AERB SAFETY GUIDE NO.AERB/SG/D-5

DESIGN BASIS EVENTS FOR PRESSURISED HEAVY WATER REACTOR

Issued in March, 2000

This document is subject to review, after a period of one year from the date of issue, based on the feedback received

Atomic Energy Regulatory Board
Mumbai 400 094

Price:

Orders for this Guide should be addressed to:

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

FOREWORD

Safety of the public, occupational workers and protection of the environment should be assured while activities for economic and social progress are pursued. These activities include the establishment and utilisation of nuclear facilities and use of radioactive sources. They have to be carried out in accordance with relevant provisions of the Atomic Energy Act 1962.

Assuring high safety standards has been of prime importance since the inception of the nuclear power programme in the country. Recognising this aspect, the Government of India constituted the Atomic Energy Regulatory Board (AERB) in November 1983, vide Statutory Order No. 4772 notified in the Gazette of India dated 31.12.1983. The Board has been entrusted with the responsibility of laying down safety standards and framing rules and regulations in respect of regulatory and safety functions envisaged under the Atomic Energy Act of 1962. Under its programme of developing safety codes and guides, AERB has issued four codes of practice in the area of nuclear safety covering the following topics:

Safety in Nuclear Power Plant Siting

Safety in Nuclear Power Plant Design

Safety in Nuclear Power Plant Operation

Quality Assurance for Safety in Nuclear Power Plants

Safety guides are issued to describe and make available methods of implementing specific parts of the relevant codes of practice as acceptable to AERB. Methods and solutions other than those set out in the guides may be acceptable if they provide at least comparable assurance that Nuclear Power Plants (NPPs) can be operated without undue risk to the health and safety of plant personnel, the general public and the environment.

Codes and safety guides may be revised as and when necessary in the light of experience as well as relevant developments in the field. The annexures, foot-notes, references and bibliography are not to be considered integral parts of the document. These are included to provide information that might be helpful to the user.

The emphasis in the codes and guides is on protection of site personnel and the public from undue radiological hazards. However, for other aspects not covered in the codes and guides, applicable and acceptable national and international codes and standards shall be followed. In particular, industrial safety shall be assured through good engineering practices and through compliance with the Factories Act 1948 as amended in 1987 and the Atomic Energy (Factories) Rules, 1996.

This Safety Guide is one of a series of guides which have been prepared or are under preparation as a follow-up to the Code of Practice on Design for Safety in Pressurised Heavy Water Based Nuclear Power Plants (AERB/SC/D). The Guide is based on the current designs of the 220 MWe and 550 MWe Pressurised Heavy Water Reactors. It lists various Postulated Initiating Events and operational transients during normal operation and analyses the behaviour of the NPP during these events with the aim of verifying that acceptable design limits are not exceeded.

This Safety Guide has been prepared by the staff of AERB, BARC, IGCAR and NPC. It has been reviewed by experts and vetted by the AERB Advisory Committees before issue. AERB wishes to thank all individuals and organisations who have prepared and reviewed the draft and helped in the finalisation of the Safety Guide. The list of persons who have participated in the committee meetings, along with their affiliation, is included for information.

Suhas P. Sukhatme

(Suhas P. Sukhatme)
Chairman,
AERB

DEFINITIONS

Acceptable Limits

Limits acceptable to the Regulatory Body.

Anticipated Operational Occurrences[1]

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.

Beyond Design Basis Events(BDBE)

Events of very low probability occurrence, which can lead to severe accident and not considered as Design Basis Events.

Design

The process and the result of developing the concept, detailed plans, supporting calculations, drawings and specifications for a facility.

Design Basis Events(DBE)

The set of events that serve as part of the basis for the establishment of design requirements for systems, structures 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.

Design Limits

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

---

1 Examples of anticipated operational occurrences are loss of normal electric power and faults such as turbine trip, malfunction of individual items of normally running plant, failure of individual items of control equipment to function, loss of power to main coolant pump, etc.

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.

Normal Operation

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

Operating Basis Earthquake (OBE)

The "Operating Basis Earthquake" (OBE) is that earthquake which, considering the regional and local geology and seismology and specific characteristics of local sub-surface material, could be reasonably expected to affect the plant site during the operating life of the plant; it is that earthquake which produces the vibratory ground motion for which the features of Nuclear Power Plant (NPP) necessary for continued safe operation are designed to remain functional.

Postulated Initiating Events(PIE)[2]

Identified Events that lead to Anticipated Operational Occurrences or Accident Conditions and their consequential failure effects.

Prescribed Limits

Limits established or accepted by the Regulatory Body for specific activities or circumstances that must not be exceeded.

Reliability

It is the probability that a structure, component, system or facility will perform its intended (specified) function satisfactorily for a specified time period under specified operating and environmental conditions.

