



GOVERNMENT OF INDIA

AERB SAFETY GUIDE

DESIGN BASIS EVENTS FOR WATER COOLED NUCLEAR POWER PLANTS



ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY GUIDE NO.AERB/NPP-WCR/SG/D-5 (Rev.1)

**DESIGN BASIS EVENTS FOR
WATER COOLED NUCLEAR POWER PLANTS**

Atomic Energy Regulatory Board

Mumbai - 400 094.

India

July 2020

Price:

Orders for this Guide should be addressed to:

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

FOREWORD

Activities concerning establishment and utilization 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 has, therefore, undertaken a programme of developing safety standards, safety codes, 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, the 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 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.

The AERB Safety Codes on Design of Light Water Reactor and Pressurized Heavy Water Reactor type NPPs (AERB/NPP-LWR/SC/D and AERB/NPP-PHWR/SC/D Rev.2) lays down the minimum requirements for ensuring adequate safety in design of nuclear power plants. This safety guide is one of the series of guides, to describe and elaborate on the specific parts of the safety code. It prescribes the guidelines for identification, categorization and classification of postulated initiating events including multiple failures. This revised safety guide supersedes AERB Safety Guide on 'Design Basis Events (AERB/SG/D-5)', published in 2000.

In drafting this guide, the relevant International Atomic Energy Agency (IAEA), especially IAEA safety guide IAEA/SSG-2 and other relevant international documents have been referred / looked into. Necessary references to existing AERB regulations, in the form of codes and design guides, have been made to keep it in line with the regulatory expectations. References are included to provide information that might be helpful to the user.

The initial draft of the guide has been prepared in-house. Experts have reviewed the draft and the Advisory Committee on Nuclear and Radiation 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 persons, who have participated in this task, along with their affiliations, is included for information.


(G. Nageswara Rao)
Chairman, AERB

SPECIAL DEFINITIONS

Beyond Design Basis Accident

This term is superseded by Design Extension Conditions.

Design Basis Accident (DBA)

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

Design Extension Conditions (DECs)

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

Design Basis Events (DBEs)

The set of events that serve as part of the basis for the establishment of design requirements for structures, systems and components within a facility. Design basis events (DBEs) include normal operations, operational transients and certain accident conditions under postulated initiating events (PIE) considered in the design of the facility. This includes DBAs and DECs.

Event

Occurrence of an unplanned activity or deviations from normalcy. It may be a single occurrence or a sequence of related occurrences. Depending on the severity in deviations and consequences event may be classified as anomaly, incident or accident in ascending order.

For the purpose of this guide “Event” includes “Postulated Initiating Event” as well as “Event Sequence”

Multiple Failures

Multiple failure events to be considered at the design stage are characterized as:

- i) A postulated common cause failure or inefficiency of all redundant trains of a safety system¹ needed to fulfil a safety function necessary to cope with an anticipated operational occurrence (AOO) or a single PIE (see examples in Table 1 below),

¹ **Safety system:** A system important to safety, provided to ensure the safe shut-down of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

Safety systems consist of the protection system, the safety actuation systems and the safety system support features. Components of safety systems may be provided solely to perform safety functions, or may perform safety functions in some plant operational states and non-safety functions in other operational states.

Or

- ii) A postulated common cause failure of a safety system or a safety related system needed to fulfil the fundamental safety functions in normal operation (see examples in Table 2 below).

Table-1: Examples of postulated common cause failures of safety systems needed to fulfil a safety function necessary to cope with an AOO or a single PIE

Denotation	Initiating Event	Loss of a safety system
LOCA	Small LOCA	Medium head safety injection
	Small LOCA	Low head safety injection
Station blackout	Loss of off-site power	Emergency power supply
Total loss of feed water	Loss of main feed water	Emergency feed water supply
ATWS	Anticipated Transient	Fast shutdown

Table-2: Examples of postulated common cause failures of safety systems needed to fulfil the fundamental safety functions in normal operation

Denotation	Initiating Condition	Loss of a safety system
Loss of RHR	<i>normal operation</i>	Residual heat removal
Loss of UHS	<i>normal operation</i>	Ultimate heat sink
Loss of CCW/ECW	<i>normal operation</i>	Component cooling water / essential cooling water

Postulated Initiating Events (PIEs)

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

Severe Accident

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

Contents

FOREWORD	i
1. INTRODUCTION.....	1
1.1 General	1
1.2 Objectives.....	2
1.3 Scope.....	2
2. IDENTIFICATION OF EVENTS.....	3
2.1 General Criteria.....	3
2.2 Methodology for Identification and Listing of Events.....	5
2.3 Identification of Events Due To Internal and External Hazards	5
2.4 Methodology for Practically Elimination of Events.....	6
2.5 Events/ Phenomena to be Practically Eliminated.....	8
3. CLASSIFICATION AND SELECTION OF EVENTS.....	9
3.1. General	9
3.2. Grouping of Events	10
3.3. Methodology for Classification of Events.....	10
3.4. Events Due to Hazards	14
3.5. Plant States	14
3.5.1 Normal Operation (NO)	15
3.5.2 Anticipated Operational Occurrences (AOO)	15
3.5.3 Design Basis Accidents (DBA).....	16
3.5.4 Design Extension Conditions (DEC)	16
3.5.4.1 Design Extension Conditions without core melt.....	17
3.5.4.2 Design Extension Conditions with core melt	17
3.6. Selection of Events for Safety Analysis.....	18
Appendix-1 on Typical Events List for PHWRs, PWRs and BWRs	22
Appendix-2 Typical List of Internal and External Hazards for NPPs.....	28
BIBLIOGRAPHY	29
LIST OF PARTICIPANTS OF IHWG	31
LIST OF PARTICIPANTS OF TF	31
ACNRS MEMBERS.....	32

1. INTRODUCTION

1.1 General

- 1.1.1 Nuclear Power Plants (NPP) are sited, designed, constructed, commissioned, operated and decommissioned in conformity with the applicable nuclear safety codes and standards. The codes and standards ensure an adequate margin of safety so that NPP is operated without undue radiological risk to the plant personnel, members of the public and environment.
- 1.1.2 Postulated Initiating Events (PIEs) and Event Sequence (ES), henceforth called as 'Events' considered in design of NPPs.. Events may lead to any one of the plant states i.e. Normal Operation², Anticipated Operational Occurrences (AOOs), Design Basis Accidents (DBAs) and Design Extension Conditions (DECs) (The plant states are described in detail in section 3.5). Assessment of the safety of an NPP requires that behaviour of the plant following an event be analysed. Also, Structures Systems and Components should be designed to ensure that under Normal Operation, Anticipated Operational Occurrences and accident conditions, design limits are not exceeded.
- 1.1.3 A systematic approach shall be adopted during the design of the nuclear power plant to identify a comprehensive set of events such that all foreseeable events with a significant frequency of occurrence and all foreseeable events with the potential for significant radiological consequences are anticipated and are considered in the design basis or in the design extension condition. The postulated events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether at full power, low power, refueling or shutdown states. A technically supported justification shall be provided for exclusion from the design of any event that is identified in accordance with the comprehensive set of postulated events. The NPP design shall identify credible design extension conditions, based on operational experience, engineering judgment, and the results of analysis and research. An analysis of design extension conditions for the plant, including assessment of radiological impact, shall be performed
- 1.1.4 There are no firm criteria for identification and categorisation of events; rather the process is a combination of iteration between design and analysis, engineering judgement and experience of previous NPP design and operation.
- 1.1.5 This Safety Guide considers the experience of current designs of Pressurised Heavy Water Reactor (PHWR), Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR).

² Normal Operation includes Operational Transients

1.2 Objectives

1.2.1 The objective of this guide is to provide guidance on methodology for:

- i. Identification of Events
- ii. Grouping of the identified events
- iii. Classification of events and Categorization in different plant states
- iv. Selection of events for design and analysis
- v. Practical Elimination of certain events.

1.2.2 The objective of this guide is to provide guidance and typical list of events for following types of water cooled NPPs.

