequences in terms of doses at the exclusion zone boundary<sup>2, 12</sup>.

---

11 Refer AERB safety guide on 'Design Basis Events in Pressurised Heavy Water Reactors' (AERB/SG/D-5).

12 Refer AERB safety guide on 'Intervention Levels and Derived Intervention Levels for Off-site Radiation Emergency' (AERB/SG/HS-1).

## 5. PLANT DESIGN REQUIREMENTS

### 5.1 Safety Classification

- 5.1.1 All structures, systems and components, including software for instrumentation and control (I&C), that are important to safety, shall be identified and classified on the basis of their function and significance with regard to safety<sup>4</sup>. They shall be designed, constructed and maintained such that their quality and reliability is commensurate with this classification. The applicable codes and standards for design, manufacture, inspection, erection and testing and in-service inspection of all these structures, systems and components should be identified.
- 5.1.2 The method for classifying the safety significance of structures, systems or components shall primarily be based on deterministic methods, complemented where appropriate by probabilistic methods and engineering judgment, with account taken of factors<sup>9</sup>, such as the:
- (i) safety function(s) to be performed by the item;
  - (ii) probability that it will be called upon to perform a safety function;
  - (iii) time following the initiation of a PIE at which, or the period throughout which, it will be called upon to perform safety function; and
  - (iv) consequences of its failure to perform its function.
- 5.1.3 Appropriately designed interfaces shall be provided between structures, systems and components of different safety classes to ensure that any failure in a system classified in a lower safety class does not propagate to a system classified 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 lower design pressure from being exceeded, on the assumption of a single failure.

### 5.2 General Design Basis

The design basis shall specify the necessary capabilities of the plant to cope with a specified range of all plant states up to design basis accidents within the defined radiological protection requirements. The design basis shall typically include the specifications for normal operation, conditions created by the PIEs, the safety classification, important assumptions and, in some cases, the particular methods of analysis.

Conservative design measures shall be applied and sound engineering practices shall be adhered 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 and will be ALARA.

The design shall also address the behaviour of the plant under specified beyond design basis accidents including selected severe accidents (Ref. clause 5.2.11). The assumptions and methods used for these evaluations may be on a best estimate basis.

#### 5.2.1 Categories of Plant States

The plant states shall be identified and grouped into a limited number of categories according to their probability of occurrence<sup>11</sup>. The categories typically cover normal operation, anticipated operational occurrences, design basis accidents and severe accidents. Acceptance criteria shall be assigned to each category that take account of the requirement that frequent PIEs shall have only minor or no radiological consequences, and that events that may result in severe consequences shall be of very low probability.

#### 5.2.2 Postulated Initiating Events

In designing the plant, it shall be recognised that challenges to all levels of defence in depth may occur and design measures shall be provided to ensure that the required safety functions are accomplished and the safety objectives can be met. These challenges stem from the PIEs, which are selected on the basis of deterministic or probabilistic considerations or a combination of the two independent events, each having a low probability, are normally not considered to occur simultaneously<sup>11</sup>.

#### 5.2.3 Design Limits

A set of design limits consistent with the key physical parameters for each structure, system or component shall be specified for operational states and accident conditions. Specific mention may be made of limits on fuel design, structural design, pressure, temperature, radiation exposure and functional requirements etc.

#### 5.2.4 Internal Events

An analysis of PIEs shall be made to establish all those internal events which may affect the safety of the plant. The events may include equipment failures or maloperation.

##### 5.2.4.1 Fire and Explosion

- (a) Consistent with other safety requirements, structures, systems and components important to safety shall be designed and located to minimise the probability and effects of fire and explosions caused by

external or internal events. The capability for shutdown, residual heat removal, confinement of radioactive material and monitoring the state of plant in the case of fire and explosion shall be established and maintained. These requirements shall be achieved by suitable incorporation of redundant parts, diverse systems, physical separation, and design for fail-safe operation such that the following objectives are achieved:

- (i) preventing fires from starting;
  - (ii) detecting and extinguishing quickly those fires which do start, thus limiting the damage;
  - (iii) preventing the spread of those fires which have not been extinguished, thus minimising their effect on essential plant functions.
- (b) 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<sup>13</sup>.
  - (c) A fire hazard analysis of the plant shall be carried out to determine the required rating of the fire barriers, and the required capability of fire detection and fire fighting systems shall be provided.
  - (d) Fire fighting systems shall be automatically initiated where necessary, and systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of structures, systems and components important to safety, and does not simultaneously affect redundant safety chains, thereby challenging compliance with the single failure criterion.
  - (e) Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, particularly in locations such as the containment and control room.

#### 5.2.4.2 Other Internal Events

The potential for internal hazards such as flooding, missile generation, pipe whip, jet impingement, and fluid release from failed systems or other plant on the site shall be taken into account in the design of the plant. Appropriate prevention and mitigation measures shall be provided to ensure that nuclear

---

<sup>13</sup> Refer AERB safety guide on 'Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/SG/D-4).

safety is not compromised<sup>14</sup>. It should be noted that some external events may initiate internal fires or floods and may cause the generation of missiles. Such interaction of external and internal events shall also be considered in the design, wherever appropriate.

#### 5.2.5 External Events

##### 5.2.5.1 Protection against Natural Phenomena

Structures, systems and components necessary to assure the capability for shutdown, residual heat removal and confinement of radioactive material shall be designed to remain functional throughout the plant life in the event of natural phenomena<sup>15</sup>. Design basis for these structures, systems and components shall include:

- (i) consideration of the most serious of each of the natural phenomena or other external events which, according to the state-of-art in science and technology must be taken into account at the specific site; and
- (ii) consideration of the radiological effects of such events.

Design basis events for these structures, systems and components arising out of these phenomena are described in the AERB 'Code of Practice on Safety in Nuclear Power Plant Siting' (AERB/SC/S) [8].

##### 5.2.5.2 Protection against Man-made Events

- (i) Structures, systems and components necessary to assure the capability for shutdown, residual heat removal and confinement of radioactive material shall be designed to remain functional despite man-made events that might occur due to aircraft crash or due to activities at or near the site<sup>16</sup>, as identified in AERB siting code (AERB/SC/S) [8].
- (ii) If the likelihood of failure due to one of these events, taking into consideration the future developments at or near the plant site can be inferred to be extremely low, failure caused by that event need not be included in the design basis for that plant.
- (iii) The design of the plant shall include appropriate provision against the possibility of sabotage and unauthorized removal of nuclear and radioactive material.

---

14 Refer AERB safety guide on 'Protection Against Internally Generated Missiles and Associated Environmental Conditions' (AERB/SG/D-3) (Under Preparation).

15 Such as earthquake, cyclone and flood, tornado, Tsunami.

16 Like dam rupture, mining operations and chemical operations.

#### 5.2.6 Site Related Characteristics

In determining the design basis of nuclear power plant, various interactions between the plant and the environment, including, such factor as population, meteorology, hydrology, geology and seismology, shall be taken into account. The availability of off-site services upon which the safety of the plant and protection of the public may depend, such as electricity supply and fire fighting services, shall also be taken into account. Further details are given in the AERB siting code (AERB/SC/S) [8].

#### 5.2.7 Combination of Events

Where combinations of randomly occurring individual events could credibly lead to anticipated operational occurrences or accident conditions, they shall be considered in the design. Certain events may be the consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered be part of the original PIE.

#### 5.2.8 Design Criteria

5.2.8.1 The engineering design rules for structures, systems and components shall be specified and shall comply with the appropriate accepted national standard engineering practices (see section 3.3.1), or those standards or practices already established in another country or used internationally, and whose use is justified and also acceptable to the regulatory body.

5.2.8.2 The plant shall be designed to ensure its protection against natural/man-made phenomena.

#### 5.2.9 Operational States

5.2.9.1 The plant shall be designed to operate safely within a defined range of parameters<sup>17</sup>, and assuming the availability of a minimum set of safety support features<sup>18</sup> shall be assumed to be available. The design shall be such that the response of the plant to a wide range of anticipated operational occurrences will allow safe operation or shutdown if required, without the necessity of invoking provisions beyond the first, or at the most the second level of defence in depth.

5.2.9.2 The potential for accident conditions to occur during low power and shutdown states, such as startup and maintenance, when safety system availability may be reduced, shall be addressed in the design, and appropriate limitations on safety system unavailability shall be identified.

---

17 e.g. pressure, temperature, power.

18 e.g. auxiliary feed water capacity and emergency electrical supply.

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

- (i) safety system settings;
- (ii) control system and procedural constraints on process variables and other important parameters;
- (iii) requirements for maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, with the ALARA principle taken into consideration; and
- (iv) clearly defined operational configurations, including operational restrictions in the event of non-availability of one or more safety systems.

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

#### 5.2.10 Design Basis Accidents

5.2.10.1 A set of design basis accidents shall be derived from the listing of PIEs, for the purpose of setting the bounding conditions according to which the structures, systems and components important to safety shall be designed.

5.2.10.2 Where prompt and reliable action is required in response to a PIE, provision shall be made to initiate the necessary safety system actions automatically, in order to prevent progression to a more severe condition that may threaten the next barrier. Where prompt action is not required, manual initiation of systems or other operator actions is permitted, provided that the need for the action is revealed in time and sufficient time is available to initiate manual action and that adequate procedures<sup>19</sup> are defined to ensure the reliability of such actions.

5.2.10.3 The design shall take into account and facilitate the operator actions that may be necessary to diagnose the plant conditions and place it in a stable long term shutdown state in a timely manner by the provision of adequate instrumentation to monitor the plant status and controls for manual operation of equipment.

5.2.10.4 Any equipment and/or control required for manual response and recovery processes shall be placed at the most suitable location to ensure its ready availability at the time of need and to allow human access for the anticipated environmental conditions.

---

<sup>19</sup> e.g. administrative, operational and emergency procedures.



#### 5.2.11 Severe Accidents

Certain low probability plant states that are beyond design basis accidents and arise owing to multiple failures of safety systems involving significant core degradation may threaten the integrity of many or all the barriers to the release of radioactive material. These event sequences are called severe accidents. Consideration shall be given to these severe accident sequences, using a combination of engineering judgment and probabilistic methods, to determine those sequences for which reasonably practicable preventive or mitigatory measures can be identified. Acceptable measures need not involve the application of conservative engineering practices used in setting and evaluating design basis accidents, but rather should be based upon realistic or best estimate assumptions and methods. On the basis of operational experience, associated safety analysis and results from safety research, design activities for addressing severe accidents shall take into account the following:

- (i) Important event sequences that may lead to severe accidents shall be identified using a combination of probabilistic methods, deterministic methods and sound engineering judgment.
- (ii) These event sequences shall then be reviewed against identified set of criteria aimed at determining which severe accidents should be addressed in the design.
- (iii) Potential design or procedural changes that could either reduce the likelihood of these selected events or mitigate their consequences, should these selected events occur, shall be evaluated, and shall be implemented.
- (iv) Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and anticipated operating conditions, and the use of additional temporary systems to return the potential accident conditions to a controlled state and/or to mitigate the consequences, provided that it can be shown that the systems are able to function in the expected environmental conditions.
- (v) For multi-unit plants, consideration shall be given to the use of available means and/or support from other units, provided that the safe operation of other units is not compromised.
- (vi) Accident management procedures shall be established, taking into account representative and dominant severe accident scenarios.