---

2 The primary causes of PIE may be credible equipment failures and operator errors both within and external to the (NPP) man-induced or natural events. The specification of the postulated initiating events has to be acceptable to the Regulatory Body.

Risk

A multiattribute quantity expressing hazard, danger or chances of harmful or injurious consequences associated with an actual or potential event under consideration. It relates to quantities such as the probability that a specific event may occur and the magnitude and character of the consequences.

Safe Shutdown Earthquake (SSE)

The "Safe Shutdown Earthquake" is that earthquake which is based on an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local sub-surface material. It is that earthquake which produces maximum vibratory ground motion for which certain structures, systems and components are designed to remain functional. These structures, systems, and components are those which are necessary to assure;

(a) The integrity of the coolant pressure boundary, or

(b) The capability to shutdown the reactor and maintain it in a safe shutdown state, or

(c) The capability to prevent the accident or to mitigate the consequences of accidents which could result in potential off-site nuclear exposures higher than the permissible limits specified by the Regulatory Body, or

(d) The capacity to remove residual heat.

Safety

Protection of all persons from undue radiological hazard.

Safety Functions

A specific purpose, that must be accomplished for safety. The list of safety functions is given in AERB Safety Guide on Safety Classification and Seismic Categorisation (AERB/SG/D-1).

Safety Limits

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

Severe Accidents

Nuclear Power Plant 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 functions. Consequential failures resulting from a single random occurrence are considered to be part of the Single Failure.

CONTENTS

1. INTRODUCTION

1.1 General

1.1.1 Nuclear Power Plants(NPP) are designed, constructed, commissioned and operated in conformity with the applicable nuclear safety standards. The standards ensure an adequate margin of safety so that NPP may be operated without undue radiological risk to the plant personnel or members of the public. Design Basis Events(DBE), which form the basis of design of NPP, include normal operation, operational transients and Postulated Initiating Events (PIE). Assessment of the safety of an NPP requires that behaviour of the plant following a PIE be analysed. Also, the plant, its systems and its equipment should be designed to ensure that under normal operation, operational transients and accident conditions, design limits are not exceeded.

1.1.2 There are no firm criteria for identification and categorisation of DBE; rather the process is a combination of iteration between design and analysis, engineering judgement and experience of previous NPP design and operation.

1.2 Objectives

1.2.1 The behaviour of an NPP following a PIE is analysed to assess the safety of the NPP. This document prescribes various PIEs. Such an analysis aims at verifying that the various design limits are not exceeded and that risk to public health caused by radioactive release is properly assessed. This Safety Guide also includes a list of operational transients during normal operation, which are considered for design of components and systems.

1.3 Scope

1.3.1 This guide provides a list of PIEs and operational transients to be considered for safety analysis and design of the plant.

1.3.1.1 DBE and their consequences depend on the design details of NPP. This Safety Guide is based on the current designs of 220 MWe and 500 MWe Pressurised Heavy Water Reactors (PHWR). If there are any changes in design details of NPP in future or if the operating experience so demands, it may be necessary to revise the list of DBEs.

1.3.1.2 The Annexure gives a list of events for which detailed safety analysis need not be carried out because of the specific design features of NPP. Qualitative reasons for not considering such analysis are also included in the Annexure.

Detailed safety analysis may not also be required for some of the PIEs. 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: probabilistic consideration; degree of defence-in-depth; site specific reasons; specific features of design/operation of NPP; or practice followed in other countries.

1.3.1.3 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 LOCA and SSE should be considered to demonstrate that this does not lead to failure of containment, 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.

1.3.1.4 Initiating events resulting from sabotage are not considered.

1.3.1.5 Missiles resulting from aircraft are not considered as initiating events as siting considerations exclude selection of such a site. [Ref. AERB Safety Code AERB/SC/S, Rev. 0, 1990: Code of Practice on Safety in Nuclear Power Plant Siting].

1.3.2 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. However, while assessing the consequences of a PIE, due weightage should be given to required operator actions with an appropriate time delay.

1.3.3 Consequences of events beyond design basis should be analysed as an aid to emergency planning. Scope of this exercise may be limited to realistically establishing radiological consequences.

2. CLASSIFICATION OF DESIGN BASIS EVENTS(DBE)

2.1 General

2.1.1 Design Basis Events (DBE), which form the basis of design of NPP, include normal operations, operational transients and Postulated Initiating Events (PIE).