- i. PHWR
- ii. PWR
- iii. BWR

1.3 Scope

1.3.1 This guide provides typical lists of events to be considered for safety analysis and design of the water cooled reactors (PHWR, PWR and BWR), as well as methodology of practical elimination of certain events/conditions. However, the Principles instituted in this safety guide may be applied to other types of NPPs as well.

1.3.2 This Safety Guide is based on the current designs of Pressurised Heavy Water Reactors (PHWR), Pressurized Water Reactor (PWR) and Boiling Water Reactor (BWR) in India. If there are any major changes in design of these NPPs or if the operating experience so demands, it may become necessary to revise the typical list of events.

1.3.3 For new type of water cooled reactors, the applicability of the typical lists of events, which are provided in the safety guide, may be checked with the design and if required, additional events may have to be considered based on the methodology provided in the safety guide.

1.3.4 Initiating events resulting from sabotage are out of scope of this safety guide.

2. IDENTIFICATION OF EVENTS

2.1 General Criteria

- 2.1.1 Events originated internally or externally and having a potential for radioactive release to the environment should be identified and appropriately considered for Safety Analysis. This should include events that can lead to a release of radioactivity not only from the reactor core but from other relevant sources such as fuel storage facility at the plant and systems dealing with radioactive materials.
- 2.1.2 The Systems, Structures and Components (SSCs) required for handling of each event should be identified. It should be demonstrated that the SSCs at one level of Defence in Depth (DiD) are independent of other levels, as far as practicable.
- 2.1.3 Single common cause which can result in events in multiple reactors, spent fuel storage facilities and any other sources of potential radioactive releases at a site should also be considered
- 2.1.4 Prediction of the plant behaviour in plant states other than normal operation (i.e. anticipated operational occurrences, design basis accidents and design extension conditions) should be based on a plant specific list of postulated initiating events possibly combined with additional equipment failures or human errors for specific event sequences definition.
- 2.1.5 Erroneous operator action need not be considered separately as a PIE, since operator action could only lead to one of the PIEs described in this Safety Guide.
- 2.1.6 A comprehensive list of events should be prepared to ensure that the analysis of the behaviour of the plant is as complete as possible so that 'all foreseeable events with the potential for serious consequences, all foreseeable events with a significant frequency of occurrence and challenging levels of Defence in Depth³ are anticipated and are considered in the design'.
- 2.1.7 Every configuration of reactor shutdown modes including refuelling and maintenance should be considered. For these modes of operation, contributors for potentially high risk should be considered, such as the inability to start some safety systems automatically or manually; disabled automation systems; equipment under maintenance; reduced amounts of coolant in the primary circuit as well as in the secondary circuit for some modes; instrumentation switched off or non-functional and measurements not made; open primary circuit and open containment.

³ Refer AERB Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D and AERB Safety Code Design Of PHWR Based Nuclear Power Plants AERB/NPP-PHWR/SC/D

- 2.1.8 For events initiated in the spent fuel pool, specific operating modes related to fuel
- 2.1.9 Events potentially taking place during plant operating modes with limited duration in time for example during First Approach to Criticality (FAC) etc. may not be considered after careful analysis and quantitative assessment of its potential of contribution to overall risk.
- 2.1.10 The list of events should take due account of operational experience feedback, this includes, depending on availability of relevant data, operating experience from the actual or from similar nuclear power plants, as applicable.
- 2.1.11 The list of events should be comprehensive and should be defined in such a way that it covers all credible failures, including:
- Failures of SSCs of the plant (partial failure if relevant), including possible spurious actuation,
 - Failures initiated by operator errors, this could range from faulty or incomplete maintenance operations to incorrect settings of control equipment limits or wrong operator actions,
 - Failures of SSCs of the plant arising from internal and external hazards.
- 2.1.12 All consequential failures that a given event could originate in the plant should be considered in the analysis of the plant response as a part of the event. These should include the following:
- If the initiating event is a failure of part of an electrical distribution system, the anticipated operational occurrences, design basis accident or design extension conditions analysis should assume the unavailability of all the equipment powered from that part of the distribution system;
 - If the initiating event is an energetic event, such as the failure of a pressurized system that leads to the release of hot water or pipe whip, anticipated operational occurrences, design basis accident or design extension conditions should consider potential failure of the equipment which could be affected;
 - For internal hazards such as fire or flood and external hazards such as earthquakes or flood, the definition of the induced postulated initiating event should include failure of all the equipment which is neither designed to withstand the effects of the event nor protected from it.
- 2.1.13 The event should only include those failures (including hazards) that directly lead to challenge safety functions and eventually to a threat to barriers against radioactive releases. Therefore any hazards, either internal or external (natural or human induced) should not be considered as events by itself. However, the effects of these hazards should be considered a potential cause of events, which include resulting multiple failures.
- 2.1.14 Failures occurring in the supporting systems that impede the operation of systems necessary for normal operation should be also considered as events if such failures

eventually require the actuation of the protection systems.

- 2.1.15 For a given event, additional credible failure (s) which is not considered as an event dependent failure, including operator errors should also be considered, if its frequency of occurrence is found to be credible and the event is not enveloped by any other event. Resulting event sequences may be appropriately categorised. However these additional failures exclude those that are assumed in safety analysis for conservatism e.g. single failure criteria.
- 2.1.16 List of events should be reviewed periodically throughout plant life, as a minimum, as part of a periodic safety review to look for any additional event based on operating experience feedback or to ensure that earlier postulated events remain valid.
- 2.1.17 Detailed safety analysis may not be required for some of the events. However, the designer should justify why such events need not be considered for specific NPP for safety analysis. Justification could be based on the following: level of defence in- depth; site specific reasons; specific features of design/operation of NPP; operational experience; engineering judgment or probabilistic consideration.
- 2.1.18 Events/Event sequences which could lead to early radioactive release or large radioactive release⁴ should be Practically Eliminated.

2.2 Methodology for Identification and Listing of Events

- 2.2.1 The set of events should be identified in a systematic way. This should include a structured approach to the identification of the events such as:
- Use of analytical methods such as hazard and operability analysis (HAZOP), failure modes and effects analysis (FMEA), engineering judgement and master logic diagrams;
 - Comparison with the list of events developed for safety analysis of similar plants ;
 - Analysis of operating experience data for similar plants;
 - Research and Development
 - Use of deterministic and probabilistic safety analysis insights and results.
- 2.2.2 Based on the above approach an exhaustive list of events should be prepared. Subsequently, the identified events should be grouped and categorized (Ref. Chapter-3 for detailed methodology) to arrive at list of events to be analysed. Typical list of events for different water cooled reactor technologies is given in Appendix -1.

⁴ An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

2.3 Identification of Events due to Internal and External Hazards

- i. Identification of events should consider effects and loads from events caused by relevant internal hazards and site specific external hazards. A typical list of examples of internal and external hazards is given in Appendix -2. The hazards themselves do not represent initiating events but they are associated with loads which can initiate single or multiple events.
- ii. In determination of events caused by site specific hazards for multiple unit plant sites, possibility of impact on several or even all units at the site simultaneously should be taken into account. Specifically, the effects from losing the electrical grid, those from losing the ultimate heat sink and the failure of shared equipment should be taken into account.
- iii. In cases where an event is caused by a hazard, the analysis should only credit SSCs that are qualified for the hazard or protected from the hazard.