#### 5.3 Design for Reliability of Structures, Systems and Components

Structures, systems and components important to safety shall be designed to be capable of coping with all identified PIEs with sufficient reliability.

### 5.3.1 Common Cause Failure

The potential for common cause failures in items important to safety shall be considered to determine where the principles of diversity, redundancy, independence and physical separation should be applied to achieve the required reliability.

### 5.3.2 Single Failure Criterion

5.3.2.1 The single failure criterion shall be applied to each safety group incorporated in the plant design.

5.3.2.2 To test compliance of the plant with the single failure criterion, the pertinent safety group shall be analysed in the following manner. A single failure (and all its consequential failures) shall be assumed to occur in sequence at each element of the safety group until all failures have been analysed. The analyses of each pertinent safety group shall then be conducted in sequence until all safety groups and all failures have been considered. (In this code, safety functions, or systems contributing to performing those safety functions, for which redundancy is necessary to achieve the required high reliability, have been identified by the statement on the assumption of a single failure). The assumption of the single failure in that system is part of the process described above. At no time during the single failure analysis, more than one random failure is assumed to occur.

5.3.2.3 Spurious action shall be considered as one mode of failure when applying the criteria to a safety group or system.

5.3.2.4 Compliance with the criterion shall be achieved when each safety group has been shown to achieve its safety function when the above analyses are applied, under the following conditions:

- (i) any potential harmful consequences of the PIE on the safety group are assumed to occur; and
- (ii) the worst permissible configuration of safety systems performing the necessary safety function is assumed, taking account of maintenance, testing, inspection and repair, and allowable equipment outage times.

5.3.2.5 Non-compliance with the single failure criterion shall be exceptional, and may be clearly justified in the safety analysis covering the following:

- (i) very rare postulated initiating events, or
- (ii) very improbable consequence of postulated initiating events, or
- (iii) very low consequences of PIE; or
- (iv) withdrawal from service for limited periods of certain components for purposes of maintenance, repair or periodic testing.

5.3.2.6 In the single failure analysis, it may not be necessary to assume the failure of a passive component designed, manufactured, inspected and maintained in service to an extremely high quality, provided it remains unaffected by the PIE. However, when it is assumed that a passive component does not fail, such an analytical approach shall be justified, taking into account the loads and environmental conditions, as well as the total period of time after the initiating event, for which the component is required.

### 5.3.3 Fail-Safe Design

The principle of fail-safe design is considered and incorporated into the design of systems and components important to safety for the plant as appropriate to the extent feasible, i.e. if a system or component should fail, the plant should pass into a safe state without requirement to initiate any actions.

### 5.3.4 Safety Support Systems

Safety support systems shall be regarded as part of the safety system and be classified accordingly. Their reliability, redundancy, diversity, independence, provision of features for isolation and for testing of functional capability shall be commensurate with reliability of the system that is supported. Safety support systems necessary to maintain a safe state of the plant may include electricity, cooling water, compressed air or other gases and means of lubrication.

### 5.3.5 System Storage Capacities

Storage capacities of systems important to safety<sup>20</sup>, commensurate with their safety functions, shall be adequate to cover the anticipated operational occurrences and accident conditions.

### 5.3.6 Equipment Outages

The design shall ensure, by the application of measures such as increased redundancy, that reasonable on-line maintenance and testing of systems important to safety can be conducted without the need to shut down the plant. Equipment outages, including unavailability of systems or components due to failure, shall be taken into account, and the impact of the anticipated maintenance, test and repair work on the reliability of each individual safety system shall be included in this consideration to ensure that the safety function can still be achieved with the required reliability. The time allowed for equipment outages and the actions to be taken shall be analysed and defined for each case before the start of plant operation and included in the plant operating documents.

---

<sup>20</sup> e.g. cooling water system, instrument air supply system, emergency power supply system, etc.

## **5.4 Materials**

5.4.1 To ensure satisfactory performance during normal operation and accident conditions, only approved materials for structures, components, etc. shall be selected<sup>21</sup> based on considerations, among others, like:

- (i) irradiation damage;
- (ii) activation and corrosion;
- (iii) creep and fatigue;
- (iv) erosion;
- (v) compatibility with other interacting materials;
- (vi) thermal effects;
- (vii) resistance to brittle fracture; and
- (viii) hydrogen pick-up.

Current state-of-art developments in material research, behavior phenomena forms an essential input for design updates.

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

5.5.1 Structures, systems and components important to safety, except as described in para 5.6.1, shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored with respect to their functional capability during the life of the nuclear power plant to demonstrate that reliability targets are being met. The plant layout shall be such that these activities are facilitated and can be performed to standards commensurate with the importance of the safety functions to be performed, with no significant reduction in system availability and without undue exposure of the site personnel to radiation<sup>22</sup>.

5.5.2 If the structures, systems and components important to safety cannot be designed to be tested, inspected or monitored to the extent desirable, then the following approach shall be followed:

- (i) Other proven alternative and/or indirect methods, such as surveillance of reference items, or verified and validated calculational methods shall be specified; and

---

21 Refer AERB safety guide on 'Material Selections and Properties for Pressurised Heavy Water Reactors' (AERB/SG/D-16) (Under Preparation).

22 Refer AERB safety guide on 'Design for In-service Inspection of Pressurised Heavy Water Reactors' (AERB/SG/D-17) (Under Preparation).

- (ii) Conservative safety margins or other appropriate precautions shall be applied to compensate for potential undiscovered failures.

## **5.6 Equipment Qualification**

5.6.1 A qualification procedure shall confirm that the equipment is capable of meeting, throughout its design operational life, the requirements for performing safety functions while subject to the environmental conditions<sup>23</sup> prevailing at the time of need. These environmental conditions shall include the variations expected during normal operation, anticipated operational occurrences and design basis accidents. In the qualification programme, consideration shall be given to ageing effects caused by various environmental factors<sup>24</sup> during the required life of the equipment<sup>14</sup>. Where the equipment is subject to external natural events and is required to perform a safety function during and following such an event, the qualification programme shall replicate as far as practicable the conditions imposed on the equipment by the natural phenomenon, either by test or analysis or by a combination of both<sup>25</sup>.

5.6.2 In addition, any unusual environmental conditions that can be reasonably anticipated and could arise from specific operational conditions<sup>26</sup> shall be included in the qualification programme. To the extent possible, equipment that is needed to operate during severe accidents<sup>27</sup> should be shown, with reasonable confidence, to be capable of achieving the design intent.

## **5.7 Ageing**

5.7.1 The design shall provide appropriate margins for all structures, systems and components important to safety so as to take into account relevant ageing and wear-out mechanisms and potential age related degradation, in order to ensure the capability of the structure, system or component to perform the required safety function throughout its design life. Ageing and wear-out effects during all normal design operational conditions, testing, maintenance, maintenance outages, PIE and post-PIE conditions shall also be taken into account<sup>28</sup>. Provision shall also be made for monitoring, testing, sampling and inspection,

---

23 e.g. vibration, temperature, pressure, jet impingement, electromagnetic interference, lightning, radiation, humidity or any likely combination thereof.

24 Such as vibration, irradiation, temperature, salinity, pollutants.

25 Refer AERB safety guide on 'Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-23).

26 Such as periodic containment leak rate testing.

27 e.g. certain instrumentation.

28 Refer AERB safety guide on 'Life Management of Nuclear Power Plants' (AERB/NPP/SG/O-14).

to assess ageing mechanisms predicted at the design stage for selected systems/ components and to identify unanticipated behaviour or degradation that may occur in service<sup>22</sup>. Required data shall be generated for these equipment for ageing management and estimation of their residual life.

- 5.7.2 Design life of the plant and its components shall be specified. In cases where the design life of equipment/component is less than the design life of the plant, mid-term in-situ replacement of the equipment is warranted. Adequate provisions should be made in the design, particularly for the in core equipment, to facilitate such replacements

## **5.8 Human Factor**

- 5.8.1 Design for Optimised Operator Performance

5.8.1.1 The design shall be 'operator friendly' and shall be aimed at limiting the effects of human errors. Attention shall be paid to plant layout and procedures (administrative, operational and emergency), including maintenance and inspection, in order to facilitate the interface between the operating personnel and the plant.

5.8.1.2 The working areas and working environment of the site personnel shall be designed according to ergonomic principles.

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

5.8.1.4 The human-machine interface shall be designed to provide the operator with comprehensive, but easily manageable information, compatible with required decision and action time. Similar provisions shall be made for the backup control room/backup control points.

5.8.1.5 Assessment (verification and validation) of human factors aspects shall be included at appropriate stages to confirm that the design adequately accommodates all required operator actions.

5.8.1.6 The operator shall have information that permits:

- (i) the ready assessment of the general state of the plant in whichever condition it is, i.e. in normal operation, in an anticipated operational occurrence, or in an accident condition, and confirm that the designed automatic safety actions are being carried out; and
- (ii) the determination of the appropriate operator initiated safety actions to be taken.

- 5.8.1.7 The operator shall be provided with sufficient information on parameters associated with individual plant systems and equipment to confirm that the required safety actions can be achieved safely.
- 5.8.1.8 The design shall aim to promote the success of operator actions in the light of the time available, the expected physical environment and the psychological pressure (operational stress) on the operator. The need for operator intervention on a short time-scale of less than 30 minutes following a PIE is kept to a minimum. The design should take into account that the credit for such operator intervention within 30 minutes of PIE is acceptable only if the:
- (i) designer can demonstrate that the operator has sufficient time to decide and to act;
  - (ii) necessary information on which the operator must base a decision to act is simply and unambiguously presented;
  - (iii) physical environment following the event is acceptable in the control room or in the backup control room/backup control points; and
  - (iv) access route to that backup control room/backup control points, is available.

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

## **5.9 Other Design Considerations**

### **5.9.1 Sharing of Structures, Systems and Components in Multi-Reactor Nuclear Power Plants**

Structures, systems and components important to safety shall generally not be shared between two or more nuclear power reactors. In exceptional cases where such structures, systems and components important to safety are shared between two or more nuclear reactors, it shall be demonstrated that all safety requirements are met for all reactors under all operational states and design basis accidents. In the event of accident conditions involving one of the reactors, an orderly shutdown, cool down and residual heat removal of the other reactors shall be achievable.

### **5.9.2 Power Plants Used for Cogeneration, Heat Generation or Desalination**

Nuclear power plants coupled with heat utilisation units (such as for district heating) and/or water desalination units shall be designed to prevent transport of radioactive materials from the nuclear plant to the desalination or district heating unit under any condition of normal operation, anticipated operational occurrences, design basis accidents and selected severe accidents.

