No: AERB/NPP-PHWR/SG/D-19

AERB SAFETY GUIDE

December 2018

DETERMINISTIC SAFETY ANALYSIS
FOR
PRESSURIZED HEAVY WATER REACTORS

ATOMIC ENERGY REGULATORY BOARD

AERB SAFETY GUIDE: AERB/NPP-PHWR/SG/D-19

DETERMINISTIC SAFETY ANALYSIS
FOR
PRESSURIZED HEAVY WATER REACTORS

Atomic Energy Regulatory Board
Mumbai - 400094
India

December 2018

Price:

Order for this Guide should be addressed to:

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

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 codes, safety standards and related guides and manuals for the purpose. While some of documents cover aspects such as siting, design, construction, operation, quality assurance, decommissioning of nuclear and radiation facilities, other documents cover regulatory aspects of these facilities.

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

This Guide is based on the current designs of 220 MWe, 540 MWe and 700 MWe Pressurised Heavy Water Reactors (PHWRs) and deals with establishing and confirming design basis by carrying out safety analysis of the plant design, applying deterministic methods, for the items important to safety. It demonstrates that the overall plant design ensures that radiation doses and releases are within the prescribed limits for operational states and acceptable limits for accident conditions. It provides guidance for the process by which events (to be analyzed) are selected, acceptance criteria for the plant states, performing accident analysis, documentation and review.

Consistent with the accepted practice, ‘shall’ and ‘should’ are used in the Guide to distinguish between a firm requirement and a desirable option respectively. Appendices are an integral part of the document whereas footnotes and references are included to provide information that might be helpful to the user. Approaches for implementation, different to those set out in the Guide, may be acceptable, if they provide comparable assurance against undue risk to the health and safety of the occupational workers and the general public and protection of the environment.

The guide applies only for facilities built after the issue of document. However during periodic safety review, a review for applicability of current guide for existing facilities would be performed.

For aspects not covered in this Guide, applicable national and international standards, codes and guides, acceptable to AERB should be followed. Non-radiological aspects such as industrial safety and environmental protection are not explicitly considered. Industrial safety is ensured through compliance with the applicable provisions of the Factories Act, 1948 and the Atomic Energy (Factories) Rules, 1996.

This Guide has been prepared by specialists in the field drawn from the Atomic Energy Regulatory Board, Bhabha Atomic Research Centre (BARC), Nuclear Power Corporation of India Limited (NPCIL) and other consultants of Department of Atomic Energy (DAE). It has been reviewed by the relevant AERB Advisory Committee on Codes and Guides & Associated Manuals for Safety in Design (ACCGD) of NPPs and Advisory Committee for Nuclear and Radiation Safety (ACNRS)

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

SABhardwaj

(S. A. Bhardwaj)
Chairman, AERB

DEFINITIONS

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

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

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

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

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

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

Defence-in-Depth
Provision of multiple levels of protection for ensuring safety of workers, the public or the environment.

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

Design Basis Accidents (DBAs)
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 Limits
Limits on the design parameters within which the design of the structures, systems and components of a nuclear facility has been shown to be safe.

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

Engineered Safety Features (ESF)
The system or features specifically engineered, installed and commissioned in a nuclear power plants to mitigate the consequences of accident condition and help to restore normalcy, e.g. containment atmosphere clean up system, containment de-pressurisation system etc..

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

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

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

Plant States (Considered in Design)

<table>
<tr><th colspan="2">Operational States</th><th colspan="3">Accident Conditions</th><th>Practically Eliminated Events (PEEs)</th></tr>
<tr><td rowspan="2">Normal Operations (NO)</td><td rowspan="2">Anticipated Operational Occurrences (AOO)</td><td rowspan="2">Design Basis Accidents (DBAs)</td><td colspan="2">Design Extension Conditions (DECs)</td><td>Large Release of Radioactivity from Containment</td></tr>
<tr><td>Accidents without core melt</td><td>Accidents with core melt*</td><td></td></tr>
</table>

* In case of PHWRs, as an exception single channel events resulting in fuel failure/melt in the affected channel shall not cause failure/melt of other channel and it comes under DBAs.