2.1.2 DBE can be classified on the basis of their consequence and expected frequency of occurrence. Consequences of a rare event can be permitted to be severe while those of a frequent event can be accepted only at very low severity. Acceptance criteria for consequences of a DBE, thus, also depend on frequency of their occurrence. PIE can also be classified into symptomatic groups depending upon the similarity of their consequences. Only limiting cases in each group need to be analysed in detail whereas other cases can be dealt with qualitatively. A sufficiently broad spectrum of DBE which ensures that all relevant types of events are considered should form the basis of design analysis. Events of very low probability of occurrence which are considered only for off-site emergency plan or site selection issues, are called as Beyond Design Basis Events (BDBE).

2.1.3 The designer may propose changes in classification of events with justified changes in design/operational features. However, if consequences of a PIE are calculated to be severe, the design should be examined to reduce likelihood of its occurrence.

2.2 Functional Classification of PIE

2.2.1 The first step in analysis is to postulate a number of events affecting process parameters following failure/malfunction of equipment. Each PIE should then be assigned to one of the following groups:-

(i) Reactivity and power distribution anomalies.

(ii) Decrease in primary heat transport (PHT) system inventory.

(iii) Increase in PHT system inventory.

(iv) Increase in heat removal by secondary system.

(v) Decrease in heat removal by secondary system.

(vi) Decrease in PHT system flow rate.

(vii) Radioactive release from a sub-system or a component

(viii) Malfunction of support/auxiliary systems.

(ix) Others.

2.3 Classification of DBE Based on Frequency of Occurrence

2.3.1 DBE are categorised on the basis of their expected frequency of occurrence. Any change in category proposed by the designer should be justified by appropriate analysis. Each of the DBE considered should be assigned to one of the following frequency groups.

(i) Category-1 events : normal operation and operational transients.

(ii) Category-2 events : events of moderate frequency.

(iii) Category-3 events : events of low frequency.

(iv) Category-4 events : multiple failures and rare events.

Events not falling in any of the above categories are called BDBE.

Acceptable radiological dose limit for plant personnel and public for the events under each category is specified in the AERB Safety Guide on Radiation Protection in Design of PHWR (AERB/SG/D-12). Limits on fuel clad and coolant are given in the Design Safety Guide on Fuel Design (AERB/SG/D-6).

For each of the category/events, appropriate evaluation criteria in the following areas, as applicable, should be specified: functional requirements; reactivity/power; fuel design; pressure and temperature; structural design and radiation effects.

2.3.2 Category-1 Events: Normal Operation and Operational Transients

2.3.2.1 Operational process transients such as start-up/shutdown/power changes, expected to occur frequently as part of normal operation and maintenance, are included under this category. Such transients may determine the life of systems/equipment/instrumentation. The frequency

---

3 The frequencies of occurrence given in this guide are only for illustrative purposes.

of events under this category is expected to be greater than or equal to 1 per reactor-year[3]. Table-1 gives a list of transients expected. This list serves as a typical example and may be supplemented with additional transients. The behaviour of the plant and its systems/equipment/ instrumentation should be analysed to prove that design limits are not exceeded. Adequate margins should be provided to meet requirements of applicable design codes.

2.3.2.2 The number of DBE during the lifetime of the reactor should be conservatively estimated for use in design of the NPP. The frequency of events may be estimated based on the operating experiences of NPP.

2.3.3 Category-2 Events: Events of Moderate Frequency

2.3.3.1 Events of moderate frequency (~ 1 to 10^{-2} per reactor-year[3]) are included in this category. Table-2 gives events of moderate frequency as well as their functional classification.

2.3.4 Category-3 Events : Events of Low Frequency

2.3.4.1 Events of low frequency which are rare events and likely to occur ~10^{-2} to 10^{-4} per reactor-year[3] are included in this category. Table-3 lists events of low frequency along with their functional classification.

2.3.5 Category-4 Events: Multiple Failures and Rare Events

2.3.5.1 Rare events in this category generally cover multiple failures considered important for design and which are likely to occur ~10^{-4} to 10^{-6} per reactor-year[3]. Table-4 gives a list of multiple failures and rare events considered important for design. For the combination, it is assumed that two independent initiating events, which do not result from a single cause cannot occur simultaneously. Multiple failures considered are based on an initiating event simultaneous with non-availability of a safety system.

2.3.6 Beyond Design Basis Events (BDBE)

2.3.6.1 Events of very low probability of occurrence (less than 10^{-6} per reactor-year[3]), which are considered only for off-site emergency plan or site selection issues, are called as Beyond Design Basis Events. Table-5 lists some of the BDBE.

3. EVENT EVALUATION

3.1 General

3.1.1 All DBE should be analysed in depth for their effect on safety.

3.2 Sequence of Events

3.2.1 A sequence of events starting from the initiating event to the final stabilized safe condition should be given on a time scale (like reactor trip, PHT system pressure reaching safety relief valve set point, safety relief valve operation, emergency core cooling system (ECCS) actuation, containment isolation signal initiation, containment isolation etc.) All required operator actions should be identified. Operator action should be qualified with availability of unambiguous signal and time available for operator action. [Ref. section 0341 of AERB Code of Practice on Design for Safety in PHWR Based NPP (AERB/SC/D, 1989) for guidance on credit for operator actions).