### 5.9.3 Fuel and Radioactive Waste Transport and Packaging

The design shall incorporate appropriate features to facilitate transport and handling of fresh fuel, spent fuel and radioactive waste<sup>29</sup>. Consideration shall be given to access facilities and lifting and packaging capabilities.

### 5.9.4 Escape Routes and Means of Communication

5.9.4.1 The nuclear power plant shall have sufficient number of safe escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other building services essential to the safe use of these routes. The escape routes shall meet the relevant requirements of industrial safety, radiation zoning, fire protection and plant security and emergency handling (including off-site) [9].

5.9.4.2 Suitable alarm systems and adequate means of communication shall be provided so that all persons present in the plant and on the site can be warned and instructed, even under accident conditions.

5.9.4.3 Communications necessary for safety, both within the plant and to the outside, shall be assured at all times. This requirement shall be taken into account in the design and in the diversity (at least two independent means) of the communication methods selected. Means for the safety of plant personnel shall be provided taking into account differing requirements from the point of view of industrial safety, radiation and fire protection and security.

### 5.9.5 Control of Access

5.9.5.1 The plant shall be isolated from the surroundings by suitable layout of the structural elements in such a way that access to it can be permanently controlled. In particular, attention shall be paid in the design of the buildings and site layout, and provision shall be made for supervisory personnel or equipment, to guard against unauthorised entry of persons and goods to the plant [10].

5.9.5.2 Unauthorised access to, or interference for any reason with structures, systems and components important to safety shall be prevented. Where access is required for maintenance, testing or inspection, the design shall ensure that such activities can be performed without significantly affecting the reliability of safety related equipment.

5.9.5.3 Necessary design features shall be incorporated as part of the physical security to monitor radioactive materials at site and restrict access to safeguard against their loss/theft.

---

<sup>29</sup> Refer AERB safety guide on 'Liquid and Solid Radwaste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/SG/D-13).



5.9.5.4 The systems should be designed based on the design basis threats identified and analysis should be carried out in order to assess the risk of unauthorised removal of nuclear materials and/or sabotage of NPP and incorporation of corrective measures.

#### 5.9.6 System Interaction

Where there is a significant probability that systems important to safety will be required to operate simultaneously, their possible interaction shall be evaluated. The analysis shall take into account not only physical interconnections, but also the effects of a system's operation, maloperation or failure on the physical environment of other required systems to ensure that changes in the environment do not affect the reliability of system components in functioning as intended.

#### 5.9.7 Electrical Grid-plant Interaction

In the design of the plant, account shall be taken of the electrical power grid-plant interactions, including the independence of and number of grid power supply lines to the plant, in relation to the required reliability of the power supply to the plant systems important to safety.

#### 5.9.8 Decommissioning

5.9.8.1 At the design stage, appropriate consideration shall be given to the incorporation of features which will facilitate the decommissioning and dismantling of the plant<sup>30</sup>.

5.9.8.2 The exposures of personnel and the public during decommissioning shall be kept within limit prescribed by the regulatory body and to ensure adequate protection of the environment from radioactive contamination. Decommissioning aspect shall be considered at the design stage itself to include:

- (i) The choice of materials, such that eventual quantities of radioactive waste are minimised and decontamination is facilitated.
- (ii) The access capabilities that may be required.
- (iii) The facilities necessary for storing radioactive waste generated during both operation and decommissioning of the plant.

### 5.10 Safety Analysis

A safety analysis of the plant design, applying methods of deterministic, shall be provided which establishes and confirms the design basis for the items

---

30 AERB safety manual for 'Decommissioning of Nuclear Facilities' (AERB/SM/DECOM-1).

important to safety and demonstrates that the overall plant design ensures that radiation doses and releases are within the prescribed limits for operational states and acceptable limits for accident conditions. In addition, to complement the deterministic safety analysis, probabilistic safety analysis shall also be performed.

Operator action for mitigation of the consequence of a PIE shall not be given credit while performing safety analysis of the plant for the first 30 minutes following a PIE.

The computer programs, analytical methods and plant models used in the safety analysis shall be verified and validated, and adequate consideration shall be given to uncertainties<sup>31</sup>.

#### 5.10.1 Deterministic Approach

The deterministic safety analysis<sup>32</sup> shall include:

- (i) confirmation that operational limits and conditions are in compliance with the design assumptions and intent for the normal operation of the plant,
- (ii) categorisation of the PIEs that are appropriate for the plant design and its location,
- (iii) analysis and evaluation of event sequences that result from PIEs,
- (iv) comparison of the results of the analysis with radiological acceptance criteria and other design limits,
- (v) establishment and confirmation of the design basis, and
- (vi) demonstration that the management of anticipated operational occurrences and design basis accidents is possible by automatic safety response in combination with prescribed operator actions.

The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified. The safety analysis of the plant design shall be updated in the light of significant changes in plant configuration, operational experience, improvements in technical knowledge or understanding of physical phenomena, and shall be consistent with the current or “as-built” state.

---

31 For LOCA Analysis, Refer AERB safety guide on ‘Loss of Coolant Accident Analysis for Pressurised Heavy Water Reactors’ (AERB/SG/D-18).

32 Refer AERB safety guide on ‘Deterministic Safety Analysis of Pressurised Heavy Water Reactor Based Nuclear Power Plants’ (AERB/SG/D-19) (Under Preparation).

## 5.10.2 Probabilistic Approach

5.10.2.1 Deterministic approach is supplemented with probabilistic approach. A probabilistic safety analysis (PSA) shall be done to prove that core damage frequency (CDF) and large early release frequency (LERF) derived from this consideration is limited<sup>33</sup> for a given NPP<sup>34</sup>. Probability of failure of different safety systems is identified in different paragraphs of this code to facilitate achieving this target.

PSA provides a systematic analysis to give confidence that the design will comply with the general safety objectives.

There are three levels of PSA:

- (i) Level 1 PSA,
- (ii) Level 2 PSA, and
- (iii) Level 3 PSA.

5.10.2.2 Level 1 PSA shall be carried out to:

- (i) demonstrate 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 the first two levels of defence in depth carry the primary burden of nuclear safety;
- (ii) provide confidence that no design basis accident is on the threshold (cliff-edge) of a sudden escalation of the consequences of associated PIEs;
- (iii) to provide assessments of the probability of occurrence and consequences of external hazards, in particular those unique to the plant site;
- (iv) to check compliance with probabilistic targets<sup>33</sup>;
- (v) to identify any design weakness; and
- (vi) to provide basis for technical specifications on testing frequencies and outage duration for equipment.

5.10.2.3 Level 2 PSA is recommended to:

- (i) provide assessments of the probability of occurrence of severe core

---

33 Limits on CDF and LERF are specified as  $10^{-5}$ /reactor-year and  $10^{-6}$ /reactor-year respectively.

34 Refer AERB safety manual on 'Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors' (AERB/NPP&RR/SM/O-1) for details for carrying out PSA.

damage states, and the risk of large off-site releases requiring short term off-site response, especially those associated with early containment failure; and

- (ii) identify systems for which design improvements or operational procedures could reduce the probability of severe accidents or mitigate their consequences.

5.10.2.4 Level 3 PSA is recommended to assess the adequacy of plant emergency procedure.

#### 5.10.3 Safety Analysis Report

A comprehensive safety analysis report shall be prepared to demonstrate that all safety objectives under subsection 5.10 are achieved<sup>35</sup>.

---

<sup>35</sup> Refer AERB safety guide on 'Standard Format and Contents of Safety Analysis Report of Nuclear Power Plants' (AERB/SG/G-9) (Under Preparation).

## 6. PLANT SYSTEM DESIGN REQUIREMENTS

### 6.1 Reactor Core and Associated Features

#### 6.1.1 Design

The reactor core and associated coolant, moderator, control and protection systems shall be designed with appropriate margin to assure that the specified design limits (para 5.2.3) are not exceeded and that radiation safety standards are applied in all operational states and in design basis accidents, with account taken of the existing uncertainties.

#### 6.1.2 Core Components

##### 6.1.2.1 The reactor core components include:

fuel bundles,

coolant channel assemblies,

calandria and endshield assembly, and

other internal structures, control and shutdown mechanisms, in-core detector assemblies etc.

##### 6.1.2.2 The design of the reactor core, pressure tubes, calandria vessel and the reactor internal structures shall account for the static and dynamic loadings expected under operational states and design basis accidents with due regard to the effects of temperature, pressure, irradiation, ageing, creep, corrosion, erosion, hydriding, vibrations, fatigue etc.. Under postulated accident conditions, adequate integrity of the core components shall be maintained to ensure:

(i) safe shutdown of the reactor and maintaining it in sub-critical state with adequate shutdown margin, and

(ii) coolable geometry and adequate core cooling is maintained.

##### 6.1.2.3 The reactor core and associated coolant control and protection systems shall be designed so as to allow adequate inspection and test capability throughout the service life of the plant<sup>22</sup>.

#### 6.1.3 Fuel Elements and Bundles

##### 6.1.3.1 The design of fuel elements and bundles shall be such that they satisfactorily withstand the intended irradiation and environmental exposure in the reactor core despite all processes of deterioration that can occur under all operational states<sup>36</sup>.

---

36 Refer AERB safety guide on 'Fuel Design for Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-6).

- 6.1.3.2 The deterioration considered shall include that arising from differential expansion and deformation, external pressure of the coolant, additional internal pressure due to the fission products within the fuel element, irradiation of fuel and other materials in the fuel bundle, changes in pressures and temperatures resulting from changes in power demand and power ramp, chemical effects, static and dynamic loading including fuelling loads, flow induced and mechanical vibrations, and changes in heat transfer performance that may result from distortions like due to creep of coolant channel or chemical effects on fuel element.
- 6.1.3.3 The design of fuel bundles shall consider their post irradiation handling and storage including those damaged during usage or handling.
- 6.1.3.4 Specified fuel design limits shall not be exceeded in normal operation, and conditions that may be transiently imposed on fuel bundle during anticipated operational occurrences shall cause no significant additional deterioration. Fission product leakage shall be restricted by design limits<sup>37</sup> and kept to a minimum.
- 6.1.3.5 Design shall ensure for timely detection and removal of any failed fuel from the core during nuclear power plant operation.
- 6.1.3.6 In design basis accidents, the fuel bundles shall remain in position and shall not suffer distortion to an extent that would render post-accident core cooling ineffective; and specified fuel integrity limits shall not be exceeded.
- 6.1.3.7 The aforementioned requirements for reactor and fuel element design shall also be maintained in the event of changes in fuel management strategy or operational conditions during the plant life.
- 6.1.4 Reactor Core Control
  - 6.1.4.1 The maximum degree and insertion rate of positive reactivity during all operational states and accident conditions shall be limited such that no resultant failure of the reactor pressure boundary occurs, cooling capability is maintained and no significant damage occurs to the reactor core.
  - 6.1.4.2 The core and its control systems shall be so designed that uncontrolled increase of power cannot occur. The control and protection systems' negative reactivity worth and the insertion rates shall be sufficient to override reactivity changes including those due to internal and dynamic reactivity coefficients during all plant states. Positive reactivity insertion rate shall be within permissible limits<sup>38</sup>.