2.4 Methodology for Practically Elimination of Events

- 2.4.1 Events that could result in an early radioactive release or a large radioactive release⁵ have to be 'practically eliminated'. The possibility of certain events occurring is considered to have been practically eliminated if it is physically impossible for the conditions /phenomena to occur or if the events can be considered with a high level of confidence to be extremely unlikely to arise.
- 2.4.2 The concept of 'practical elimination' is to be considered as part of a general approach to safety and its appropriate application as an enhancement of defence in depth. The 'practical elimination' is achieved by prevention of the conditions that could lead to an early radioactive release or a large radioactive release.
- 2.4.3 As a first step for the implementation of design provisions for the practical elimination of undesired conditions it is necessary to identify the design provisions for these conditions. A strong design, manufacturing and operation provisions are required for their practical elimination. The practical elimination is a design process followed by the necessary inspection and surveillance processes during manufacturing, construction, commissioning and operation.
- 2.4.4 Following are the broad considerations for safety demonstration towards Practical Elimination of events:

⁵ An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

i. Physical impossibility

Where a claim is made that it is ‘physically impossible’ for the conditions to arise that could lead to an accident condition that needs to be ‘practically eliminated’, it should be examined that the inherent safety features of the system or reactor type to be demonstrated that the event cannot, by the laws of nature, occur and that the fundamental safety functions of reactivity control, heat removal and limitation of accidental radioactive releases will be achieved.

ii Extremely unlikely conditions

- a) Extremely unlikely conditions are generally determined by low probability of occurrence. When it is claimed that a particular accident condition is practically eliminated making use of probabilistic arguments, it should be taken into account that the cumulative contribution of all the different cases must not exceed the target for Large Early Release Frequency (LERF⁶).
- b) Practical elimination of an accident sequence cannot be claimed solely based on compliance with a general cut-off probabilistic value. It should be adequately supported by operational experience, experimental outcomes, international practices for such events and engineering evaluation as applicable.
- c) The necessary high confidence in low likelihood should, wherever possible, be supported by means such as:
 - multiple layers of protection
 - application of the safety principles of independence, diversity, separation, redundancy
 - use of passive safety features
 - use of multiple independent controls
- d) Even if the probability of an accident sequence is very low, additional “reasonably practicable” design features, operational measures or accident management procedures to lower the risk should further be implemented.
- e) Achievement of any probabilistic value cannot be considered a justification for not implementing reasonable design or operational measures, for example, very low probability of occurrence of an accident with core melt is not a reason for not protecting the containment against the conditions generated by such accident. Core melt conditions need to be postulated regardless of the provisions implemented in the design and the energetic phenomena associated with the core melt need to be prevented to exclude containment failure.
- f) It should be ensured that the practical elimination provisions remain in place and

⁶ Section 5.43 of Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

valid throughout the plant lifetime; for example, through in-service and periodic inspections.

- 2.4.5 Accident sequences with core melt resulting from extreme external hazards which would lead to early or large releases should be practically eliminated.
- 2.4.6 Practical elimination concept for extreme external hazards should be treated separately from those associated with internal plant sequences. Practical elimination for external events is site dependent and the requirements prescribe all-risk approach, with appropriate consideration of probability of occurrence, associated uncertainties, and potential consequences, including cliff edge effects. The design of nuclear power plant should address this by providing sufficient safety margins.
- 2.4.7 Based on the above considerations, the practically eliminated events and phenomenon should be identified w.r.t type of design and location of the site and addressed accordingly.

2.5 Events/ Phenomena to be Practically Eliminated

For practical purpose, the cases to be addressed for 'practical elimination' could be grouped within the following five categories:

- 1) Events/Phenomena that could lead to prompt reactor core damage and consequent early containment failure due to :
 - a. Failure of a large component in the reactor coolant system (RCS);
 - b. Uncontrolled Reactivity Accidents;
 - c. Prompt Criticality.
- 2) Severe accident phenomena which could lead to early containment failure due to:
 - a. Direct Containment Heating;
 - b. Large Steam Explosion;
 - c. Hydrogen Detonation.
- 3) Severe accident phenomena which could lead to late containment failure due to:
 - a. Molten Core Concrete Interaction (MCCI);
 - b. Loss of containment heat removal.
- 4) Accident Conditions with Containment Bypass/ Failure of Isolation;
- 5) Significant Fuel Degradation in a Storage Pool.

3. CLASSIFICATION AND SELECTION OF EVENTS

3.1. General

- 3.1.1 The identified events should be classified into representative functional groups and categories corresponding to plant states. Subsequently, the events should be selected from the classified list based on certain criteria for analysis. This chapter provides guidelines for classification of events and then selection of events for deterministic safety analysis. For purpose of Probabilistic Safety Analysis, the listed events in this document can be used, however the required exhaustive list of events should be prepared using a structured approach as described in section 2.2.1 of this document.
- 3.1.2 The plant states shall be identified and grouped into a limited number of categories according to their likelihood of occurrence and DiD level which is required to mitigate such an event. It should be further ensured that there are no, or only minor, potential radiological consequences for all the plant states with a significant likelihood of occurrence.
- 3.1.3 Events should be classified to arrive at plant states (considered in the design) as defined in AERB Safety Code on Design for Light Water Reactors (AERB/NPP-LWR/SC-D) and Design for Pressurized Heavy Water Reactors (AERB/NPP-PHWR/SC/D, Rev. 2)⁷.
- 3.1.4 The plant states considered in design for the deterministic safety analysis should cover:
- a) Normal Operation (NO);
 - b) Anticipated Operational Occurrences (AOO);
 - c) Design Basis Accidents (DBA);
 - d) Design Extension Conditions (DEC), including sequences without core melt and sequences with core melt (severe accident).
- 3.1.5 It may not be practical or necessary to analyze all of the identified events (identified based on the methodology provided in Chapter 2).
- 3.1.6 The identified events should be grouped into functionally representative groups based on similarity of the initiating failures, key phenomena, or system and operator responses, or physical evolution. Examples of event groups include decrease of the reactor coolant inventory, reactivity and power anomalies, and increase/decrease of heat removal. Since plant responses to an event depend on the design and availability of plant systems, the most suitable classification of events may vary.
- 3.1.7 The grouped events should then be categorised into plant states to be analysed as indicated in 3.1.4 above considering the frequency of occurrence and Defence in Depth levels.

⁷ Presently in a Draft Stage

- 3.1.8 Events within each category of plant states should have same acceptance criteria, assumptions (level of conservatism), type of initial and boundary conditions and analysis methodology⁸. The detailed guidance on classification of events is given in section 3.3.
- 3.1.9 The identified events which are not considered for analysis should be justified and the consequences of such events should be enveloped by other bounding representative event .The detailed guidance on grouping of events is given in section 3.2 below.

3.2. Grouping of Events

Events should be grouped into functionally representative groups taking into account possible physical evolution of the event scenario. The focus is on reduced core cooling, possible reactivity addition, effect on primary pressure boundary, containment pressurization and radiological consequences. Following is the typical list of functional grouping of events

- a) Increase in heat removal;
- b) Decrease in heat removal;
- c) Increase of primary coolant system inventory;
- d) Decrease of primary coolant system inventory;
- e) Decrease of the primary coolant system flow rate;
- f) Anomalies in reactivity and power distribution in the reactor core;
- g) Leaks inside and outside containment;
- h) Fresh or spent fuel storage related events;
- i) Refueling related events;
- j) Release of radioactive material from a subsystem or component (typically from treatment or storage systems for radioactive waste);
- k) Malfunction of support or auxiliary systems.

The typical list of events for PHWR, PWR and BWR is provided in Appendix 1. The list serves as a typical example and may be supplemented or modified based on actual NPP design and new developments.

3.3. Methodology for Classification of Events

- 3.3.1 The plant states shall be identified and grouped into a limited number of categories according to their likelihood of occurrence⁹. The categories typically cover normal operation, anticipated operational occurrences, design basis accidents and design extension conditions, including severe accidents with significant degradation of the reactor core which are co-related to DiD levels¹⁰.

⁸ Detailed guidelines are given in Safety Guide on Safety Analysis for PHWRs No. AERB/NF/SG/D-19.