Postulated Initiating Events (PIEs)
Identified events during design that lead to anticipated operational occurrences or accident conditions, and their consequential failure effects.

Prescribed Limits
Limits established or accepted by the regulatory body.

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

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

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

Safety Function
A specific purpose that must be accomplished for safety.

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

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

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

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

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

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

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

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

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

Verification (Computer Code)
The process of determining that the controlling physical and logical equations have been correctly translated into computer code.

Special Definitions

Controlled State

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

(a) Core is subcritical
(b) Core heat is adequately removed.
(c) Activity discharges are within acceptable limits.

Safe Shutdown State

Safe Shutdown State is a state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and maintained continuously. This state is characterized by

(a) Reactor under shutdown with desired margin below sub-criticality
(b) Continuous decay heat removal up to ultimate heat sink through close loop cooling chain.
(c) Availability of containment functions

Safe State

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

(a) Core is under long term subcritical
(b) Long term decay heat removal is established
(c) Containment functions are available and activity discharges are in accordance with the acceptable limits.

Severe Accident Safe State

This is a state which shall be achieved subsequent to a design extension condition with significant core damage or core melt phenomena. Severe Accident Safe State shall be reached at the earliest after an accident initiation and can be maintained indefinitely. This state is characterized by

(a) No possibility of re-criticality
(b) Fuel or debris are continuously cooled
(c) Uncontrolled release of radioactivity to environment is arrested
(d) Means to maintain above conditions are available for long term, including critical parameter monitoring
(e) Monitoring of radiological releases and containment conditions.

CONTENTS

1. INTRODUCTION

1.1 General

1.1.1 AERB Safety Code on Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants- AERB/NPP-PHWR/SC/D (Rev. 1) [1] requires carrying out a comprehensive safety analysis[1] to evaluate the radiation doses that could be received by plant personnel and the public, as well as the potential effects on the environment. Safety analysis is required to be carried out for all plant states, viz. (i) Normal Operation (NO) (ii) Anticipated Operational Occurrences (AOO) (iii) Design Basis Accidents (DBA) and (iv) Design Extension conditions (DEC) as defined in section 2.1. DEC are divided in two categories i.e, DEC without core melt and DEC with core melt. DEC includes severe accident conditions involving significant core degradation or core melt. From this analysis, the robustness of the engineering design to withstand postulated events and accidents can be established, the effectiveness of the safety systems and safety related items or systems is demonstrated, and requirements for emergency response are prepared. Safety analysis of the plant design, applying deterministic methods, establishes and confirms that the design basis for the items important to safety and demonstrates that the overall plant design ensures radiation doses and releases are within the prescribed limits for operational states and acceptable limits for accident conditions.

1.1.2 AERB Safety Code on Nuclear Power Plant Operation- AERB/NPP/SC/O (Rev. 1) [2] requires that operating limits and conditions shall be confirmed by the results of safety analysis. The safety analysis of the plant design needs to be updated in the light of significant changes in plant configuration, operational experience, improvements in technical knowledge and better understanding of physical phenomena, and shall be consistent with the current or "as-built" state. During Periodic Safety Review (PSR), the validity of the existing safety analysis shall be examined and if required it shall be updated.

1.1.3 This safety guide provides guidance for carrying out Deterministic Safety Analysis (DSA) in order to demonstrate safety of pressurized heavy water reactor based nuclear power plants. This safety guide aims to standardize conducting and reporting of safety analysis in Preliminary/Final Safety Analysis Reports (PSAR and FSAR), as well as analysis for any other modifications in the plant affecting safety analysis of plants.

1.2 Objective

The objective of this guide is to provide guidance for deterministic safety analysis for PHWRs based nuclear power plants, taking into account the specific design. The aim is to provide guidance for the process by which events (to be analysed) are selected,

[1]Safety analysis consists of deterministic safety analysis and probabilistic safety analysis. This Safety Guide deals with deterministic safety analysis only. The term 'safety analysis' used in this Safety Guide should be considered as deterministic safety analysis.

categorized, assigning relevant acceptance criteria to the plant states, performing accident analysis, documentation and review.

1.3 Scope

1.3.1 This design safety guide provides information on the preparation and presentation of deterministic safety analysis reports, review and how and when update the safety analysis.