---

37 Iodine activity in the primary coolant shall be limited to 100  $\mu\text{Ci/l}$ .

38 Refer AERB safety guide on 'Core Reactivity Control in Pressurised Heavy Water Reactors' (AERB/SG/D-7).

- 6.1.4.3 Isotopic purity of heavy water coolant shall be greater than or equal to the design value limits of positive void coefficient.
- 6.1.4.4 The reactor core including the associated coolant, moderator, control and protection system shall be designed to assure that power oscillations and/or unstable core coolant flow which can result in conditions exceeding specified fuel design limits do not occur or can be readily and reliably detected and suppressed.
- 6.1.4.5 The fuel design limits<sup>36</sup> 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 anticipated operational occurrences.
- 6.1.4.6 The flux shapes shall be monitored continuously to ensure that the fuel design limits are not violated in any region of the core.
- 6.1.4.7 The design of the core and the fuel management scheme provided should minimise the demands made on control system for maintaining flux shapes and levels and stability within specified limits in all operational states.
- 6.1.4.8 For any nuclear power plant, at the time of first start-up, the reactivity coefficients, excess reactivity and control element worth shall be verified in the commissioning experiments before the reactor is operated at power.
- 6.1.4.9 The design of reactivity control devices shall take into account wear-out and effects of irradiation, such as burnup, changes in physical properties etc.
- 6.1.5 Reactor Shutdown
  - 6.1.5.1 The reactor shutdown shall be performed by two diverse systems of different design principles. Each of the systems shall be, on its own, capable of quickly rendering the nuclear reactor sub-critical by an adequate margin from operating and accident conditions<sup>39</sup>. Each of these systems shall also be capable of reliably overriding reactivity changes resulting from refuelling during shutdown, withdrawal of any control rod/shut-off rods for maintenance during shutdown, withdrawal sequence of the shut-off rods for startup with reactor in cold condition and reactivity changes during shutdown. Each shutdown system shall be, on its own, capable of rendering the reactor sub-critical from normal operating conditions and of maintaining the reactor sub-critical by an adequate margin in the most reactive core including the capability of reliably overriding reactivity changes resulting from xenon decay after shutdown<sup>36</sup>.

---

<sup>39</sup> Refer AERB safety guide on 'Safety Systems for Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-10).

- 6.1.5.2 The reactor shutdown system(s) shall be capable of making and holding the core adequately sub-critical in the event of any anticipated operational occurrences and postulated accident conditions. The shutdown function shall be ensured even for the most reactive situation of the core.
- 6.1.5.3 The shutdown margin and the effectiveness of the negative reactivity insertion rate of the shutdown system shall be such that fuel design limits<sup>36</sup> are not exceeded during anticipated operational occurrences<sup>38</sup>. The resultant reactivity during any PIE, due to the positive reactivity addition resulting from the PIE and the negative reactivity insertion caused by the shutdown system after a PIE, should meet the above requirement. During postulated accident conditions it shall be ensured that the core along with all internals is not damaged to the extent that adequate core cooling cannot be maintained.
- 6.1.5.4 In order to guard against dropping of loads which may result in inoperability of the reactor control and shutdown systems, there should be no movement of crane or any lifting devices over the reactivity mechanisms (reactor control and reactor shutdown systems) and calandria whenever reactor is critical.
- 6.1.5.5 Each shutdown system shall perform safety function assuming single failure and with failure probability less than  $10^{-3}$ /demand.
- 6.1.5.6 Instrumentation shall be provided and tests specified to ensure that the shutdown systems are always in the state required, for the given plant condition.
- 6.1.5.7 Design shall ensure that periodic in-service inspection, calibration, and functional testing are feasible<sup>22</sup>. For those equipments, which are not designed for entire life of the plant, shall be replaceable.

## **6.2 Moderator System**

- 6.2.1 Moderator system includes the main moderator circulation system, adjuster rods cooling system, purification system, cover gas system and other associated systems.
- 6.2.2 Components which are part of moderator system shall be designed, fabricated, inspected, erected and tested to the quality standards as commensurate with the safety classification<sup>9</sup>.
- 6.2.3 The design shall consider possible corrosive environment due to radiolytic dissociation of heavy water and neutron poison in moderator for determining system construction materials.
- 6.2.4 Moderator system should ensure that temperature in calandria is such that sustained dry-out does not take place on calandria tube under LOCA plus failure of ECCS.



- 6.2.5 The moderator system design shall provide means to control build-up of deuterium to prevent possibility of explosion<sup>40</sup>.
- 6.2.6 An on-line purification system shall be provided to maintain chemistry of moderator and to facilitate removal of dissolved neutron poison. The purification flow should ensure that poison removal rates meet the reactivity addition rate criteria.
- 6.2.7 Design provision shall be made to remove tritium activity from the moderator system.

### **6.3 Reactor Coolant System**

#### **6.3.1 Design**

- 6.3.1.1 Reactor coolant system includes the main coolant system, pressure control system, residual heat removal system (shutdown cooling system), emergency core cooling system and other associated systems.
- 6.3.1.2 Fuelling machine and its associated control system shall also form part of reactor coolant system during the period when it is connected to the coolant channel.
- 6.3.1.3 The components of reactor coolant system include pressure tubes, end fittings, seal plugs, shield plug, feeders, headers, pumps, steam generators, heat exchangers, pressuriser, accumulators, valves, connected piping and associated component support structures.
- 6.3.1.4 The reactor coolant system, its associated auxiliary systems, and the control and protection systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during operational states<sup>41</sup>. The operation of pressure relief devices, even in design basis accidents, shall not lead to unacceptable releases of radioactive material from the plant. The reactor coolant pressure boundary shall be equipped with adequate isolation devices to limit any loss of radioactive fluid.
- 6.3.1.5 The component parts containing the reactor coolant<sup>42</sup> together with the devices by which such parts are held in place, shall be designed in such a way as to withstand the static and dynamic loads anticipated during all plant states .

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

---

40 Refer AERB safety manual on 'Hydrogen Release and Mitigation Measures under Accident Conditions' (AERB/NPP-PHWR/SM/D-2).

41 Refer 'Technical Specifications for Operation'.

42 e.g. pressure tubes, piping and connections, valves, fittings, pumps and heat exchangers, etc.

- 6.3.1.6 Components which are part of reactor coolant pressure boundary shall be designed, fabricated, inspected, erected and tested to the highest quality standards<sup>43</sup>.
- 6.3.1.7 The pressure retaining boundary for reactor coolant shall be so designed that flaws are very unlikely to be initiated but, if initiated, would propagate only very small amounts. Even if significantly higher growth were to take place it will take place in such a manner that leak occurs before break permitting timely detection of flaws. Designs and plant states, in which components of the reactor coolant pressure boundary could exhibit brittle behaviour, shall be avoided. Process of leak before break needs to be established and proved as per the criteria laid down.
- 6.3.1.8 Choice of suitable ductile materials and their limited controlled degradation (due to corrosion, hydrogen and radiation embrittlement etc.) is essential to ensure that leak precedes any catastrophic failure. System shall be provided for early leak detection and its adequacy should be demonstrated by analysis.
- 6.3.1.9 The design shall reflect consideration of all boundary material under operational, maintenance and testing conditions and in design basis accidents, taking into account the expected end of life properties (which are affected by erosion, creep, fatigue, the chemical environment, the radiation environment and ageing), and for any uncertainties in determining the initial state of the components and the rate of possible deterioration.
- 6.3.1.10 The design of the components contained within the reactor coolant pressure boundary<sup>44</sup> shall be such as to minimise the likelihood of failure and associated consequential damage to other items of the primary coolant system important to safety in all operational states and in design basis accidents, with due allowance made for deterioration that may occur in service.
- 6.3.1.11 If any significant change is made in the reactor system (like quarantining of coolant channels), its effect on the safety should be evaluated.
- 6.3.2 In-Service Inspection of the Reactor Coolant Pressure Boundary
- 6.3.2.1 The components of the reactor coolant pressure boundary shall be designed, manufactured and arranged in such a way that it is possible, throughout the service lifetime of the plant, to carry out at appropriate intervals adequate inspections and tests of the boundary<sup>22</sup>.

---

43 Refer AERB safety guide on 'Primary Heat Transport System for Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-8).

44 Such as pump impellers and valve parts.

- 6.3.2.2 Provision shall be made to implement a material surveillance programme for the reactor coolant boundary, particularly in high irradiation locations, and other important components as appropriate for determining the metallurgical effects of factors<sup>45</sup>.
- 6.3.2.3 Monitoring for soundness of the reactor coolant pressure boundary shall be provided by detection of flaws, distortion, or of excessive leakage and reduction in thickness at location prone to erosion<sup>46</sup>.
- 6.3.2.4 Where the safety analysis of the nuclear power plant indicates that particular failures in the secondary cooling system may result in serious consequences, it shall be ensured that inspection of relevant parts of the secondary cooling system is possible.
- 6.3.3 Reactor Coolant Inventory
- Provision shall be made for controlling the inventory or/and pressure of coolant to ensure that specified design limits are not exceeded in any operational state, with volumetric changes and leakage taken into account<sup>47</sup>. The systems performing this function shall have adequate capacity (flow rate and storage volumes) to meet this requirement. They may be composed of components needed for the processes of power generation and may be specially provided for performing this function. If heat removal function under the accident conditions involving primary heat transport pressure boundary is likely to be adversely affected, the system (provided to cope with this application) shall be designed assuming single failure.
- 6.3.4 Clean-up of the Reactor Coolant
- An online system shall be provided to clean the reactor coolant system from corrosion products and radioactive substances including fission products leaking from the fuel to minimise the crud and radioactivity level and keep below their specified limits<sup>41</sup>.
- 6.3.5 Residual Heat Removal from the Core
- 6.3.5.1 Means for removing residual heat<sup>47</sup> shall be provided. Their safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified fuel design limits and the design basis limits of the reactor coolant pressure boundary are not exceeded.

---

45 Such as irradiation, stress corrosion cracking, thermal embrittlement, hydrogen embrittlement and ageing of structural materials.

46 For example; feeders.

47 Refer AERB Technical Document on 'Decay Heat Load Calculations in Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/NPP-PHWR/TD/D-1) (Under Preparation).