⁹ Section 5.1 Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

¹⁰ Section 2.4.2 Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

- 3.3.2 Application of the concept of defence in depth in the design of a nuclear power plant provides several levels of defence (inherent features, equipment, adequate design margin and procedures) aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails.
- 3.3.3 It is to be ensured that, plant state resulting in high radiation doses or radioactive releases are of very low likelihood of occurrence and plant state with significant likelihood of occurrence have only minor or no radiological consequences. For the purpose of this guide the ‘likelihood of occurrence’ is taken as ‘frequency of occurrence’.
- 3.3.4 DiD approach provides realistic representation of all features at various DiD levels, which can be directly correlated with different plant states. In general, frequency of occurrence of an event at higher¹¹ level of DiD is low while at lower level of DiD, it is relatively high. In the higher frequency domain the uncertainties are low but it increases in domain of low frequency especially in multiple failures. Therefore, an approach of frequency informed and DiD based has been followed for classification of events.
- 3.3.5 The identified events are categorized into plant states using the ‘frequency informed and Defence in Depth based’ approach. This approach is explained in Section 3.3.6 and the correlation of plant states with defence in depth level and frequency of occurrence is shown below in Table 3:

Table-3: Correlation of Plant States with DiD level and frequency of occurrence

Plant State (considered in design)	Defence in Depth Level	Illustrative Range of Frequency of Occurrence (per year)	Event Category	Remarks
Normal Operation	I	-	1	Normal Operation includes Operational Transients
Anticipated Operational Occurrences	II	$10^{-2} \leq f$	2	Single initiating event
Design Basis Accidents	III	$10^{-6} \leq f < 10^{-2}$	3	Single initiating event
Design Extension Conditions ¹² (without core melt)	IV	$f < 10^{-4}$	4A	'Multiple Failure' and rare external events

¹¹ Higher DiD refers to higher level of DiD that is towards level 5

¹² All DEC's do not result in higher radiological consequence. DEC's, as per its characterization, are multiple failures.

Design Extension Conditions (with core melt)		$f < 10^{-6}$	4B	Event sequences leading to core melt
--	--	---------------	----	--------------------------------------

Level-V of defence in depth does not have any associated plant state. It is related to implementation of emergency plans due to accidents considered at earlier defence in depth levels i.e. Level-III and Level-IV.

Although boundaries between plant states are shown by frequency of occurrence in the above Table-3, these are specific numbers which should be considered as qualitative indicators rather than firm limits. In particular there may be events which are traditionally considered as DBAs [i.e Large Break Loss of Coolant Accidents (LOCAs)], even though such events may have lower frequencies than those indicated in Table-3 for DBAs. Frequency of occurrence in spite of its importance should not be used as the only basis for categorization of plant states.

3.3.6 ‘Frequency Informed and Defence in Depth Based’ Categorization Approach

The concept in this approach involves categorisation of events in plant states based on the combination of level in defence in depth and frequency of occurrence of event. It should be ensured that plant state resulting in high radiation doses or radioactive releases are of very low likelihood of occurrence and plant state with significant likelihood of occurrence have only minor or no radiological consequences.

3.3.7 The item important to safety that are necessary to fulfill the fundamental safety functions and for identifying the inherent safety features that are contributing to, or that are affecting, the fundamental safety functions for all plant states are systematically identified.

3.3.8 In line with above, SSCs designed to perform fundamental safety functions at each level of defence in depth should be identified. These identified SSCs should comply with the objectives of designated defence in depth levels as brought out in Table-4 below:

Table-4: Objectives of Defence in Depth levels

Defence in Depth Level	Objective of Defence in Depth Level	Essential SSCs
I	Prevention of abnormal operation and system/equipment failure	SSCs required for normal operation to keep NPP within Operational Limits and Conditions (OLCs)
II	Detection and Control of deviation from normal operational state	Control limiting and protection systems and other surveillance features to keep NPPs within Operational Limits and Conditions (OLCs)

Therefore certain DEC (multiple failures) may not have any impact on the radioactive release or dose to public like in Station Blackout although they are multiple failures with relatively higher frequency of occurrence.

III	Prevention of core damage	Inherent and/or design provisions, Safety Systems and Engineered Safety Features
IV	Prevention of escalation to core melt conditions	Additional Safety Features
	Mitigation of accident with core melt	Complementary Safety Features

- 3.3.9 For a given event, it should be assessed as to SSCs of which defence in depth level are invoked to mitigate the event, and then plant state corresponding to that defence in depth level should be assigned to that event. It may be possible that for a given event for fulfilling different fundamental safety functions, SSCs of different levels are invoked; and in that case the highest defence in depth level invoked for event mitigation should be the plant state.
- 3.3.10 While doing so, check should be made that all the earlier independent DiD measures have failed to fulfil their function.
- 3.3.11 In general, any single initiating event should be limited within first three categories of plant states (i.e. upto DBA) through design provisions. The Event Sequence or multiple failure of SSCs may fall into category 4A or 4B¹³ depending on failure of measures at preceding DiD Levels.
- 3.3.12 This is the ‘defence in depth based’ component of the approach which explicitly maps consequences of the event. Once a plant state is arrived at, it should be ensured that following the event, with credited SSCs, plant can be brought to reactor safe state as mandated for that plant state¹⁴.
- 3.3.13 Allocation of SSCs and safety features to defence in depth levels is design specific and this allocation should be justified and documented¹⁵.
- 3.3.14 Once plant state of the event is deterministically obtained, the estimated frequency of occurrence of the event should be checked against the illustrated frequency range of the corresponding plant state.
- 3.3.15 The assignment of frequency of occurrence should be based on appropriate methodology, including operating experience, if available. It should be ensured that event frequency, as used for plant state categorization, is the same, as used in Level-1 PSA.
- 3.3.16 If the estimated frequency of occurrence of the event matches or is less than the illustrated frequency of the corresponding plant state, the event categorization should be considered as final. In case estimated frequency of occurrence of the event is more than illustrated

¹³ Category 4A represents Design Extension Conditions without core melt for which Additional Safety Systems/Features are provided in Design while Category 4B refers to Design Extension Conditions with core melt for which Complementary Safety Features are provided in Design

¹⁴ Section 5.20 of Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

¹⁵ Safety Guide on Classification of SSCs and their Seismic categorization AERB/SG/D-1 (Draft)

frequency of the corresponding plant state, then possible design enhancements should be explored to bring frequency of the occurrence in the band associated with the assigned plant state. This is the 'frequency informed' component of the approach.

- 3.3.17 In exceptional cases where the frequency of occurrence falls in the lower category and further lowering of frequency (by design improvements) is not practical then in such cases DiD based categorization should still be assigned.
- 3.3.18 From the association of plant states with Defence in Depth levels, it is imperative that with successive failure in provisions for Defence in Depth levels, plant state severity increases. The frequency associated with Defence in Depth level (and hence plant states) signifies that on account of failure of designed SSCs at earlier Defence in Depth levels, the frequency of occurrence of events at more severe plant states is lower. Thus keeping the plant states in the illustrated frequency bands along with compliance to acceptance criteria of the respective plant states ensure that frequently occurring plant states have no or minor radiological consequences and plant states that could give rise to serious consequences have very low frequency of occurrence.

3.4. Events Due to Hazards

- 3.4.1 Loads and conditions generated by external and internal hazards are used for designing SSCs. These hazards also used for determining PIEs, and such PIEs should be categorized into plant states as per the methodology given in 3.3.6-3.3.17 above.
- 3.4.2 Hazards used for designing SSCs need not be categorized as plant states and should be dealt with separately.
- 3.4.3 Design basis hazards should be arrived at based on guidelines given in applicable AERB documents¹⁶; and under the conditions resulting from the hazard, fulfillment of the fundamental safety functions with designed systems should be demonstrated.
- 3.4.4 In addition to design basis external natural events, beyond design basis natural events (extreme events) should also be defined using a methodology agreeable to AERB. While design basis external events should govern the design of SSCs, functionality of the most safety relevant SSCs should be shown to be maintained under extreme events.

3.5. Plant States

The plant states considered in design for the deterministic safety analysis are:

¹⁶ AERB/SG/S-7 on Evaluation of Design Basis for External Human-induced Events for Nuclear Power Plants

3.5.1 Normal Operation (NO)

Normal operation which includes operational transients, defined as operation within specified operational limits and conditions of NPPs. Normal operation should typically include conditions such as:

- a. Normal reactor start-up from shutdown, approach to criticality, and approach to full power;
- b. Power operation, including full power and low power operation;
- c. Changes in reactor power, including load follow modes and return to full power after an extended period at low power, if applicable;
- d. Reactor shutdown from power operation;
- e. Hot shutdown Cooling down process and cold shutdown;
- f. Refueling during power operation, where applicable;
- g. Shutdown state: Reactor in refueling mode or maintenance conditions that open the reactor coolant or containment boundary;
- h. Normal operation modes of the spent fuel pool;
- i. Storage and handling of fresh fuel;
- j. Refueling during shutdown (For PHWRs, if carried out);
- k. Grid frequency variation within normal operating range

The behaviour of the plant and its systems should be analysed to establish the design data and verify the same during commissioning.