3.3 Consequences of Events

3.3.1 Consequences of each event should be analysed assuming a single failure in applicable mitigating system(s). However, in the case of any mitigating feature, provided for coping with multiple failures, the requirement of meeting single failure criterion should be considered case by case based on the impact on overall risk. This is on the basis that since the multiple failure itself has very low likelihood of occurrence, postulation of additional failure (as implied by application of single failure criterion) may not be warranted.

3.4 Evaluation of Results

3.4.1 Results considered important for safety assessment should be brought out. This may include safe shutdown of the reactor, core cooling, fuel integrity, integrity of PHT system boundary, integrity of secondary system, radiation shielding, monitoring status of nuclear steam supply system, decay heat removal, performance of containment and other barriers. Radioactive release should also be evaluated. Criteria for acceptable value for each of the parameter considered important shall be defined by the designer based on applicable codes, standards and practices. Methodologies/computer codes used for each evaluation should be suitably validated.

3.5 Evaluation of BDBE

3.5.1 Consequences of events beyond design basis should be analysed[4] as an aid to emergency planning. Scope of this exercise may be to establish radiological consequences on best estimation basis.

4 Agreed methodology for these analysis should be arrived at by the Utility and the Regulatory Body.

TABLE-1: CATEGORY-1 EVENTS

NORMAL OPERATION AND OPERATIONAL TRANSIENTS

EVENT NO.	EVENTS
C1-1	Reactor start-up from cold to 100% full power (FP).
C1-2	Reactor power operation.
C1-3	Reactor shutdown from 100% FP to cold and maintaining at shutdown state.
C1-4	Reactor trip and its re-startup before poison out.
C1-5	Reactor start-up just after poison out.
C1-6	Reactor trip and cool-down.
C1-7	Reactor shutdown and maintaining at shutdown state.
C1-8	Operational hydro-test. (viz., after repairs affecting the system pressure boundary)
C1-9	Reactor operation with specific items of equipment out of service or under test as may be permitted by the technical specifications for the plant. (viz., operation with unavailability of two main primary coolant pumps under 1-1 mode).
C1-10	Reactor operation with failed fuel within the technical specifications.
C1-11	Plant disturbances due to electric power supply fluctuation (changes in frequency and voltage)
C1-12	Power changes between 0% and 100%FP (including sudden changes).
C1-13	Island mode of reactor operation.

Note:- Ck-m type numbering convention has been followed for numbering of events. First number "Ck" refers to category, second number "m" refers to the serial number of the event. This note applies to Table-1 only.

TABLE-2: CATEGORY-2 EVENTS

EVENTS OF MODERATE FREQUENCY

EVENT NO.	EVENTS
C2-1.0	**Reactivity and Power Distribution Anomalies**
C2-1.1	Positive reactivity insertion at a range of rates up to and including the maximum credible rate while the reactor is **subcritical** (assuming the most unfavourable reactivity conditions of the core and PHT system).
C2-1.2	Positive reactivity insertion at a range of rates up to and including the maximum credible rate from **all power levels** including start up condition (assuming the most unfavourable reactivity condition of the core and PHT system). Apart from global effects local distortion in flux/power should also be addressed for large reactors (500 MWe). Positive reactivity insertion could result from one of the following:- (a) Uncontrolled withdrawal of adjusters (control rods/ regulating rods/shim rods) including inadvertent draining of zone control compartments (500 MWe reactors). The failure/malfunction of reactivity devices could be a single failure of a device and/or failure of one regulating channel or one control computer. (b) Uncontrolled withdrawal of one bank of shut-off rods in primary shutdown system or draining of one bank of liquid poison tubes in secondary shutdown system. (c) Malfunction resulting in decrease in boron (or any other neutron poison) concentration in moderator.

TABLE-2: Contd.