(a) This safety guide aims to provide harmonized guidance for performing such analysis for PHWRs primarily for PSAR, FSAR and PSR; as also for other submission related to safety analysis.

(b) This safety guide deals only with events and events sequences originating in the reactor or in its associated process systems.

(c) The guide provides the information for the events to be analysed for licensing purpose. Applicable acceptance criteria for the plant states are also provided in the guide.

(d) Deterministic safety analysis approaches, analysis rules, presentation and review aspects of results are provided in the guide. Application of deterministic safety analysis for design, emergency operating procedures are also provided in the guide.

(e) The safety guide focuses on neutronic, thermal hydraulic, fuel, and radiological analysis. Aspects of other types of analysis, such as structural mechanical analysis or analysis of electrical transients, are not covered in the Guide.

(f) This guide specifically deals with safety analysis of PHWRs only. The guide does not consider the external and internal hazard aspects.

2. PLANT STATES AND EVENTS TO BE ANALYSED

2.1 Plant States

2.1.1 As per AERB Safety Code on Design of Light Water Reactor Based Nuclear Power Plants- AERB/NPP/LWR/SC/D [3], plant states (considered in design) for nuclear power plants are divided into operational states, accident conditions and practically eliminated events as per definition. Operational states include normal operation and anticipated operational occurrences. Accident conditions include Design Basis Accidents (DBAs) and Design Extension Conditions (DEC). The DECs are accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility. DECs are divided in to two categories DEC without core melt and DEC with core melt. DECs include severe accident conditions involving significant core degradation or core melt[2]. The severe accident sequences which may lead to early or large radioactivity release are required to be practically eliminated. Considerations of DEC are also in line with IAEA Safety Standard, Specific Safety Requirements (No. SSR 2/1) – Safety of Nuclear Power Plants: Design [4]. Accident sequences must be assessed before concluding them Practically Eliminated Events (PEEs). For guidance on practical elimination of events and event sequences, Design Safety Guide (AERB/SG/D-5, Rev.1) [5] should be referred.

2.2 Events Identification and Categorization

2.2.1 The set of events and events sequences developed for the safety analysis should be comprehensive and should be defined in such a way that they cover all credible failures of plant systems and components and human errors which could occur during any of the plant states.

2.2.2 Guidance on categorization of events is given in AERB Safety guide of Design basis events for Pressurized Heavy Water Reactors, AERB/SG/D-5, Rev.1 [5].

[2]In PHWRs, single channel events due to sudden or complete flow stoppage in the affected channel may result in fuel failure/fuel melt in that channel. Such events are categorized as DBA; however, this event should not cause failure/melt of other channels

2.3 Events to be Analysed

2.3.1 The design basis events that are required to be analysed for safety analysis of PHWR based NPPs are given in AERB Safety Guide on Design Basis Events for Pressurized Heavy Water Reactors, AERB/SG/D-5, Rev.1 [5] and additional PIEs if identified in 2.2.1.

2.3.2 Computational analysis of all possible scenarios may not be practicable. A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each functional category of events for all plant states with appropriate justification [6]. 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.

2.3.3 The event to be analysed should first be assigned to a particular plant state to enable checking of the consequences against the defined acceptance criteria for the plant state/specific acceptance criteria for the event (See Section 3.2 and 3.3).

2.3.4 Any event that has occurred in a NPP need to be assessed to ensure that it is enveloped within the existing safety analysis, otherwise it has to be analysed.

2.3.5 Safety analysis/assessment may also need to be carried out as required for event sequences identified in Probabilistic Safety Assessment (PSA), and preparation of Emergency Operating Procedures (EOPs)/Accident Management Programme (AMP) guidelines (See Section 6.4 and 6.5).

3. ACCEPTANCE CRITERIA

3.1 General

3.1.1 Once the events are identified, and assigned to a particular plant state as described in section 2, then the safety analysis must show compliance with the set of acceptance criteria.

3.1.2 Acceptance criteria shall be assigned to each category that take account of the requirement that frequent events shall have only minor or no radiological consequences, and that events that may result in severe consequences shall be of very low probability. Acceptance criteria should be established to serve as thresholds of safe operation in normal operation, AOO and DBA and DEC.