Deterministic analyses of normal operation should use an iterative process to support development of operational limits and conditions and confirm their adequacy. These reflect the limiting conditions of operation in terms of values of process variables and system requirements. The limits and conditions used in normal operation, such as reactor power and coolant inventory, should cover all important initial and boundary conditions that will be subsequently used in the analysis of AOO, DBA and DEC.

It should be taken into account that in some cases during normal operation, the main plant parameters are changing due to the transfer to different plant modes or the changes in the plant power output. A major aim of the analysis for normal operation transients should be to prove that the plant parameters can be kept within the specified operational limits and conditions.

3.5.2 Anticipated Operational Occurrences (AOO)

All operational processes deviating from normal operation which may occur during the operating life of the plant and which in view of appropriate design provisions, neither cause any significant damage to Items Important to Safety nor lead to Accident Conditions. AOOs

should include all the postulated initiating events which might be expected to occur during the lifetime of the plant. Expected frequency of occurrence of AOO is in the range $10^{-2} \leq$ per reactor-year.

The main objective of the AOO analysis is to check that the plant operational systems (in particular control and preventive protection systems) can prevent a wide range of AOOs from evolving into accident conditions and that the plant can return to NO following an AOO. It should be demonstrated that some or all of the barriers to the release of radioactive material from the plant will maintain their integrity to the extent required that the fundamental safety functions are always maintained.

3.5.3 **Design Basis Accidents (DBA)**

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

Expected frequency of occurrence of DBA is in the range $10^{-6} \leq f < 10^{-2}$ per reactor- year. The analysis of DBA should demonstrate that the safety systems are capable of achieving a safe shutdown state¹⁷ by ensuring that the fundamental safety functions are always maintained.

Safety analysis of DBA should establish the design capabilities, safety system set points, and emergency operating procedures. It should also be demonstrated that some or all of the barriers to the release of radioactive material from the plant will maintain their integrity to the extent required. The analysis provides the basis for the design of the safety systems and the engineered safety features.

3.5.4 **Design Extension Conditions (DEC)**

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

Design extension conditions, that are either more severe than design basis accidents or that involve additional failures, should be identified using engineering judgment as well as deterministic and probabilistic assessment with the objective of identifying design provisions to prevent as far as possible such conditions or mitigate their consequences¹⁸.

¹⁷ Please refer Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

¹⁸ Section 5.18 of Safety Code Design Of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC-D

DEC conditions include postulated event along with failure of safety system (or safety related system) provided in DiD level 3 resulting in propagation of accident to Level 4 of DiD.

The design basis may get exceeded due to postulated multiple failures¹⁹ resulting due to common cause failure for other reasons than a postulated hazard, affecting similar equipment in the same safety (or safety related) system. Two separate categories of design extension conditions should be considered: design extension conditions without core melt and design extension conditions with core melt, i.e. severe accidents.

3.5.4.1 Design Extension Conditions without core melt

The initial selection of design extension conditions sequences without core melt should be based on the consideration of multiple failures. These multiple failures are of very low frequency $\leq 10^{-4}$ per reactor-year.

Multiple failures considered are based on an initiating event simultaneous with non-availability or beyond the capability of a safety system (or safety related system). The failures of safety support system should implicitly be included among the causes of failure of safety systems. Specific attention should be paid to auxiliary and support systems (e.g. ventilation, cooling, electrical supply) as some of these systems may have the potential of causing immediate or delayed consequential multiple failures in both operational and safety systems.

DEC without core melt conditions includes postulated event along with failure of safety system (or safety related system) provided in DiD level 3 resulting in propagation of accident to Level 4 of DiD but has not escalated to core melt condition due to provisions of additional safety systems/features.

Different design extension conditions sequences without core melt, which present the greatest challenge to the relevant acceptance criterion should be analysed. The events, which are not considered for analysis should be justified and the consequences of such events should be enveloped by other bounding representative event. Multiple failures considered in each sequence of design extension conditions without core melt should be specifically listed.

3.5.4.2 Design Extension Conditions with core melt

Design Extension Condition with core melt includes postulated event along with failure of safety systems (or safety related system) provided in DiD level 3 resulting in propagation of accident to Level 4 of DiD that had escalated to core melt condition and mitigation of

¹⁹ Definition provided in Special Definition

consequences requires use of complementary safety features

A selection of specific sequences with core melting (severe accidents) should be made in order to establish the design basis for the safety features for mitigating the consequences of accident conditions with core melt, according to the plant safety objectives. These sequences should be selected in order to represent all main physical phenomena involved in core melt sequences. Typically, these conditions should have very low frequency of occurrence ($\leq 10^{-6}$ per reactor-year) which are not practically eliminated and need to be analysed towards design of complementary safety features and the development of severe accident management guidelines.

Some representative sequences should be selected by adding additional failures or incorrect operator responses to the design basis accident or design extension conditions sequences and to the dominant accident sequences identified in the probabilistic safety analysis. Representative sequences that could Challenge containment structural integrity should be used to provide input to the design of the containment and of those safety features necessary to mitigate the consequences of such design extension conditions. The low frequency of occurrence of a Design Extension Condition with core melt is not sufficient reason for failing to protect the containment against the conditions generated by such accident.

Core melt conditions should be postulated regardless of the provisions implemented in the design and the possibility of some very energetic phenomena that may result from the core melt accident should be prevented (i.e. the possibility of the conditions arising may be considered to have been 'practically eliminated') to exclude containment failure.

3.6. Selection of Events for Safety Analysis

3.6.1 A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each category of events (refer section 3.3.5). These bounding or enveloping scenarios should be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment. A bounding scenario may combine or amplify the consequences of several events in order to encompass all the possible events in the group. The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.

3.6.2 It should be taken into account that a single event should in some cases be analysed from different points of view with different acceptance criteria. A typical example is a loss of coolant accident, which should be analysed for many aspects: degradation of core cooling, containment pressure build-up, radioactivity transport and environmental releases, and specifically for pressurized water reactors as leakage of primary coolant to the steam generator by-passing the containment, pressurized thermal shock and boron dilution (reactivity accident) e.g. due to boiling condensing regime.

- 3.6.3 Handling accidents with both fresh and irradiated fuel should also be evaluated. Such accidents can occur both inside and outside the containment.
- 3.6.4 In addition, there are a number of other different types of postulated initiating events that would result in a release of radioactive material outside the containment and whose source term should be evaluated. Such accidents include:
- a. A reduction in or loss of cooling of the fuel in the spent fuel pool when the pool is located outside the containment;
 - b. Reactivity anomalies in the fresh or spent fuel;
 - c. An accidental discharge from any of the other auxiliary systems that carry solid, liquid or gaseous radioactive material;
 - d. A failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation;
 - e. An accident during reload or maintenance where the reactor or containment might be open.
- 3.6.5 All operating modes of normal operation covered by operational limits and conditions should be analysed, with particular attention paid to transient operational regimes such as changes in reactor power, reactor shutdown from power operation, reactor cooling down, handling of irradiated fuel and off-loading of irradiated fuel from the reactor to the spent fuel pool. Planned operator actions performed in accordance with normal operating procedures should be considered in the analysis.
- 3.6.6 The safety analysis for normal operation should also include analysis of the radiological situation in the plant and an estimate of the plant's releases of radioactive material to the environment. These are necessary inputs for determining radiation doses to the plant staff and to the public around the nuclear power plant.
- 3.6.7 The anticipated operational occurrences category should include all the postulated initiating events which might be expected to occur during the lifetime of the plant. In addition, the anticipated operational occurrences should not lead to any unnecessary challenges to safety equipment primarily designed for only protection in the event of design basis accidents. It is therefore advisable to demonstrate by the analysis that, in case of the operation of plant control and limitation systems²⁰ as intended, these systems will be capable of preventing the initiation of the safety systems.
- 3.6.8 The conservative analysis²¹ of anticipated operational occurrences and design basis accidents should demonstrate that the safety systems alone in the short term, and with operator actions in the long term, are capable of achieving a safe state by fulfilling the following safety requirements
- Shut down the reactor and achieve long term subcritical condition during and after

²⁰ Refers not only to the instrumentation systems for control and limitation of the plant variables but also to the systems for normal operation and those for anticipated operational occurrences actuated by them

²¹ Kindly Refer Detailed guidelines are given in Safety Guide on Safety Analysis for PHWRs No. AERB/NF/SG/D-19

anticipated operational occurrences or design basis accident conditions.