EVENT NO.	EVENTS
C2-2.0	**Decrease in PHT System Inventory**
C2-2.1	Rupture at any location of any small pipe (e.g. instrument line) connected to PHT system.
C2-2.2	Rupture of tube(s) of heavy water heat exchangers other than steam generator (like gland cooler, shutdown cooler and bleed cooler).
C2-2.3	Failure of PHT pressure control system with PHT system (cold/hot) [for example, feed valves are stuck closed and bleed valves are stuck open simultaneously as a result of spurious signals from pressure controller].
C2-2.4	Rupture at any location of PHT system up to size of double ended largest feeder pipe.
C2-2.5	Unlatching of fuelling machine head from coolant channel without re-sealing.
C2-2.6	Failure at any location of any coolant channel assembly (including failure at any location of coolant channel followed by failure of its calandria tube).
C2-2.7	Failure resulting in opening of instrumented relief valves of the PHT system and failure of the relief valve on the bleed condenser to re-close.
C2-2.8	Failure of mechanical seals of a single PHT pump.
C2-2.9	Rupture of a single steam generator tube.
C2-3.0	**Increase in PHT System Inventory**
C2-3.1	Failure of PHT pressure control system with PHT system (cold/hot). Consider, also all such incidents when fuelling machine is coupled to PHT system (cold/hot) (For example: feed valves stuck open, bleed valves stuck closed, bleed isolation valves closed by mistake of the operator during maintenance).
C2-3.2	Inadvertent operation of ECCS during cold shutdown condition leading to pressure tube brittle failure.

TABLE-2: Contd.

EVENT NO.	EVENTS
C2-4.0	**Increase in Heat Removal by Secondary System**
C2-4.1	Feed water system malfunctions that result in decrease in feed water temperature.
C2-4.2	Feed water system malfunctions that result in increase in feed water flow.
C2-4.3	Failures that result in increase in steam flow. (For example: boiler pressure controller malfunction, inadvertent opening of main steam line relief or safety valve, steam discharge/dump valve).
C2-5.0	**Decrease in Heat Removal by Secondary System**
C2-5.1	Loss of external electrical load.
C2-5.2	Turbine trips.
C2-5.3	Loss of condenser vacuum.
C2-5.4	Loss of normal feed water flow (multiple trains).
C2-6.0	**Decrease in PHT System Flow Rate**
C2-6.1	Single and multiple primary coolant pumps trip.
C2-6.2	Credible flow blockage in any reactor coolant channel assembly.
C2-6.3	Shutdown cooling system pump failure.
C2-7.0	**Radioactive Release from a Sub-system or a Component**
C2-7.1	Leak or failure in systems having radioactive liquids.
C2-7.2	Fuel handling accidents during transfer to spent fuel storage bay.
C2-7.3	Failure of the cooling of a fuelling machine when off reactor, containing full complement of irradiated fuel.

TABLE-2: Contd.

EVENT NO.	EVENTS
C2-8.0	**Malfunction of Support/Auxiliary Systems**
C2-8.1	Process water system circulation failure.
C2-8.2	Class-IV electrical power supply failure.
C2-8.3	Moderator system cooling failure
C2-8.4	Moderator system small size pipe break or heat exchanger tube rupture.
C2-8.5	Failure of end shield cooling.
C2-8.6	Failure of calandria vault cooling.
C2-8.7	Instrument air failure.
C2-8.8	Process water system piping failure (small size).
C2-8.9	Single failure in any one of the safety related electrical power supply systems (Class-III,II or I).
C2-9.0	**Others**
C2-9.1	Failure of computer based systems important to safety [e.g. failure of programmable digital comparator system (PDCS)]
C2-9.2	Design Basis Fire (such as in reactor building, main control room): [Ref. AERB/SG/D-4: Fire Protection]
C2-9.3	Operating Basis Earthquake (OBE**):** [Ref. AERB/SC/S, 1990: Code of Practice on Safety in Nuclear Power Plant Siting]
C2-9.4	Accidental dropping of spent fuel cask into the spent fuel storage bay.

[It may be possible to have design feature to exclude this event]

Note:- Ck-m.n type numbering convention has been followed for numbering of events. First number "Ck" refers to category, second number "m" refers to functional classification and the third number "n" is the serial number for a particular functional group. Serial numbers are given sequentially in all categories of events. This note is applicable to Tables-2,3 and 4.

TABLE-3: CATEGORY-3 EVENTS

EVENTS OF LOW FREQUENCY

EVENT NO.	EVENTS
C3-2.0	**Decrease in PHT System Inventory**
C3-2.9	Rupture at any location of PHT system piping of a size bigger than double-ended largest feeder pipe and including up to double-ended guillotine break of biggest piping in the system.
C3-2.10	Failure of a coolant channel leading to ejection of fuel bundles from coolant channel and consequential LOCA.
C3-4.0	**Increase in Heat Removal by Secondary System**
C3-4.4	Steam system pipe or header break inside and outside containment.
C3-5.0	**Decrease in Heat Removal by Secondary System**
C3-5.5	Feed water pipe break.
C3-6.0	**Decrease in PHT System Flow Rate**
C3-6.4	Primary heat transport main coolant pump shaft seizure or pump shaft break.
C3-8.0	**Malfunction of Support/Auxiliary System**
C3-8.10	Loss of on-site electrical power supply (Class-III,II or I; one at a time).
C3-8.11	Rupture at any location of any pipe in process water system/ process water cooling system.
C3-8.12	Rupture at any location of any pipe of reactor moderator system.