- 6.3.5.2 Suitable redundancy shall be provided in the design of the system to meet its functional requirements with sufficient reliability assuming single failure.
- 6.3.5.3 Main coolant system coast down characteristics coupled with suitable layout of the system, to ensure cooling by thermosyphon, may be considered as part of residual heat removal system.
- 6.3.6 Emergency Core Cooling
- 6.3.6.1 Suitable redundancy, diversity and design features<sup>48</sup> shall be provided, with sufficient reliability, assuming a single failure<sup>39</sup>. The ECCS shall be designed such that the fraction of time for which it is not available can be demonstrated as the failure probability to be less than specified value<sup>49</sup>.
- 6.3.6.2 Adequate core cooling in the event of loss of coolant accident (LOCA)<sup>31</sup> due to rupture anywhere in the reactor coolant system shall be provided by incorporating high pressure injection and long term cooling systems to minimise damage to the core and to limit the escape of fission products from the core<sup>43</sup>. This means that cooling shall ensure that:
- (i) the cladding or fuel integrity limiting parameters will not exceed the acceptable value for design basis accidents<sup>36</sup>;
  - (ii) possible chemical reactions are limited<sup>40</sup>;
  - (iii) the changes in the fuel and internal structural geometry will not significantly reduce the effectiveness of the emergency core cooling<sup>27</sup>. The cooling of the core shall be ensured for a sufficient time.
- 6.3.6.3 Adequate consideration shall be given to extending the capability of ECCS to remove heat from the core following a severe accident.
- 6.3.7 Inspection and Testing of the Emergency Core Cooling System
- The emergency core cooling system shall be designed to permit appropriate periodic inspection and testing of important components<sup>22</sup> to ensure<sup>43</sup>:
- (i) the structural and leaktight integrity of its components;
  - (ii) the operability and performance of the active components of the system during normal operation, as far as feasible; and

---

48 Such as interconnection, leak detection and isolation capability.

49 Less than  $10^{-3}$ /demand.

- (iii) the operability of the system as a whole under the conditions as close to design basis as practicable<sup>50</sup>.

#### 6.3.8 Auxiliary Feed Water System

An auxiliary feed water system of high reliability for steam generator shall be provided to ensure that process parameters of the reactor coolant system during specified operational state and accident conditions are maintained within stipulated limits<sup>41</sup>. To ensure that:

- (i) appropriate provision of steam discharge from steam generator shall be made;
- (ii) steam generator auxiliary feed water system shall be independent of the steam generator main feed water system;
- (iii) the system shall be designed with sufficient reliability assuming a single failure; and
- (iv) backup system, such as fire water injection shall be provided.

#### 6.3.9 Fuelling System

6.3.9.1 During on power refuelling, the fuelling machine is considered a part of the reactor coolant system starting from coupling of fuelling machine (to coolant channel) till its decoupling (from coolant channel).

6.3.9.2 Fuelling machine integrity requirements shall be consistent with the integrity of reactor coolant boundary<sup>51</sup>. The probability of loss of coolant and/or ejection of spent fuel should be minimised. In order to ensure the integrity of reactor coolant pressure boundary during fuelling operations, means shall be provided to verify the leak tightness of the system before removal and after installation of the seal plug.

6.3.9.3 Since the movement of fuelling machine connected to a coolant channel could lead to breaching of reactor coolant boundary, measures to prevent this from occurring shall be employed.

### 6.4 Ultimate Heat Sink and Associated Systems

#### 6.4.1 Heat Transfer to an Ultimate Heat Sink

---

50 e.g. the performance of the full operational sequences that bring the system into operation, including operation of applicable portions of the protection system, the transfer between normal and the operation of the associated safety system support features is verified. However, it may be possible to carry out verification of the system subsystem wise in steps during operation.

51 Refer AERB safety guide on 'Design of Fuel Handling and Storage Systems of Pressurised Heavy Water Reactors' (AERB/SG/D-24).

- 6.4.1.1 Systems shall be provided to transfer residual heat from structures, systems and components important to safety to an ultimate heat sink during all operational states and design basis accidents.

The system's safety function shall be to transfer combined heat load of the structures, systems and components under all operational states and design basis accidents at a rate such that specified fuel design limits and the design limits of the reactor coolant pressure boundary are not exceeded. All systems that contribute to the transport of heat, by supplying fluids to the heat transport systems, by conveying heat; or by providing power, shall be designed to achieve reliability commensurate with importance to their contribution to the overall heat transfer function<sup>52</sup>.

- 6.4.1.2 Suitable redundancy in components and systems and suitable interconnections, leak detection and isolation capabilities shall be provided to assure that the system safety functions can be accomplished assuming a single failure.
- 6.4.1.3 Natural phenomena and man-made events shall be taken into account in the design of systems and in the possible choice of diversity in the ultimate heat sinks and in the storage systems from which heat transfer fluids are supplied. Availability of heat sink should be ensured under the condition of non-availability of off-site and on-site power for an extended period.
- 6.4.1.4 Adequate consideration shall be given to extending the capability to transfer core residual heat to an ultimate heat sink to ensure that acceptable temperatures can be maintained in structures, systems and components important to the safety function of confinement of radioactive materials in the event of a severe accident.

#### 6.4.2 Inspection and Testing

- 6.4.2.1 The system shall be designed to permit appropriate periodic inspection of important components to assure the integrity and capability of the system<sup>22</sup>.
- 6.4.2.2 The system shall be designed to permit appropriate periodic functional testing to assure:
- (i) the structural and leak tight integrity of its components;
  - (ii) the operability and the performance of the active components of the system; and
  - (iii) the operability of the system as a whole and, under conditions as

---

52 Refer AERB safety guide on 'Ultimate Heat Sink and Associated Systems in Pressurised Heavy Water Reactors' (AERB/SG/D-15).

close to design as practical, the performance of full operational sequence that brings the system into operation for reactor shutdown and for loss of coolant accidents, including operation of applicable portions of the protection systems and the transfer between normal and emergency power sources including operation under complete loss of power.

## **6.5 Civil Structures and Containment System**

### **6.5.1 Design**

6.5.1.1 All safety related civil engineering structures and their components shall be designed to achieve the safety objectives in this safety code. For this, requirements stipulated in the AERB safety standard on 'Civil Engineering Structures Important to Safety of Nuclear Facilities' (AERB/SS/CSE) [11] shall be complied with.

6.5.1.2 A containment system shall be provided to enclose completely the reactor coolant system and other radioactive fluid containing systems (low pressure systems isolatable from containment, like purification system, spent fuel storage bay and waste storage, may be exempted from this requirement) to keep the release of radioactivity to the environment within prescribed dose limits in normal operation and accident conditions<sup>53</sup>.

The containment system may, depending on design requirements, include:

- (i) leaktight structures;
- (ii) associated systems for the control of pressure and temperature;
- (iii) features for isolation; and
- (iv) management and removal of fission products, hydrogen<sup>40</sup>, oxygen, and other substances that may be released into the containment atmosphere.

6.5.1.3 The design of the containment system shall take into account all identified design basis accidents. For calculating design pressure for containment no credit should be given to leak before break. In addition, consideration shall be given to the provision of features for the mitigation of the consequences of severe accidents.

6.5.1.4 Consideration should be given in the design for containment response during postulated severe accident beyond the design basis such as potential for generation and behaviour of flammable gases such as hydrogen, assessment

---

53 Refer AERB safety guide on 'Containment System Design for Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-21).

of ultimate load bearing capability of the primary containment envelope structure [11], assessment of containment pressure build-up in the event of selected beyond design basis accidents. For detailed requirements refer sub section 5.2.11.

#### 6.5.2 Strength of the Containment Structure

6.5.2.1 Calculation of the strength of the containment structure, including access openings and penetrations and isolation valves, shall be based, with sufficient margin, on the internal pressures and temperatures and dynamic effects such as missiles and reaction forces resulting from the design basis accidents [11]. The effects of other potential energy sources, including, for example, possible chemical and radiolytic reactions<sup>40</sup>, shall also be considered. Calculation of the required strength of the containment structure shall include consideration of natural phenomena and provision shall be made to monitor the condition of the containment and associated features following a PIE.

6.5.2.2 The layout of the containment should be so designed that sufficient testing, and repair if necessary, can be conducted at any time during life of the plant. The annular space between the primary and secondary containment envelopes shall be provided with a purging arrangement to maintain a negative pressure in the space.

6.5.2.3 The design pressure of the containment shall not be less than the peak pressure, as calculated by accepted methods<sup>53</sup>. The structural design of the containment shall consider the thermal stresses arising from the calculated temperature transients during postulated accident conditions.

#### 6.5.3 Containment Proof Tests

The containment structure shall be designed and constructed in such a way that it is possible to perform a pressure test before plant operation, at a specified pressure to demonstrate its structural integrity.

#### 6.5.4 Containment Leakage

6.5.4.1 The reactor containment system shall be designed such that the leakage rate during accident conditions throughout the service life of the plant does not exceed the prescribed limit<sup>54</sup>. The design leakage rate shall be kept to a minimum in keeping with the ALARA principle.

6.5.4.2 The containment structure and other equipment and components relevant to the leaktightness of the system shall be designed and constructed with testing provisions in such a way that the leakage rate tests of the containment and all

---

54 Refer AERB safety guide on 'Proof and Leakage Rate Testing of Reactor Containments' (AERB/NPP/SG/O-15).



penetrations can be carried out at the design pressure after all penetrations are installed. Re-determination of the leakage rate of the containment system shall be possible at periodic intervals throughout the reactor's service life, either at the containment design pressure or at reduced pressures that permit estimation of the leakage rate at the containment design pressure<sup>54</sup>.

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

#### 6.5.5 Containment Penetrations

6.5.5.1 The number of penetrations through the containment shall be kept to a practical minimum.

6.5.5.2 Portion of steam and feed pipes passing through secondary containment shall be designed to preclude possibility of over-pressurisation of the secondary containment in the event of pipe rupture.

6.5.5.3 All penetrations through the containment shall meet the same design requirements as the containment structure itself. They shall be protected against reaction forces stemming from pipe movement or accidental loads<sup>55</sup>.

6.5.5.4 If resilient seals<sup>56</sup> or expansion bellows are used with penetrations, they shall be designed to have leak testing capabilities, at containment design pressure, independent of the overall leak rate determination of the containment, to demonstrate their continuing integrity throughout the life of the plant.

#### 6.5.6 Containment Isolation

6.5.6.1 Each line that penetrates the containment and is directly connected to the containment atmosphere shall be automatically and reliably sealable in the accident conditions in which the leak tightness of the containment is essential to prevent release of radioactivity to the environment above acceptable limits. These lines should, therefore in general, be fitted with at least two adequate containment isolation valves consistent with containment design. Isolation valves shall be located as close to the containment as is practical. Containment isolation shall be accomplished assuming a single failure<sup>39</sup> and its unavailability target<sup>57</sup>.

6.5.6.2 If the application of single failure criterion reduces the reliability of a safety system (such as ECCS) that penetrates containment, redundancy shall be

---

55 Such as missiles, jet forces and pipe whip.

56 Such as elastomeric seals, electrical cable penetrations.

57 Less than  $10^{-3}$ /demand.

provided in such systems. Containment isolation should not jeopardise functioning of safety systems<sup>39</sup>.

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

#### 6.5.7 Containment Testing and Inspection

The containment and associated systems shall be designed to permit appropriate inspection<sup>22</sup> and testing to ensure functionally correct and reliable actuation of the containment isolation valves and dampers and their leak tightness during the design life of the plant<sup>54</sup>.

#### 6.5.8 Containment Airlocks

Personnel and equipment access to the containment shall be through airlocks equipped with doors that are interlocked to ensure that containment integrity is not violated during reactor operation and under accident conditions, with single failure criterion being met.