- Remove residual heat from the core after reactor shutdown from all anticipated operational occurrences or design basis accident conditions.
- Reduce the potential for the release of radioactive material and ensure that any releases are below acceptable limits during anticipated operational occurrences or design basis accident conditions.

3.6.9 Certain events (e.g. large break loss of coolant accidents, secondary system pipe breaks, control rod ejection in pressurized water reactors or rod drop in boiling water reactors) traditionally considered in deterministic safety analysis as design basis accidents should not be excluded from this category of accidents without careful analysis and quantitative assessment of its potential of contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release, while meeting design dose target specified in AERB/SC/S.

3.6.10 Simultaneous independent occurrence of loss of coolant accident (LOCA) and safe shutdown earthquake (SSE) is considered as of very low probability. A designer, by using conservative methods, should demonstrate that LOCA is not caused by SSE. However, simultaneous occurrence of Main Steam Line Break (MSLB)/Loss of Coolant Accident (LOCA), whichever is governing, and SSE should be considered to demonstrate that this does not lead to failure of containment (loss of structural integrity), which is the ultimate barrier. Supports/hangers, whose failure could be a threat to containment integrity, should be designed for simultaneous occurrence of LOCA and SSE.

3.6.11 The objective of the safety analysis of design extension conditions without core melt is to demonstrate that core melt can be prevented with an adequate level of confidence and that there is adequate margin to avoid cliff-edge effects ensuring compliance to design dose targets specified in AERB/SC/S.

3.6.12 The analysis of design extension conditions with core melt should identify the bounding plant parameters resulting from the postulated core melting sequences, and demonstrate that:

- a. the plant can be brought into a severe accident safe state where the containment functions can be maintained in the long term;
- b. the plant structures, systems, and components (e.g., the containment design) and procedures are capable of preventing a large radioactive release or an early radioactive release, including containment by-pass;
- c. control locations remain habitable to allow performance of required staff actions on the basis of on-site Radiological Impact Assessment (RIA);
- d. planned severe accident management measures are effective;
- e. adequate time is available to effect emergency countermeasures in public domain

adhering to the specified dose values mentioned in AERB/SG/EP-5, on the basis of off-site RIA.

Appendix-1 on Typical Events List for PHWRs, PWRs and BWRs

S.No.	Event	*Category (1-4B)	PHWR	PWR	BWR
1.0	Increase in heat removal from system				
1.1	Feed water temperature decrease (system malfunction)	2	+	+	+
1.2	False actuation of the secondary cooling system (If applicable)	2	NA	+	NA
1.3	Feed water flow increase (system malfunction)	2	+	+	+
1.4	Steam flow increase to Turbine (malfunction of the steam pressure controller)	2	+	+	+
1.5	Inadvertent opening of steam discharge /relief/dump valves followed by their failure to seat	2	+	+	+
1.6	False actuation of emergency condenser/passive heat removal from primary system (If applicable)	2	NA	+	+
1.7	Spectrum of steam line breaks inside and outside the containment	3	+	+	+ ^s
2.0	Decrease in primary Coolant inventory				
2.1	Compensable leak in the primary circuit	2	+	+	+
2.2	Malfunctions of the chemical and inventory control system resulting in decrease in primary inventory [Feed and Bleed (PHWR)/ Cleanup system (BWR)]	2	+	+	+
2.3	Rupture of tube(s) of heavy water heat exchangers other than steam generator (like gland cooler, shutdown cooler and bleed cooler)	2	+	NA	NA
2.4	Inadvertent opening of the pressurizer relief valve and its failure to seat	2	+	NA	NA
2.5	Compensable leak in main-steam line inside and outside the containment	2	NA	NA	+
2.6	Medium Size break in main-steam line inside and outside the containment	3	NA	NA	+
2.7	Large break in main-steam line inside and outside the containment	3	NA	NA	+
2.8	Reactor recirculation line large break inside containment	3	NA	NA	+
2.9	Unlatching of fuelling machine head from coolant channel without re-sealing leading to primary coolant leak	2	+	NA	NA
2.10	FM/C magazine pressure relief valve stuck open during on power refueling	2	+	NA	NA
2.11	Inadvertent opening of the primary pressure relief valve and its failure to seat	2	+	NA	NA
2.12	Inadvertent opening of the primary pressure relief valve and its failure to seat	3	NA	+	+
2.13	Single channel event like: i. PT failure leading to channel seal bellow or CT failure ii. Break of inlet feeder of different diameter iii. Stagnation feeder break	3	+	NA	NA
2.14	Failure of a coolant channel leading to ejection of fuel bundles from coolant channel and consequential LOCA	3	+	NA	NA
2.15	SB LOCA spectrum from primary pressure boundary pipe breaks	3	+	+	+
2.16	LB LOCA spectrum from primary pressure boundary pipe breaks including those resulting into very low flow conditions to core	3	+	+	+
2.17	Reactor Pressure Vessel -Bottom drain line break	3	NA	NA	+

<i>Note:- A check should also be made for impact on containment in terms of pressure and temperature rise in containment for item no 1.0 and 2.0</i>					
3.0	Increase in Primary Coolant System inventory				
3.1	False injection of water from the makeup-blow-down system into the pressurizer	2	NA	+	NA
3.2	Inadvertent operation of the safety systems leading to primary inventory increase (if applicable)	2	NA	+	+
3.3	System malfunction resulting in increase of the primary coolant inventory [chemical and inventory control system (PWR) /Feed and Bleed (PHWR)/ Clean up system (BWR)]	2	+	+	+
3.4	Inadvertent operation of the ECCS during cold shutdown condition	2	+	NA	NA
3.5	Inadvertent pressurization of primary coolant system by actuation of Control Rod Drive (CRD) pumps at cold conditions	2	NA	NA	+
4.0	Anomalies in reactivity and power distribution in the reactor core or in the Fresh fuel or spent fuel storage				
4.1	Uncontrolled withdrawal / Drift out of Reactivity control device (single or single bank) under subcritical/ low power/ start-up/ nominal power	2	+	+	+
4.2	Drop/Insertion / Drift in of one or group of reactivity devices [Control Rod (CR), Adjuster Rod (AR), or Shim Rod (SR)]	2	+	+	+
4.3	Static misalignment in AR or AR group	2	NA	+	NA
4.4	Control malfunction/(operator's error)in xenon oscillation suppression (If applicable)	2	+	+	+
4.5	Inadvertent actuation of neutron poison injection system during power operation	2	+	+	NA
4.6	Decrease of neutron poison concentration in the moderator	2	+	+	NA
4.7	Incorrect loading and operation of fuel assembly/bundle (one and more)	2	+	+	+
4.8	Inadvertent draining of Liquid Zone Control (LZC) compartment	2	+	NA	NA
4.9	Wrong start-up of an inactive reactor coolant loop	2	NA	+	NA
4.10	Spurious operation of chemical volume and control system	2	NA	+	NA
4.11	Inadvertent actuation of boron injection system during power operation	2	NA	+	NA
4.12	Abnormal startup of reactor circulation pumps	2	NA	NA	+
4.13	Uncontrolled withdrawal of CR group under low power/ start-up/ nominal power (if applicable)	3	+	+	NA
4.14	Spectrum of accidents with one CR/AR ejection/ at power /low-power /start-up	3	NA#	+	+
5.0	Decrease in heat removal from system (Reactor)				
5.1	Steam flow decrease (Malfunction of steam pressure controller)	2	+	+	+
5.2	Loss of external electric load	2	+	+	+
5.3	Turbine trip	2	+	+	+
5.4	Inadvertent closure of the main steam isolation valve	2	+	+	+