TABLE-3: Contd...

EVENT NO.	EVENTS
C3-9.0	**Others**
C3-9.5	Safe shutdown earthquake (SSE) [Ref. AERB/SC/S, 1990: Code of Practice on Safety in Nuclear Power Plant Siting]
C3-9.6	Turbine failure leading to missile being thrown off
C3-9.7	Design Basis Flood [Ref. AERB/SC/S, 1990: Code of Practice on Safety in Nuclear Power Plant Siting]
C3-9.8	Design Basis Cyclone [Ref. AERB/SC/S, 1990: Code of Practice on Safety in Nuclear Power Plant Siting]
C3-9.9	Loss of normal and auxiliary feed water flow.
C3-9.10	Dam failure leading to loss of ultimate heat sink.

Note:- Ck-m.n type numbering convention has been followed for numbering of events. First number "Ck" refers to category, second number "m" refers to functional classification and the third number "n" is the serial number for a particular functional group. Serial numbers are given sequentially in all categories of events. This note is applicable to Tables-2,3 and 4.

TABLE-4: CATEGORY-4 EVENTS

MULTIPLE FAILURES AND RARE EVENTS

EVENT NO.	EVENTS
C4-2.0	**Decrease in PHT System Inventory**
C4-2.11	Small or large LOCA coupled with any one of the following: 1. Failure of ECCS (in injection or recirculation mode). 2. Failure to close the isolation devices on the interconnects between the PHT loops. 3. Failure of steam generator auto-crash cooling. 4. Containment impairment characterised by any one of the following. (a) degraded operation of reactor building air coolers. (b) failure of one set of containment isolation dampers. (c) failure of containment isolation logic. (d) one door of main airlock stuck open and seals on second door deflated. (e) excessive communication between Volumes V1 and V2 of containment (bypassing suppression pool). (f) degraded operation of primary containment clean-up system. (g) excessive leakage from primary containment. (h) failure of secondary containment clean up and purge system.
C4-2.12	Failure of tube(s) in PHT system heavy water heat exchangers other than steam generator coupled with any one of the following:- 1. Failure of emergency core cooling system (in injection/ recirculation mode). 2. Failure to close the isolation devices on the interconnection between PHT loops. 3. Failure of steam generator auto-crash cooling actuation. 4. Failure to close the isolation devices on the pipes carrying process water to and from the heat exchangers.

TABLE-4: Contd...

EVENT NO.	EVENTS
C4-9.0	**Others**
C4-9.11	Station blackout (Simultaneous failure of Class-III and Class-IV Electrical Power Supply) for specified duration.
C4-9.12	Safe Shutdown Earthquake (SSE) simultaneous with loss of coolant accidents (LOCA): This is to be considered only for the purpose of design of those equipment/systems/structures whose failure could impair integrity of containment.
C-4-9.13	Fuel handling failure (event C2-7.2 or C2-7.3) coupled with containment impairment characterised by (a) failure of one set of containment isolation dampers or (b) failure of containment isolation logic or (c) one door of main airlock stuck open and seals on second door deflated.

Note:- Ck-m.n type numbering convention has been followed for numbering of events. First number “Ck” refers to category, second number “m” refers to functional classification and the third number “n” is the serial number for a particular functional group. Serial numbers are given sequentially in all categories of events. This note is applicable to Tables-2,3 and 4.

TABLE-5: BEYOND DESIGN BASIS EVENTS[5]

EVENT NO.	EVENTS
BDBE-1	Loss of coolant accident (LOCA) plus failure of both the reactor shutdown systems.
BDBE-2	Loss of coolant accident plus failure of emergency core cooling system followed by loss of moderator heat sink.
BDBE-3	Failure of coolant channel seal plug or end fitting leading to ejection of fuel bundle from coolant channel (event C3-2.10) coupled with containment impairment characterised by (a) failure of one set of containment Isolation Dampers or (b) failure of containment isolation logic or (c) one door of main airlock stuck open and seals on second door deflated.

5 An agreed methodology for analysis of these events should be arrived at by the Utility and the Regulatory Body.

ANNEXURE

EXAMPLES OF EVENTS THAT NEED NOT BE CONSIDERED FOR SAFETY ANALYSIS BASED ON DESIGN FEATURES AND JUSTIFICATIONS

A-1 Anticipated transients without scram:

It is assumed that multiple, reliable, independent and diverse parameters are provided for the reactor scram. Also, two independent and diverse systems are available for reactor shutdown.