3.1.3 The criteria should be sufficient to meet the General Nuclear Safety Objective, the Radiation Protection Objective and the Technical Safety Objective as given in AERB Safety Code on Design of Pressurised Heavy Water Reactor Based Nuclear Power Plants-AERB/NPP-PHWR/SC/D (Rev. 1) [1]. These acceptance criteria should be specified with respect to fundamental safety functions and condition of barrier to radioactivity release. Acceptance criteria are also specified in terms of end state desired for a plant state.

3.2 Acceptance Criteria for Plant States

The following acceptance criteria should be assigned for the various plant states.

3.2.1 Normal Operation

The annual radioactivity release limits for all the facilities within a particular site (taken together) shall ensure that the effective dose limit for any individual at off-site, due to normal operation is less than the limit specified by AERB [7].

-Effective doses to plant personnel shall be within the annual dose limits.

-Releases of radioactive material to the environment shall be within the allowable limits of normal operation.

-Fundamental safety functions shall be reliably continuing with designed systems.

-Fuel center line temperature shall not exceed as per limit given in [8].

-Critical heat flux to normal heat flux ratio shall as per limit given in [8].

-Fuel cladding strain limit shall be as per limit given in [8]

-Plant parameters shall be within their respective Limiting Condition of Operation (LCO) values, as defined in Station Technical Specifications.

3.2.2 Anticipated Operational Occurrences

The annual radioactivity release limits for all the facilities within a particular site (taken together) shall ensure that the effective dose limit for any individual at off-site, due to anticipated operational occurrences is less than the limit specified by AERB [7]

-Control of reactivity should be established following events. Reactivity control shall be established by reactor regulating system or by automatic shutting down reactor on reaching trip set points or by manual reactor shut down.

-Fuel center line temperature shall not exceed as per limit given in [8]
-Critical heat flux to normal heat flux ratio shall be as per limit given in [8]
-Sheath strain limited should be as per limit given in [8]
-Controlled state shall be achieved following AOOs
-Primary and Secondary system pressure shall be maintained below 110% of design value [9]
-Containment pressure shall remain above the designed negative pressure and below the designed positive pressure.
-Differential Pressure on Containment internal structures shall not cause internal structure failure.

3.2.3 Design Basis Accidents

Permitted calculated off-site releases during accident conditions shall be linked to the radiological consequence targets as specified. For design basis accident (DBA) in an NPP there shall be no need for offsite countermeasures (i.e. no need for prophylaxis, food control, shelter or evacuation) involving public beyond Exclusion Zone.
In such cases the design target for effective dose calculated using realistic methodology shall be less than limit given as per [7].

-Reactor shall be tripped following event and maintained in safe shutdown state
-There shall be no prompt criticality following the event
-There shall not be any fuel melting (except for single channel event) [8].
-The fuel pellet radial average enthalpy of the hottest fuel element shall not exceed the specified limit given in [8]
-Emergency core cooling acceptance criteria shall be satisfied as per [9, 10] for the events requiring actuation of emergency core cooling system for mitigation.
-Fuel channels integrity shall be maintained except single channel failure.
-Fuel channels geometry shall remain coolable.
-Primary and Secondary system pressure shall be maintained below 120% of design value [11]
-Containment pressure shall remain above the designed negative pressure and below the designed positive pressure
-Differential Pressure on Containment internal structures shall not cause internal structure failure
-Local hydrogen concentration in containment maintained outside the bounds of deflagration and detonation limit on ternary diagram [12] AERB/SG/SM-D2
-Containment integrity shall be maintained without venting system.

3.2.4 Design Extension Condition (without core melt)

For accidents without core melt within design extension conditions (multiple failure situations and rare external events) there shall be no necessity of protective measures in terms of sheltering or evacuation for people living beyond Exclusion Zone. Required control on agriculture or food banning should be limited to a small area and to one crop. However, the design target for effective dose, with such interventions considered, remains same as for DBA [7].