5.5	Loss of condenser vacuum	2	+	+	+
5.6	Loss of non-emergency A.C. power	2	+	+	+
5.7	Loss of normal feed water flow	2	+	+	+
5.8	Failure of main heat sink (without loss of main feed water supply)	2	NA	NA	+
5.9	Failure of main heat sink and loss of main feed water due to common cause	2	NA	NA	+
5.10	Small leak in feedwater line	2	NA	NA	+
5.11	Feed water pipeline break ^s	3	+	+	+
6.0	Decrease in Primary Coolant Flow rate.				
6.1	Loss of forced reactor coolant flow (one or more Reactor Coolant Pump trip)	2	+	+	+
6.2	Credible flow blockage in any reactor coolant channel assembly	2	+	NA	NA
6.3	Inadvertent closure of one steam generator isolation valve	2	+	NA	NA
6.4	Decrease in grid frequency (high rate or low rate of frequency drop)	2	+	+	+
6.5	shutdown cooling failure during normal operation	2	+	+	+
6.6	Reactor coolant pump rotor seizure	3	+	+	+
6.7	Reactor coolant pump shaft break	3	+	+	+
6.8	Shutdown cooling failure during header level control	3	+	NA	NA
7.0	Radioactive release from a sub-system or a component				
7.1	Leak or failure of the systems containing radioactive gas	2	NA	+	+
7.2	Leak or failure of the system containing radioactive liquid	2	+	+	+
7.3	Transients caused by large and small leaks in the Residual Heat Removal (RHR)-system outside the containment	2	NA	NA	+
7.4	Failure of systems storing radioactive resins/solid waste, failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation	2	+	+	+
7.5	Loss of Fuelling Machine (FM) cooling on reactor considering i. Failure of FM supply pumps ii. Failure of supply and return line hose	2 2	+	NA	NA
7.6	Fuel handling accidents during transfer to spent fuel storage bay	2	NA	+	+
7.7	Bundle crushed with FM latched to reactor with nominal Steam generator tube leak	2	+	NA	NA
7.8	Failure of the cooling of vessel containing irradiated fuel during fuel handling	3	NA	+	+
7.9	Fuel handling accidents during transfer of spent fuel from FM to Spent Fuel Storage Bay (SFSB): i. Fuelling machine not connected to channel with 8 spent fuel bundles inside the magazine and loss of magazine cooling supply ii. Loss of cooling while spent fuel bundles are in mobile transfer machine / transfer magazine	3	+	NA	NA

	iii. Spent fuel stuck during dry transfer exceeding normal dry transfer time				
7.10	Failures of cooling in Spent Fuel Storage Bay (SFSB)	2	+	+	+
7.11	Spent fuel cask drop accidents	3	+	+	+
8.0	Events to be analysed for Containment Analysis				
8.1	Disturbance of heat removal from the containment	2	+	+	+
8.2	Malfunction or inadvertent operation of the system resulting into containment pressure decrease / increase	3	+	+	+
9.0	Leaks into atmosphere or secondary coolant system				
9.1	Failure of SDCS in view of hot valve in feature of 700MWe with SG tube allowable leak with high Iodine-131 concentration	2	+	NA	NA
9.2	SG tube rupture (SGTR)	3	+	+	NA
9.3	Primary to secondary seal failure in SG (if applicable)	3	NA	+	NA
10.0	Fuel Pool related Accidents				
10.1	Compensable leak of spent fuel pool lining	2	+	+	+
10.2	Damage/loss of spent fuel pool cooling	2	+	+	+
10.3	Boric acid dilution in Fuel Pool (Spent and fresh)	2	NA	+	NA
11.0	Malfunction of support/auxiliary systems				
11.1	Instrument air failure	2	+	+	+
11.2	Single failure in any one of safety related electrical power supply system bus (e.g. class-III,II or I in PHWR)	2	+	+	+
11.3	Rupture at any location of any pipe in process water system/process water cooling system	2	+	+	+
11.4	Process water system circulation failure	2	+	+	+
11.5	Failure of computer based systems important to safety	2	+	+	+
11.6	Loss of moderator circulation or decrease or loss of moderator cooling	2	+	NA	NA
11.7	Moderator system pipe break or heat exchanger tube rupture	2	+	NA	NA
11.8	Failure of end shield cooling/loss of inventory	2	+	NA	NA
11.9	Failure of calandria vault cooling	2	+	NA	NA
11.10	SDCS heat exchanger tube failure	2	+	NA	NA
11.11	An event during reload or shutdown maintenance where the reactor or containment might be open	2	NA	+	+
11.12	Loss of on-site electrical power supply buses (class-III,II or I; one at a time)	3	+	+	+

12.0	Design Extension Condition without core melt (DEC)				
12.1	Failure to scram under AOO (ATWS)	4A	NA	+	+
12.2	Failure of end shield cooling/loss of inventory with SDCS failure	4A	+	NA	NA
12.3	Failure of tube(s) in PHT system heavy water heat exchangers other than steam generator coupled with any one of the following:- i. Failure of emergency core cooling system (in injection/recirculation mode) ii. Failure to close the isolation devices on the interconnection between PHT loops iii. Failure of steam generator auto-crash cooling actuation iv. Failure to close the isolation devices on the pipes carrying process water to and from the heat exchangers	4A	+	NA	NA
12.4	Single SG tube rupture with failure of Isolation of affected SG/Bank	4A	+	+	NA
12.5	Multiple Steam Generator Tube Rupture (SGTR)	4A	+	+	NA
12.6	Station Black Out (including effects on fuel pool cooling)	4A	+	+	+
12.7	Loss of residual heat removal to ultimate heat sink (shutdown & refueling) e.g. total loss of the component cooling water system or of the essential service water system, loss of normal cooling path to the ultimate heat sink	4A	+	+	+
12.8	Steam line break of largest size inside or outside containment with single ^{SS} SG tube rupture.	4A	+	+	NA
12.9	MSLB+ containment spray system failure	4A	+	+	+
12.10	LOCA+ containment spray system failure	4A	+	+	+
12.11	LOCA+ fast cool down /crash cool down logic failure	4A	+	NA	NA
12.12	Total loss of feed water: loss of main feed water combined with total loss of emergency/auxiliary feed water	4A	+	+	+
12.13	Inadvertent closing of steam isolation valve with stuck open relief valves	4A	+	+	+
12.14	Loss of the component cooling water system or the essential service water system (ESWS)	4A	+	+	NA
12.15	LOCA plus loss of one or more emergency core cooling system (either the high pressure or the low pressure emergency cooling system ^{\$\$\$})	4A	+	+	+
12.16	Fuel handling failure in transit coupled with containment impairment characterised by i. Failure of one set of containment isolation dampers or ii. Failure of containment isolation logic or iii. One door of main airlock stuck open and seals on second door deflated	4A	+	NA	NA
12.17	MSLB+CCD failure	4A	+	NA	NA
13.0	Design Extension Condition with core melt (Severe Accidents)				
13.1	Multiple failure accident sequence leading to core melt, such as	4B	(see 13.2 and	+	+

	<ul style="list-style-type: none"> i. LOCA + failure of safety systems/ engineered safety features in Level III of DiD and applicable additional safety systems/ engineered safety features in level IV of DiD (Also refer 2.1.2) ii. SBO with failure of additional safety systems in level IV of DiD iii. Any other event specific to reactor with failure of safety systems in level III and additional safety systems in level IV of DiD <p>Note: A check should be made for impact of hydrogen generation into containment from above core melt accident conditions as a bases of design of hydrogen management provisions</p>		13.3 below)		
13.2	LOCA+LOECCS ^{\$\$\$} +Failure of moderator heat sink	4B	+	NA	NA
13.3	Unmitigated SBO (SBO + Loss of fire water system+ Failure of SG heat sink* + Failure of Moderator Sink) *Including PDHRS (if applicable)	4B	+	NA	NA
13.4	Loss of the component cooling water system or the essential service water system (ESWS)	4B	NA	NA	+