A-2 Failure resulting from drop of loads on control rod drive mechanisms:

It is assumed that during operation of NPP the load handling over the reactor control mechanism should be permitted only after ensuring the reactor in guaranteed shutdown state with all the reactor shutdown devices in actuated condition.

A-3 Failure of steam generator support:

It is assumed that steam generator supports are conservatively designed having factor of safety much more than required in their designing for LOCA and SSE.

A-4 Massive failure of primary coolant pump casing:

It is assumed that the thickness of primary coolant pumps (PCP) casing is much higher than that required by design based on pressure consideration and governed by casting practices including quality control by NDT (examination by radiography etc.). Thus, stress level in the casing is low and casing failure is very remote.

A-5 Multiple steam generator (SG) tubes failure:

SG tubes have been designed to withstand all mechanical loads including those arising due to main steam line break(MSLB). SG tubes are periodically inspected as per in-service inspection (ISI). SG water chemistry is maintained within limits during operation. Thus, multiple failure of SG tubes is improbable.

A-6 Sudden and full flow blockage in reactor coolant channel:

Sudden and full flow blockage in any reactor coolant channel assembly is not considered credible. Possible blockages objects (viz. nuts, bolts etc.) fitting exactly with the geometry of the flow passage are unlikely.

A-7 Failure of mechanical joints in the primary coolant pump assembly:

Margin in designing bolts for flange joints of pump and its casing is normally high as compared to other pressure retaining components. Failure of all the bolts simultaneously in cascaded manner is very unlikely. Thus, failure of mechanical joints in pump assembly is quite unlikely.

A-8 Missiles resulting from aircraft :

Missiles resulting from aircraft are not considered as initiating events as siting considerations exclude selection of such a site. [Ref. AERB Safety Code AERB/SC/S, Rev. 0, 1990: "Code of Practice on Safety in Nuclear Power Plant Siting"].

BIBLIOGRAPHY

1. Lalere J. and Lebouleux, Ph., Analysis de Surete et Transferts de Technologie Associes des Reacteurs Francais exportes, paper No. IAEA-SM-275/l. IAEA Conference on Application of Safety Codes and Guides (NUSS Documents) in the light of Current Safety Issues, Vienna, (29 October-02 November, 1984).

2. Documenc A., Prise on Compte des Evenments Externes Extremes d’Origine Naturalle on Humaine dans la conception et L’Analyse de Surete des Reacteurs Nucleaires paper IAEA- SM-275/3, ibid.

3. Quenjart Daniel, Brisbois Jacques, Lanors Jeanre-Marie, Utilisation de Methods Probabilities Pour l’Evaluation De la surete de Reacteurs a Eau Pressurisee Construits en France, Paper No. IAEA-SM-275/5, ibid.

4. USNRC Regulatory guide No. 170, Standard format and Content of Safety Analysis Reports for Nuclear Power Plants, Chapter 15 on Accident Analysis, Rev. 3, (November 1978).

5. AECB-1149,Proposed Safety Requirements for Licensing of CANDU Nuclear Power Plants,(November 1978).

6. AECB-39, Draft Licensing Guide, (June 1980).

7. AECB, CANADA, Consultative Document C-6, (June 1980).

8. Yaremy E.M. Licensing Requirements for PHWR Safety Analysis, IAEA-AERB Workshop in Safety Analysis, Bombay (5-16 May 1986)

9. IAEA, International Nuclear Event Scale, Revised and Extended Edition, IAEA User’s Manual on INES (1992).

10. IAEA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level-1), IAEA Safety series No. 50-P-4 (1992).

11. IAEA, External Man-Induced Events in Relation to Nuclear Power Plant, IAEA Safety Series No. 50-SG-D5 (1982)

12. AERB, Fire Protection, AERB Safety Guide No. AERB/SG/D-4 (1999).

13. AERB, Code of Practice on Safety in Nuclear Power Plant Design,AERB Safety Code No.AERB/SC/D,Rev. 0 (1989)

14. AERB, Code of Practice on Safety in Nuclear Power Plant Siting, AERB Safety Code No.AERB/SC/S, Rev. 0 (1990)

15. NUCLEAR POWER CORPORATION OF INDIA LIMITED, Safety Analysis Reports Vol.-II for NAPS/KAPS., (1989)

16. AMERICAN NUCLEAR SOCIETY, ANS 18.2, (January 1972).

LIST OF PARTICIPANTS

WORKING GROUP

Dates of meeting :	February 13, 1996	November 11, 1997
	February 16, 1996	April 23, 1998
	May 6, 1996	July 1, 1998
	September 8, 1997	January 13, 1999
	September 15, 1997	May 27, 1999
	September 18, 1997	

Members of the Working Group:

Shri V.K. Mehra (Chairman)	: Head, LWRD, BARC
Shri S.S. Bajaj	: Chief Engineer (RSA), NPCIL
Shri A.K. Babar	: RSD, BARC
Shri C.N. Bapat	: Chief Engineer (RP), NPCIL
Dr. S.K. Gupta (Invitee)	: RSD, BARC
Shri S.A. Khan (Member-Secretary)	: DRI&E, AERB

ADVISORY COMMITTEE FOR CODES, GUIDES AND ASSOCIATED MANUALS FOR SAFETY IN DESIGN OF NUCLEAR POWER PLANTS (ACCGD)

Dates of meeting :	July 29 & 30, 1996	December 2, 1998
	November 4, 1997	January 15, 1999
	June 16, 1998	February 5, 1999
	August 28, 1998	June 4, 1999

Members and alternates participating in the meetings:

Shri S.B. Bhoje (Chairman)	:	Director, RG, IGCAR
Shri S. Damodaran	:	NPCIL (Formerly)
Prof. N. Kannan Iyer	:	IIT, Mumbai
Shri V.K. Mehra	:	Head, LWRD, BARC
Shri Umesh Chandra	:	Head, RCnD, BARC
Shri A.K. Asrani	:	Director, DRI&E, AERB
Shri S. Sankar	:	Head, ROD, BARC
Shri C.N. Bapat	:	Chief Engineer (RP), NPCIL
Shri S.A. Bhardwaj	:	RSA Group, NPCIL
Shri S.K. Gupta	:	RSD, BARC
Dr. R.I.K. Murthy	:	RED, BARC (up to June 1998.)
Shri R.S. Singh (Member-Secretary)	:	DRI&E, AERB
Shri S.A. Khan (Permanent-Invitee)	:	DRI&E, AERB

ADVISORY COMMITTEE FOR NUCLEAR SAFETY (ACNS)

Date of Meeting : March 20, 1999

Members and alternates participating in the meetings:

Shri S.K. Mehta (Chairman)	:	Director RG, BARC (Formerly)
Shri S.M.C. Pillai	:	President & Chief Executive, Nagarjuna Power Corporation Limited, Hyderabad.
Prof. U.N. Gaitonde	:	IIT, Mumbai
Shri S.K. Goyal	:	Addl. General Manager, BHEL, Hyderbad.
Shri Ch. Surendar	:	Executive Director (Operations), NPCIL
Dr. U.C. Mishra	:	Director, H&SE Group, BARC (Formerly)
Shri S.K. Sharma	:	Director, RG, BARC
Dr. V. Venkat Raj	:	Director, H&SE and RDDG, BARC
Shri S.P. Singh	:	Head, NSD, AERB (Formerly)
Shri G.K. De	:	Head, NSD, AERB (Formerly)
Shri K. Srivasista (Member-Secretary)	:	NSD, AERB

PROVISIONAL LIST OF SAFETY CODES, GUIDES & MANUALS ON DESIGN OF PRESSURISED HEAVY WATER REACTOR

Safety Series No.	Provisional Title
AERB/SC/D	Code of Practice on Design for Safety in PHWR Based Nuclear Power Plants
AERB/SG/D-1	Safety Classification and Seismic Categorisation
AERB/SG/D-2	Application of Single Failure Criteria
AERB/SG/D-3	Protection Against Internally Generated Missiles and Associated Environmental Conditions.
AERB/SG/D-4	Fire Protection
AERB/SG/D-5	Design Basis Events
AERB/SG/D-6	Fuel Design
AERB/SG/D-7	Core Reactivity Control
AERB/SG/D-8	Primary Heat Transport Systems
AERB/SG/D-9	Process Design
AERB/SG/D-10	Safety Critical Systems
AERB/SG/D-11	Electrical Power Supply Systems
AERB/SG/D-12	Radiation Protection in Design
AERB/SG/D-13	Liquid and Solid Radwaste Management
AERB/SG/D-14	Control of Air-borne Radioactive Materials
AERB/SG/D-15	Ultimate Heat Sink and Associated Systems
AERB/SG/D-16	Materials Selection and Properties
AERB/SG/D-17	Design for In-Service Inspection
AERB/SG/D-18	LOCA Analysis
AERB/SG/D-19	Hydrogen Release and Mitigation Systems under Accident Conditions
AERB/SG/D-20	Safety Related Instrumentation and Control
AERB/SG/D-21	Containment Systems Design
AERB/SG/D-22	Vapour Suppression System
AERB/SG/D-23	Seismic Qualification
AERB/SG/D-24	Design of Fuel Handling and Storage Systems
AERB/SG/D-25	Computer Based Safety Systems
AERB/SM/D-1	Decay Heat Load Calculations

N O T E S