-Reactor shall be tripped following event and maintained in safe state
-There shall be no prompt criticality following the event
-Fuel channels integrity shall be maintained.
-Containment structural integrity shall be ensured for those events having radiological consequences.
-Differential Pressure on Containment internal structures shall not cause internal structure failure
-Global hydrogen concentration in containment shall be maintained outside the bounds of deflagration limit on ternary diagram. Local hydrogen concentration shall be such as to prevent local detonation.
-Credit for Containment Filtered Venting System (CFVS) shall not be taken for the licensing analysis for new NPPs (700 MWe), and for old PHWR units (up to 540 MWe), the venting system credit would be considered on a case to case basis (wherever containment pressure exceeds design pressure).

3.2.5 Design Extension Condition (with core melt)/including Severe Accident
In case of severe accident e.g. accidents with core melt within design extension conditions, the release of radioactive materials should cause no permanent relocation of population. The need for offsite interventions should be limited in area and time [7].
-Prevention of re-criticality of the partial or complete core melting shall be achieved
-Sufficient cooling of core debris shall be maintained within the containment
-Prevention of hydrogen detonation shall be achieved, which could result in containment failure
-Severe accident safe state shall be maintained.
-Credit for Containment Filtered Venting System (CFVS) shall not be taken for the licensing analysis for new NPPs (700 MWe), and for old PHWR units (up to 540 MWe), the venting system credit would be considered on a case to case basis (wherever containment pressure exceeds design pressure).

3.3 Acceptance Criteria for Specific Events

3.3.1 Following are the acceptance criteria for specific events of PHWRs. These acceptance criteria are in addition to the respective plant state acceptance criteria.

3.3.2 Single Channel Event
(a) Fuel failure/melt in the affected channel may occur.
(b) Failure/melt in the affected channel shall not cause failure/melt of other channel [9]
(c) Calandria pressure transient shall not cause calandria vessel failure.

3.3.3 Moderator System Failure
For anticipated operational occurrences and design basis accidents
(a) Deuterium concentration in the cover gas shall not exceed deflagration limits.
(b) Calandria tube-Endshield tube sheet rolled joint temperature shall not exceed its design temperature.

3.3.4 Endshield Cooling System Failure
For anticipated operational occurrences and design basis accidents

(a) There shall not be consequential failure of Primary Heat Transport (PHT) system boundary

(b) Calandria tube – endshield tube sheet rolled joint temperature shall not exceed design temperature

4. DETERMINSITIC SAFETY ANALYSIS

4.1 General

4.1.1 Safety analysis consists of deterministic safety analysis and probabilistic safety analysis. It is customary to refer to deterministic safety analysis as accident analysis.

4.1.2 This design safety guide mainly covers deterministic safety analysis aspects. The aim of the safety analysis should be by means of appropriate computational tools to establish and confirm the design basis for the items important to safety, and to ensure that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant states [13].

4.1.3 Inputs from the design, manufacture, construction and commissioning should be considered in the final safety analysis report to ensure that the design intent has been incorporated into the as-built plant.

4.1.4 The safety analysis should proceed in parallel with the design process, with iteration between the two activities. The scope and level of detail of the safety analysis should increase as the design programme progresses so that the final safety analysis reflects the final plant design as constructed.

4.1.5 Guidance contents in this document can also be used for a periodic safety analysis of an operating plant or for the safety justification of a proposed design modification.

4.1.6 The plant design models and data in the plant analytical models (which are essential foundations for the safety analysis) should be kept up to date during the design phase and throughout the lifetime of the plant. This should be the responsibility of the designer during the design phase and of the operating organization over the life of the plant.

4.1.7 For licensing calculations, if at any time credible information comes to light which brings into question the conservatism of the existing analysis, the re-analysis with new information shall be performed and it should be shown that acceptance criteria continued to be satisfied.

4.1.8 The safety analysis process should be credible, with sufficient scope, quality, completeness and accuracy to generate the confidence of the designer, the regulatory body, the operating organization and the public in the safety of a plant's design.

4.2 Responsibility

The responsible organization should ensure that the safety analysis meets all applicable regulatory requirements. The responsible organization should

(a) maintain adequate capability to perform or obtain safety analysis, meeting the relevant quality requirements.

(b) have an established process to update safety analyses which takes into consideration operational experience, research findings and identified safety issues.

4.3 Objective of Deterministic Safety Analysis

4.3.1 The deterministic safety analysis should formally assess the performance of the plant under various plant states, against applicable acceptance criteria. [14].