+ *Applicable to the type of Reactor*

NA: *Not Applicable to that type of reactor*

Rod Ejection is not envisaged in PHWR Type NPP due to low pressure moderator system

\$ *It is LOCA for BWR(Also refer 2.5, 2.6 & 2.7). Leaks in the feed water and main-steam lines comprise leaks in these lines themselves and in those pipe sections that connect to the reactor cooling system and cannot be isolated. With these types of leaks the leaking coolant flows over into the pressure-suppression pool and thus becomes available for residual-heat removal. For BWR it leads to loss of primary inventory which becomes bounding and is covered separately in the list.*

\$\$\$ *In PHWRs complete loss of ECCS should be considered, as failure of MVs can lead to failure of entire ECCS. LOCA includes CT-PT failure.*

\$\$ *subject to qualification of SG tubes to withstand largest steam line break.*

Appendix-2 Typical List of Internal and External Hazards for NPPs

S.No.	Event	PHWR	PWR	BWR
i.	Design Basis Fire (such as in reactor building, main control room)	+	+	+
ii.	Operating Basis Earthquake (OBE)	+	+	+
iii.	Safe Shutdown Earthquake (SSE)	+	+	+
iv.	Turbine failure leading to missile being thrown off	+	+	+
v.	Internal Missiles	+	+	+
vi.	Design Basis Flood	+	+	+
viii.	Design Basis Cyclones	+	+	+
ix.	Dam failure leading to loss of ultimate heat sink	+	+	+
x.	Aircraft Impact	+	+	+
xi.	Beyond Design Basis Flood	+	+	+
xii.	Beyond Design Basis Earthquake	+	+	+
xiii.	Beyond Design Basis Cyclone	+	+	+

BIBLIOGRAPHY

- i. ATOMIC ENERGY REGULATORY BOARD SAFETY CODE on Site Evaluation AERB/SC/S Rev.1
- ii. ATOMIC ENERGY REGULATORY BOARD SAFETY CODE on Design of Light Water Reactor Based Nuclear Power Plants AERB/NPP-LWR/SC/D
- iii. ATOMIC ENERGY REGULATORY BOARD SAFETY CODE Design of Pressurized Heavy Water Reactor Based Nuclear Power Plants AERB/NPP-PHWR/SC/D (in draft stage)
- iv. ATOMIC ENERGY REGULATORY BOARD SAFETY GUIDE on Safety Analysis for PHWRs No. AERB/NF/SG/D-19
- v. ATOMIC ENERGY REGULATORY BOARD SAFETY GUIDELINES on Criteria for Emergency Preparedness and Response AERB/SG/EP-5
- vi. ATOMIC ENERGY REGULATORY BOARD SAFETY GUIDE on Classification of SSCs and their Seismic Categorization AERB/SG/D-1 Rev.1 (in draft stage)
- vii. ATOMIC ENERGY REGULATORY BOARD SAFETY GUIDE on Evaluation of Design Basis for External Human-induced Events for Nuclear Power Plants AERB/SG/S-7
- viii. Report of AERB committee for Fukushima review (Ref. AERB/SSED/2014/53 dated March 28, 2014)
- ix. INTERNATIONAL ATOMIC ENERGY AGENCY SPECIFIC SAFETY REQUIREMENTS on Design of the Nuclear Power Plants IAEA SSR 2.1 Rev.1
- x. INTERNATIONAL ATOMIC ENERGY AGENCY SPECIFIC SAFETY GUIDE on Deterministic Safety Analysis for Nuclear Power Plants,SSG-2 Rev. 1,DS491 (Draft, 22 July 2016)
- xi. INTERNATIONAL ATOMIC ENERGY AGENCY TECDOC 1791 on Considerations On The Application Of The IAEA Safety Requirements For The Design Of Nuclear Power Plants
- xii. INTERNATIONAL ATOMIC ENERGY AGENCY TECDOC 1787 on Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants
- xiii. CANADIAN NUCLEAR SAFETY COMMISSION REGDOC-2.5.2 on Physical Design of Reactor Facilities: Nuclear Power Plants
- xiv. CANADIAN NUCLEAR SAFETY COMMISSION REGDOC-2.4.1 on

Deterministic Safety Analysis

- xv. AERB report of the working group constituted to identify the need for revision and requirements of revision, based on Fukushima experience.
- xvi. FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY, Safety Design Of A Nuclear Power Plant, GUIDE YVL B.1 / 15 November 2013
- xvii. FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY, Probabilistic Risk Assessment And Risk Management Of A Nuclear Power Plant, GUIDE YVL A.7 / 15 November 2013
- xviii. FINNISH CENTRE FOR RADIATION AND NUCLEAR SAFETY, Deterministic Safety Analyses For A Nuclear Power Plant, GUIDE YVL B.3 / 15 November 2013
- xix. WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION RHWG Report on Safety of new NPP designs, 2013

LIST OF PARTICIPANTS OF IHWG
AERB In-house Working Group for Preparation of R-0 Draft

Dates of meeting

January - April 2017

Members In-House Group:

Shri Utkarsh. S.C, NPSD	Convener
Shri D. Bhattacharya, OPSD	Member
Dr. S P Lakshmanan, NSAD	Member
Shri Amar Kulkarni, NPSD	Member-Secretary
Shri Harpal Singh, NPSD	Co-opted Member
Shri. Arbind Krishnan,NPSD	Co-opted Member

**LIST OF PARTICIPANTS OF TF
AERB TF/SG/D-5 for Preparation of R-1 Draft**

Dates of meeting

28/07/2017	27/09/2017	07/01/2018	20/03/2018
09/08/2017	06/10/2017	08/01/2018	22/03/2018
14/08/2017	27/10/2017	12/03/2018	23/03/2018
14/09/2017	01/11/2017	14/03/2018	11/04/2018
22/09/2017	02/11/2017	17/03/2018	16/04/2018

Members Task Force for Review and Revision of R0:

Shri Malhotra P.K, Rtd. NPCIL	Convener
Shri D. Mukhopadhyay, BARC	Co- Convener
Shri Hajela Sameer, NPCIL	Member
Shri Utkarsh S.C, AERB	Member
Smt Gopika V., BARC	Member
Shri Dubey S.K, AERB	Member
Shri R. B. Solanki. R, AERB	Member
Shri Krishna Kumar P, NPCIL	Member
Shri Pahari Santanu, NPCIL	Member
Shri Bansal.P, AERB	Member Secretary
Shri Prasad Mahendra	Co-opted Member
Smt Vijaya A.K., NPCIL	Co-opted Member
Shri Shaikh Sameer, AERB	Permanent Invitee

**ADVISORY COMMITTEE FOR NUCLEAR AND RADIOLOGICAL SAFETY
(ACNRS)**

Dates of meeting

24/08/2018 06/07/2019

Members of ACNRS

Shri S. S. Bajaj, Former Chairman, AERB	Chairman
Shri D. K. Shukla, Chairman, SARCOP, AERB	Member
Dr. N. Ramamoorthy, Chairman, SARCAR, AERB	Member
Dr. M. R. Iyer, Former Head, RSSD, BARC	Member
Shri U. C. Muktibodh, Director (T), NPCIL	Member
Shri V. Rajan Babu, Director (T), BHAVINI	Member
Prof. C.V. R. Murthy, Director, IIT, Jodhpur	Member
Shri H. S. Kushwaha, Former Director, HS&E Group, BARC	Member
Shri K. K. Vaze, Former Director, RD&D Group, BARC	Member
Shri S. K. Ghosh, Former Director, CE Group, BARC	Member
Dr. S. C. Chetal, Former Director, IGCAR	Member
Shri A. R. Sundararajan, Former Director, RSD, AERB	Member
Dr. A. N. Nandakumar, Former Head, RSD, AERB	Member
Shri S. C. Chetal, Former Director, RSD, AERB	Member
Shri S. T. Swamy, Head, RDS, R&DD, AERB	Member-Secretary

AERB SAFETY GUIDE NO. AERB/NPP-WCR/SG/D-5 (Rev.1)

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