#### 6.5.9 Pressure Suppression System

Wherever, pressure suppression system is provided, it shall have adequate capacity and capability to condense, under accident conditions most of the steam. For a pool type vapour suppression system<sup>58</sup>, design shall ensure condensing of all steam passing from volume V1 to volume V2 (Volume V1 and V2 refer to those parts of the containment which are upstream and downstream respectively of the pressure suppression pool). During its passing steam and air mixture shall have sufficient contact with water in the suppression pool to dissolve soluble radioactive releases. Vent shafts shall be suitably located in volume V1 to equalise pressure in building compartments. Vent shafts shall be designed to withstand dynamic loading due to flow of fluids. The interface between volume V1 and V2 shall have pressure sealing such that the prescribed equivalent leakage path area is not exceeded.

#### 6.5.10 Internal Structures of the Containment

6.5.10.1 The design shall provide ample flow routes between separate compartments inside the containment designed to act as one single interconnected volume during accident conditions. The cross-sections of openings between

---

58 Refer AERB safety guide on 'Vapour Suppression System (Pool Type) for Pressurised Heavy Water Reactors' (AERB/SG/D-22).

compartments shall be sized to ensure that the pressure differentials during accident conditions do not result in damage to the pressure bearing structure or to other systems of importance for limiting the effects of design basis accidents [11].

- 6.5.10.2 In case, during normal operational state these openings are necessary to be sealed, the sealing arrangement shall be designed to blow open under accident conditions so that the pressure equalisation proceeds as designed.
- 6.5.10.3 The operable hatches, doors etc. provided between the sealed safety-related volumes shall be designed and operated to maintain adequate leak tightness.
- 6.5.11 Containment Heat Removal
  - 6.5.11.1 The capability to remove heat from the reactor containment shall be ensured. The safety function shall be to reduce the containment pressure and temperature after any accidental releases of high-energy fluids in design basis accidents and to maintain them within acceptably low levels. The system performing the containment heat removal function shall have adequate reliability and redundancy to ensure that the function can be accomplished, on the assumption of a single failure<sup>53</sup>.
  - 6.5.11.2 Functional and reliable performance of other features for which credit has been taken for calculating the containment pressure rise during postulated accident conditions shall be designed to permit appropriate inspection and testing.
- 6.5.12 Control and Clean-up of the Containment Atmosphere
  - 6.5.12.1 Systems shall be provided, as necessary, to control fission products, hydrogen, oxygen and other substances that may be released into the reactor containment<sup>53</sup> to:
    - (i) Reduce the amount of fission products that might be released to the environment during accident conditions.
    - (ii) Control the concentration of hydrogen<sup>40</sup> and other substances released in the containment atmosphere during design basis accidents in order to prevent deflagration or detonation which could jeopardise containment integrity.
  - 6.5.12.2 The containment atmosphere clean-up systems shall have suitable redundancy in components and features to ensure that their safety functions can be accomplished, assuming a single failure<sup>53</sup>.
  - 6.5.12.3 Filter facilities intended for accident conditions shall be separately located. They shall not be in continuous use during normal operation.

6.5.12.4 The design of the plant shall be such that following an accident, it is possible to isolate all sources of compressed air and other non-condensable gases leading into the containment atmosphere, other than those required for the operation of necessary equipment.

#### 6.5.13 Coverings and Coatings

The coverings and coatings for components and structures within the containment system and their methods of application shall ensure fulfillment of their safety functions under all operational states and accident conditions and to minimise interference with other safety functions in the event of deterioration.

### **6.6 Instrumentation and Control**

#### 6.6.1 General Requirements for Instrumentation and Control (I&C) Systems Important to Safety

6.6.1.1 Instrumentation shall be provided to monitor process variables and status of systems for all plant states as appropriate to assure adequate information on plant status. Instrumentation shall be provided for measuring all main process variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment and for obtaining any plant information required for the reliable and safe operation of the plant<sup>59</sup>. The instrumentation and control system shall incorporate adequate redundancy and diversity to achieve the required reliability. Recording of measurements of process variables important to safety shall be provided<sup>39</sup>.

6.6.1.2 Appropriate and reliable controls shall be provided to maintain process variables, referred in subsection 6.6.1.1 above, within prescribed operating ranges.

6.6.1.3 Instrumentation and recording equipment shall be provided to ensure that essential information is available to monitor the course of design basis accidents and the status of essential equipment and for predicting, as far as is necessary for safety, the locations and quantities of radioactive materials that could escape from their locations intended in the design. The instrumentation and recording equipment shall be adequate to provide information, as far as practicable, about the status of the plant during severe accidents and for decisions during accident management.

#### 6.6.2 Periodic Testing and Maintenance

---

<sup>59</sup> Refer AERB safety guide on 'Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants' (AERB/NPP-PHWR/SG/D-20).

- 6.6.2.1 Design and layout of instrumentation systems shall be such as to permit periodic testing, calibration and maintenance<sup>22</sup>.
- 6.6.3 Instrument Power Supply System
  - Instrument power supplies, both pneumatic and electrical, shall be designed, installed and tested to ensure adequate availability and reliability<sup>60</sup>.
- 6.6.4 Control Room
  - 6.6.4.1 A control room shall be provided from where the plant can be safely operated in all its operational states, and from where it can be brought and maintained in the safe state after the onset of accident conditions (ref. clauses 5.2.9.1 to 5.2.10.1). Appropriate measures shall be taken and adequate information provided to safeguard the occupants of the control room against resulting hazards, such as undue radiation resulting from an accident condition, release of radioactive material, and explosive or toxic gases and fire, that could jeopardise habitability of control room (for necessary operator actions).
  - 6.6.4.2 Displays in the control room shall provide the operator with adequate and comprehensive information of 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 states of all safety systems during all operational states and accident conditions. Also, if any part of the safety systems has been temporarily rendered inoperative for testing, it should be done under administrative control and the bypass shall be displayed in the control room.
  - 6.6.4.3 Devices shall be provided to give in an efficient way visual and if appropriate also audible indications of operational conditions and processes that have deviated from normal and could impair safety.
  - 6.6.4.4 Ergonomics shall be taken into account in the control room design.
  - 6.6.4.5 Special attention shall be given to identifying those events, both internal and external to control room, which may pose a direct threat to its continued availability, and the design shall include reasonably practicable measures to minimise the effects of such events.
- 6.6.5 Backup Control Room

---

<sup>60</sup> Refer AERB safety guide on 'Emergency Electric Power Supply System for Pressurised Heavy Water Reactors' (AERB/SG/D-11).

- 6.6.5.1 Sufficient instrumentation and control equipment shall also be located, preferably at a single location, that is physically and electrically separated from the control room, so that the reactor can be placed and maintained in a shutdown state, residual heat removed, and the essential plant variables monitored should there be a loss of ability to perform these essential safety functions from the control room. The backup control room will meet the design requirements of the control room with respect to safety classification, seismic category, single failure criterion and radiation shielding. In view of identical design safety features in both the control rooms, control transfer from the control room is not needed to perform operations from the backup control room, even in case of unavailability of the control room.
- 6.6.6 Use of Computer in Systems Important to Safety
- 6.6.6.1 When computer based systems are employed for safety and safety related functions, the dependability of computer based systems shall be ensured by following a systematic, fully documented and reviewable engineering process during the design, fabrication, integration and commissioning. As software faults could result from errors in requirements, design or implementation, a software quality assurance plan involving verification and validation shall be followed during entire software as well as hardware development cycle<sup>61</sup>.
- 6.6.6.2 The level of reliability of computer based systems shall be commensurate with the safety importance of the system<sup>39</sup>. As software is not amenable to quantitative assessment of reliability, testing, analysis, and product documentation, inspection shall be performed to achieve high level of assurance.
- 6.6.6.3 Computer based systems shall be designed to have the fault tolerance commensurate with the safety category of the system. It should have self-diagnostic features. It shall have maintainability features. Security features for access to computer system shall be provided.
- 6.6.7 Automatic Control
- Various safety actions shall be automated such that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or design basis accidents, and in addition appropriate information shall be available to the operator to monitor the effect of the automatic actions.
- 6.6.8 Protection System Functions

---

61 Refer AERB safety guide on 'Computer-based Safety Systems of Pressurised Heavy Water Reactors' (AERB/NPP-PHWR/SG/D-25) (Under Preparation).

#### 6.6.8.1 General Requirements

- (a) The protection system is provided to maintain safety in situations in which the control systems are not able to maintain the plant variables within acceptable values. The protection system in conjunction with safety actuation systems and safety system support features perform all safety tasks that may become necessary.
- (b) The protection system shall be designed<sup>39</sup> to:
  - (i) detect and initiate automatically the operation of appropriate systems, including, as necessary, reactor shutdown systems, in order to ensure that the specified fuel design limits are not exceeded as a result of anticipated operational occurrences;
  - (ii) detect design basis accidents and initiate automatically operation of system necessary to limit the consequences of such accidents within the design basis; and
  - (iii) be capable of overriding unsafe actions of the control systems.

#### 6.6.8.2 Reliability and Testability of the Protection System

- (a) The protection system shall be designed for high functional reliability and periodic testability<sup>22</sup> commensurate with the safety function(s)<sup>9</sup> to be performed. Redundancy and independence designed into the protection system shall be sufficient<sup>39</sup> at least to ensure that:
  - (i) no single failure results in loss of protection function;
  - (ii) 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;
  - (iii) effects of natural phenomena and postulated accident conditions on any channel do not result in loss of the protection system function; and
  - (iv) it is fail safe.
- (b) The protection system shall be designed to ensure that the effects of all plant states on redundant channels do not result in loss of its function, or it shall be demonstrated to be acceptable otherwise<sup>39</sup>. Design techniques such as testability, including a self-checking capability where necessary, fail-safe behaviour, functional diversity, and diversity in component design or principles of operation shall be used to the extent practical to prevent loss of a protection function<sup>59</sup>.
- (c) Unless adequate reliability is obtained by some other means, the

protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including the possibility of testing channels independently to determine failures and losses of redundancy that may have occurred. The design shall permit all aspects of functionality from the sensor to the input signal to the final actuator to be tested during operation.

- (d) The design shall be such as to minimise the likelihood of operator actions defeating the effectiveness of the protection system in all plant states, but not negating correct operator actions in design basis accidents.

#### 6.6.8.3 Use of Computer Based Systems in Protection

Where a computer-based system is intended to be used in a protection system, the following requirements shall supplement those of paragraphs 6.6.6.1 to 6.6.6.359:

- (i) The highest quality and practices for the hardware and software shall be applied.
- (ii) The whole development process, including control, testing and commissioning of the design changes, shall be systematically documented and reviewable.
- (iii) In order to confirm confidence in the computer based systems reliability, an assessment of the computer-based system by expert personnel independent of the designers and suppliers shall be undertaken; and
- (iv) Where the required system integrity cannot be demonstrated with a high level of confidence, a diverse means of ensuring the protection functions shall be provided.

#### 6.6.8.4 Separation of Protection and Control Systems

Interference between the protection system and the control systems shall be prevented by avoiding interconnections or by suitable functional isolation. If common signals are used in both the protection system and any control system, appropriate separation<sup>62</sup> shall be ensured and it shall be demonstrated that all safety requirements of paragraphs 6.6.8.1 to 6.6.8.3 are met.

### 6.7 Emergency Control Centre

An emergency control centre, separated from the plant control room, shall be

---

62 e.g. by adequate isolation.



provided to serve as meeting place for the emergency staff who will operate from there in the event of an emergency. Information about important plant parameters and the radiological situation in the plant and its immediate surroundings should be available there. The room should provide means for communication with the control room, the backup control room, and other important points in the plant and the emergency organisations. Appropriate measures shall be taken to protect the occupants for a protracted time against radiological hazards resulting from severe accidents<sup>63</sup>.

## **6.8 Electrical Power System**

### **6.8.1 General Requirements**

- 6.8.1.1 Electric power system shall comprise off-site supplies and on-site including emergency power supply system. The systems shall be designed, installed, tested, operated and maintained to permit functioning of structures, systems and components important to safety during all plant states<sup>59</sup>.
- 6.8.1.2 Functional adequacy of both off-site and on-site systems shall be assured by having adequate capacity, redundancy, independence and testability<sup>59</sup>.
- 6.8.1.3 Consideration should be given for emergency power supply system for severe accident as per subsection 5.2.11.

### **6.8.2 Off-Site Power System**

Electric power from the transmission network to the on-site electric distribution system shall be supplied by two physically independent circuits. These should be designed and located so as to minimise the probability of their simultaneous failure during normal operation and under accident conditions. Switchyard common to both circuits is acceptable. 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<sup>59</sup>.

### **6.8.3 Emergency Power Supply System**

- 6.8.3.1 Various systems and components important to safety require emergency power following some PIEs. 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<sup>35</sup>.

---

<sup>63</sup> Refer AERB safety guide on 'Preparedness of the Operating Organisation for Handling Emergencies at Nuclear Power Plants' ( AERB/SG/O-6).

- 6.8.3.2 Various means of supplying emergency power are available<sup>64</sup>. Power may be supplied directly to the driven equipment or through an emergency electric power system.
- 6.8.3.3 The emergency electrical loads shall be identified; 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.
- 6.8.4 Inspection of Emergency Power Supply Systems
- The system shall be designed with a provision to test periodically<sup>60</sup>:
- (i) the operability and functional performance of the components of the on-site power systems;
  - (ii) operability of the system as a whole and the full operational sequence that brings the system into operation.

## **6.9 Radioactive Waste Treatment and Control Systems**

### 6.9.1 Radioactive Waste Treatment

- 6.9.1.1 Adequate systems shall be provided to treat the radioactive liquid and gaseous effluents in order to keep the quantity and the concentration of radioactive discharge within prescribed limits<sup>29</sup>. ALARA principle should be applied.
- 6.9.1.2 Adequate systems shall be provided for the handling of radioactive solid or concentrated wastes and safely storing them for a reasonable period of time, on the site. Transportation of solid wastes from the site shall be accomplished according to the decisions of the regulatory body. Adequate consideration should be given to make provision for handling waste generated during decommissioning<sup>29</sup>.

### 6.9.2 Control of Release of Radioactive Liquid Effluents to the Environment

Provisions shall be made for processing and release of the liquid effluents that may be generated during normal operation and during and following accident conditions satisfying the radiological limits specified by the design based on the prescribed limits.

### 6.9.3 Control of Airborne Radioactive Substances

A ventilation system with appropriate filtration shall be provided to:

---

<sup>64</sup> e.g. water, steam or gas turbines, diesel engines and batteries.

- (i) prevent unacceptable dispersion of airborne radioactive substances within the plant,
- (ii) reduce the concentration of airborne radioactive substances to levels<sup>65</sup> compatible with access requirements of the particular area<sup>2</sup>,
- (iii) keep the level of airborne radioactive substances in the nuclear power plant below prescribed limits<sup>2</sup>, the ALARA principle being applied in normal operation and anticipated operational occurrences<sup>61</sup>,
- (iv) ventilate rooms containing inert or noxious gases without impairing the ability to control radioactive releases<sup>65</sup>,
- (v) ensure flow of air from low activity zones to high activity zones<sup>2</sup>, and
- (vi) maintain reactor containment building under negative pressure.

Filter systems shall be sufficiently reliable and so designed that under the expected prevailing conditions the necessary retention factors are achieved. Filter systems shall be designed such that their efficiency can be periodically tested during normal operation of the plant.

#### 6.10 Fuel Handling and Storage Systems

Fuel handling and storage system includes equipment, structures and tools for fuel transfer and fuel storage.

Fuel handling and storage systems shall be designed to assure adequate safety under normal and accident conditions<sup>51</sup>.

##### 6.10.1 New Fuel Handling and Storage

The new fuel handling and storage systems shall be designed:

- (i) with a capability to permit appropriate maintenance and periodic inspection and testing of components important to safety,
- (ii) to minimise the probability of loss or damage to the fuel, and
- (iii) to provide for identification of fuel bundles.

##### 6.10.2 Spent Fuel Handling and Storage

The spent fuel handling and storage systems shall be designed:

- (i) with adequate heat removal capability under all operational states and accident conditions<sup>51</sup>,

---

<sup>65</sup> Refer AERB safety guide on 'Control of Air-borne Radioactive Materials in Pressurised Heavy Water Reactors' (AERB/SG/D-14).

- (ii) with a capability to permit appropriate periodic inspection and testing of components important to safety,<sup>22</sup>
- (iii) with adequate shielding for radiation protection under all handling and storage conditions during operational states and accident conditions,
- (iv) with appropriate systems to detect conditions that may result in loss of heat removal capability and excessive radiation levels and to initiate appropriate safety action (particular mention may be made for monitoring and control of water level in the fuel storage bay and leak detection),
- (v) to prevent dropping of fuel bundle during handling,
- (vi) to ensure that fuel bundle is not stuck during fuel transfer,
- (vii) to prevent unacceptable handling loads on fuel bundles during handling,
- (viii) to prevent the inadvertent dropping of heavy objects like cask or crane on the fuel bundle or in the spent fuel bays,
- (ix) with a capability to inspect, identify and to store suspected and damaged fuel bundle,
- (x) with means for controlling the chemistry and activity of any water in which spent fuel bundle is handled or stored,
- (xi) with a capacity to accommodate one full core fuel discharge, under all conditions,
- (xii) to facilitate maintenance of fuel handling system and inspection bay equipment,
- (xiii) to ensure that adequate operating and accounting procedures can be implemented to prevent and detect unauthorised removal of fuel,
- (xiv) with means to maintain at least the minimum required water level in spent fuel bays in the event of pipe breaks (antisiphon measures),
- (xv) with means to prevent sliding and overturning of stacks of fuel trays, and
- (xvi) to facilitate decontamination of inspection bay and its equipment when required.

## **6.11 Radiation Protection**

### **6.11.1 General Requirements**

Radiation protection is directed to avoid unnecessary radiation exposures and to keep unavoidable exposures as low as reasonably achievable. This objective shall be accomplished in the design<sup>2</sup> by:

- (i) appropriate layout and shielding of structures, systems, and components containing radioactive materials,
- (ii) giving due attention to the design of the plant and equipment so as to reduce the duration of exposure and number of site personnel exposed to radiation or contamination,
- (iii) minimising leakage from systems having heavy water and associated cover gas,
- (iv) making the provision for collection and segregation of radioactive materials in an appropriate form and condition, either for their disposal on the site or for their removal from the site, and
- (v) making arrangements to control, minimise the quantity and concentration of radioactive materials spread within the plant or released to the environment.

Full account shall be taken of the build-up of radiation levels with time in areas of personnel occupancy and the generation of radioactive materials as wastes.

#### 6.11.2 Design for Radiation Protection

- 6.11.2.1 The plant shall be designed to limit radiation exposures, both within and outside the plant to prescribed limits for the operational states and to acceptable levels for accident conditions<sup>2</sup>.
- 6.11.2.2 Suitable provisions shall be made in the design and layout of the plant to minimise exposure and contamination from all sources. Such provisions shall include adequate design of systems and components in terms of minimising exposure during maintenance and inspection, shielding from direct and scattered radiation, ventilation and filtration for control of airborne activity, reduction of corrosion product activation by proper specification of material, tritium removal to maintain activity level below specific value in moderator system means of monitoring and control of access to the plant.
- 6.11.2.3 The shielding shall be such that radiation levels in operating areas do not exceed the prescribed limits, and shall facilitate maintenance and inspection so as to minimise exposure of maintenance personnel. In addition, the ALARA principle shall be applied.
- 6.11.2.4 The plant area should have defined radiation zones based on levels of contamination and radiation levels, each having appropriate control of access, occupancy and need for protective clothing. Inter-zonal monitors should be installed for monitoring surface contamination from the movement of materials and personnel within the plant. The plant layout shall provide for efficient

operation, inspection, maintenance and replacement as necessary to minimise radiation exposure.

- 6.11.2.5 Provision shall be made for appropriate decontamination facilities, for both personnel and equipment, and for handling any radioactive waste arising from decontamination activities.
- 6.11.2.6 Access control provisions (interlocks, turnstiles, locked gates) and procedures shall exist for entering into areas where activity levels are expected to be high. Areas requiring personnel occupation<sup>66</sup> 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, etc..
- 6.11.2.7 Appropriate provisions and procedures should exist for the measurement of radiation doses to individuals (personnel dosimeters) for assessment of exposures of personnel, engaged in operation and maintenance activities.
- 6.11.3 Radiation Monitoring
  - 6.11.3.1 Equipment shall be provided to ensure adequate radiation protection surveillance in operational states, accident conditions and as practicable during severe accidents<sup>59</sup>.
  - 6.11.3.2 The nuclear power plant shall provide suitable means for on-line monitoring and recording of the release of radioactive liquids and gases to the environment. This shall include an integrated monitoring and recording system for the stack effluent for identified radionuclides<sup>67</sup>.
  - 6.11.3.3 The final exit point from the plant shall have a portal monitoring system for monitoring surface contamination (hand, foot and body) with provision for alarm to ensure that persons, materials with contamination do not leave the plant.
  - 6.11.3.4 In addition to monitoring within the plant, means to measure meteorological parameters and arrangements shall also be provided to determine the radiological impact, if any, in the vicinity of the plant.

---

66 e.g., during maintenance and in-service inspection.

67 Like Iodine (I131), tritium, particulates and gaseous fission products.

## APPENDIX

### LIST OF SAFETY FUNCTIONS

A list of safety functions,<sup>4</sup> performed by various SSCs, is given below. For classification, each SSC is identified with related safety functions in this list. The serial designation (a, b, c, etc.) assigned to the safety functions below are referred to later at various places in AERB safety guides for reference purposes.

- (a) To prevent unacceptable reactivity transients.
- (b) To maintain the reactor in a safe shutdown condition after all shutdown actions.
- (c) To shut down the reactor as required to prevent anticipated operational occurrences from leading to accident conditions and to shutdown the reactor to mitigate the consequences of accident conditions (see also (d)).
- (d) To shut down the reactor on sensing a loss-of-coolant accident.
- (e) To maintain sufficient reactor coolant inventory for core cooling during and after all operational states.
- (f) To remove heat from the core after a failure of the reactor coolant pressure boundary in order to limit fuel damage.
- (g) To remove decay heat during appropriate operational states and accident conditions with the reactor coolant pressure boundary intact.
- (h) To transfer heat from other systems to the ultimate heat sink.
- (i) To ensure necessary services (e.g., electric, pneumatic, hydraulic power supplies, lubrication) as a support function for the safety systems.
- (j) To maintain acceptable integrity of the cladding of the fuel in the reactor core.
- (k) To maintain the integrity of the reactor coolant pressure boundary.
- (l) To limit the release of radioactive material from the reactor containment during and after an accident.
- (m) To keep the radiation exposure of the public and site personnel within acceptable limits during and after accident conditions that release radioactive materials from sources outside the reactor containment.
- (n) To limit the discharge or release of radioactive waste and airborne radioactive material below the prescribed limits during all operational states.
- (o) To control environmental conditions within the nuclear power plant for operation of safety systems and for personnel habitability necessary to allow performance of operations important to safety.
- (p) To control radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, during all operational states.

- (q) To remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site.
- (r) To maintain sufficient sub-criticality of the fuel stored outside the reactor coolant system but within the site.
- (s) To prevent the failure or limit the consequences of failure of a component or structure which would cause the impairment of a safety function.
- (t) To provide information and control capabilities for specified manual actions required to mitigate the consequences of a PIE and prevent it from leading to a significant sequence<sup>68</sup>.
- (u) To continuously monitor the systems to accomplish their protective and mitigating safety functions or to alert the control room staff of failures in these systems.
- (v) To control the plant so that the process variables are maintained within the limits assumed in the safety analysis.
- (w) To limit the consequences of events such as a fire or flood.

---

68 A credible series or set of events that would result in unacceptable consequences such as:

- (i) unacceptable radioactive release at the site or into the wider environment. This might be either a massive, uncontrolled release at a frequency that is outside the NPP design basis, or release at a frequency that is within the design basis but exceeding specified magnitude and/or frequency limits;
- (ii) unacceptable fuel damage. There might be damage to the fuel clad that leads to an unacceptable increase in the activity of the primary coolant, or structural damage to the fuel that impairs the ability to cool it.



## REFERENCES

1. ATOMIC ENERGY REGULATORY BOARD; 'Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants'; AERB Safety Code No. AERB/SC/D, Mumbai, India (1989).
2. INTERNATIONAL ATOMIC ENERGY AGENCY; 'Safety of Nuclear Power Plants: Design Requirements'; IAEA Safety Standards Series No. NS-R-1, IAEA Vienna (2000).
3. ATOMIC ENERGY REGULATORY BOARD, 'AERB Safety Directive 2/91'; Mumbai, India (1991).
4. INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, '1990 Recommendations of the International Commission on Radiological Protection, Publication No. 60', Pergamon Press, Oxford and New York (1991).
5. DEPARTMENT OF ATOMIC ENERGY, 'Atomic Energy (Radiation Protection) Rules, 2004', Mumbai, India (2004).
6. ATOMIC ENERGY REGULATORY BOARD, 'Quality Assurance in Nuclear Power Plants'; AERB Safety Code No. AERB/SC/QA (Rev. 1); Mumbai, India (2009).
7. ATOMIC ENERGY REGULATORY BOARD, 'Intervention Levels and Derived Intervention Levels for Off-site Radiation Emergency' AERB Safety Guide No. AERB/SG/HS-1; Mumbai, India (1992)
8. ATOMIC ENERGY REGULATORY BOARD; 'Code of Practice on Safety in Nuclear Power Plant Siting', AERB Safety Code No. AERB/SC/S; Mumbai, India (1990)
9. DEPARTMENT OF ATOMIC ENERGY; 'Atomic Energy (Factories) Rules , 1996'; Mumbai, India (1996).
10. ATOMIC ENERGY REGULATORY BOARD; 'Nuclear Power Plant Operation'; AERB Safety Code No. AERB/NPP/SC/O (Rev. 1); Mumbai, India (2008).
11. ATOMIC ENERGY REGULATORY BOARD; 'Civil Engineering Structures Important to Safety of Nuclear Facilities', AERB Safety Standard No. AERB/SS/CSE; Mumbai, India (1998)
12. ATOMIC ENERGY REGULATORY BOARD; 'Glossary of Terms for Nuclear and Radiation Safety', AERB Safety Guide No. AERB/SG/GLO; Mumbai, India (2005)

## LIST OF PARTICIPANTS

### WORKING GROUP

Dates of meeting : May 2, 3 & 4, 2000  
May 5, 8 & 9, 2000  
May 11 & 15, 2000  
May 16, 17 & 18, 2000  
August 15, 2000  
November 1, 2 & 3, 2000  
November 9, 2000  
May 18, 2001  
February 10, 2002  
April 6, 2009

### Members and Invitees of the Working Group:

Shri V.K. Mehra (Chairman) : BARC  
Shri S. Damodaran : NPCIL (Former)  
Shri S.A. Bhardwaj : NPCIL  
Shri S.G. Ghadge : NPCIL  
Shri C.K. Pithawa : BARC  
Shri S.A. Khan (Member-Secretary) : AERB  
Late Shri C.N. Bapat (Co-opted) : NPCIL (Former)  
Dr. S.K. Gupta (Co-opted) : AERB  
Shri Deepak De (Invitee) : AERB (Former)  
Shri A.K. Babar (Invitee) : BARC  
Shri V.V.S. Sanyasi Rao (Invitee) : BARC  
Shri U.C. Muktibodh (Invitee) : NPCIL



## **ADVISORY COMMITTEE ON NUCLEAR SAFETY (ACNS)**

Dates of meeting: April 13, 2006  
April 18, 2006  
May 11, 2006  
June 07, 2006  
November 27, 2008  
March 30, 2009

### **Members of ACNS:**

Shri G.R. Srinivasan (Chairman)	:	AERB (Former)
Shri S.C. Hiremath	:	HWB (Former)
Shri S.S. Bajaj	:	NPCIL (Former)
Shri R.K. Sinha	:	BARC
Shri H.S. Kushwaha	:	BARC
Prof. J.B. Doshi	:	IIT, Bombay
Shri A.K. Anand	:	BARC (Former)
Shri D.S.C. Purushottam	:	BARC (Former)
Shri S. Krishnamony	:	BARC (Former)
Dr. S.K. Gupta	:	AERB
Shri K. Srivasista (Member-Secretary)	:	AERB

**PROVISIONAL LIST OF SAFETY CODES, GUIDES AND  
MANUALS ON DESIGN OF PRESSURISED HEAVY  
WATER REACTOR BASED NUCLEAR POWER PLANTS**

<b>S.No.</b>	<b>Safety Series No.</b>	<b>Titles</b>
1	AERB/SC/D	Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants
2	AERB/NPP-PHWR/SC/D (Rev.1)	Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants
3	AERB/NPP-PHWR/SG/D-1	Safety Classification and Seismic Categorisation for Structures, Systems and Components of Pressurised Heavy Water Reactors
4	AERB/SG/D-2	Structural Design of Irradiated Components of Pressurised Heavy Water Reactors (Under Preparation)
5	AERB/SG/D-3	Protection Against Internally Generated Missiles and Associated Environmental Conditions in Pressurised Heavy Water Reactors (Under Preparation)
6	AERB/SG/D-4	Fire Protection in Pressurised Heavy Water Reactor Based Nuclear Power Plants
7	AERB/SG/D-5	Design Basis Events for Pressurised Heavy Water Reactors
8	AERB/NPP-PHWR/SG/D-6	Fuel Design for Pressurised Heavy Water Reactors
9	AERB/SG/D-7	Core Reactivity Control in Pressurised Heavy Water Reactors
10	AERB/NPP-PHWR/SG/D-8	Primary Heat Transport System for Pressurised Heavy Water Reactors
11	AERB/NPP-PHWR/SG/D-10	Safety Systems for Pressurised Heavy Water Reactors
12	AERB/SG/D-11	Emergency Electric Power Supply Systems for Pressurised Heavy Water Reactors
13	AERB/NPP-PHWR/SG/D-12	Radiation Protection Aspects in Design for Pressurised Heavy Water Reactor Based Nuclear Power Plants
14	AERB/SG/D-13	Liquid and Solid Radioactive Waste Management in Pressurised Heavy Water Reactor Based Nuclear Power Plants

**PROVISIONAL LIST OF SAFETY CODES, GUIDES AND  
MANUALS ON DESIGN OF PRESSURISED HEAVY  
WATER REACTOR BASED NUCLEAR POWER PLANTS  
(CONT.)**

<b>S.No.</b>	<b>Safety Series No.</b>	<b>Titles</b>
15	AERB/SG/D-14	Control of Airborne Radioactive Materials in Pressurised Heavy Water Reactors
16	AERB/SG/D-15	Ultimate Heat Sink and Associated Systems in Pressurised Heavy Water Reactors
17	AERB/SG/D-16	Material Selection and Properties for Pressurised Heavy Water Reactors (Under Preparation)
18	AERB/SG/D-17	Design for In-Service Inspection of Pressurised Heavy Water Reactors (Under Preparation)
19	AERB/SG/D-18	Loss of Coolant Accident Analysis for Pressurised Heavy Water Reactors
20	AERB/SG/D-19	Deterministic Safety Analysis of Pressurised Heavy Water Reactor Based Nuclear Power Plants (Under Preparation)
21	AERB/NPP-PHWR/SG/D-20	Safety Related Instrumentation and Control for Pressurised Heavy Water Reactor Based Nuclear Power Plants
22	AERB/NPP-PHWR/SG/D-21	Containment System Design for Pressurised Heavy Water Reactors
23	AERB/SG/D-22	Vapour Suppression System (Pool Type) for Pressurised Heavy Water Reactors
24	AERB/NPP-PHWR/SG/D-23	Seismic Qualification of Structures, Systems and Components of Pressurised Heavy Water Reactors
25	AERB/SG/D-24	Design of Fuel Handling and Storage Systems for Pressurised Heavy Water Reactors
26	AERB/SG/D-25	Computer Based Safety Systems of Pressurised Heavy Water Reactors (Under Preparation)
27	AERB/NPP-PHWR/SM/D-2	Hydrogen Release and Mitigation Measures under Accident Conditions in Pressurised Heavy Water Reactors
28	AERB/NPP-PHWR/TD/D-1	Decay Heat Load Calculations in Pressurised Heavy Water Reactors (Under Preparation)

**AERB SAFETY CODE NO. AERB/NPP-PHWR/SC/D (Rev. 1)**

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