4.3.2 The safety analysis should assess whether all levels of defence in depth has been provided and are preserved.

4.3.3 To understand operational transients and plant system response.

4.3.4 To arrive at performance requirements for design of safety systems[3].

4.3.5 To develop a basis for various limits and 'Limiting conditions for Operation' (LCOs) to be specified in the technical specifications for operation of the plant.

4.3.6 Assist in establishing and validating accident management strategies, procedures and guidelines, EOPs, SAMGs and human factor aspects.

4.3.7 Confirm that modifications to the design and operation of the NPP have no significant adverse effects on safety.

4.3.8 Predict source term and doses during accident conditions to support emergency preparedness and response.

4.4 Safety Analysis Procedures

4.4.1 The steps involved in deterministic safety analysis using appropriate computer codes are illustrated below (Figure 4.1). This figure also includes cross reference where more guidance is provided.

---

[3]Examples are requirements for speed of actuation, and 'reactivity worths' of reactor shutdown devices; process requirements of emergency core cooling system; containment design parameters; safety system and their settings. Also, whether a particular corrective action can be manual or should be automated based on how fast the action is required to be completed.

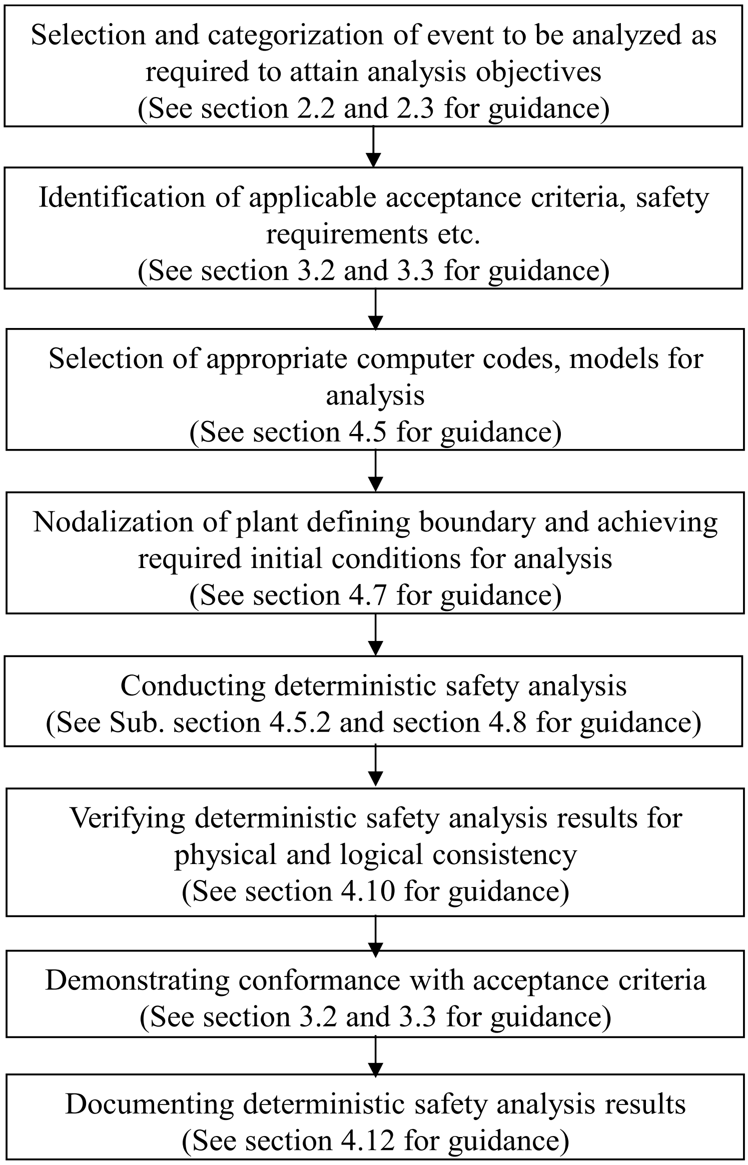

Figure 4.1: Steps involved in deterministic safety analysis

4.5 Performing Safety Analysis with Computer Codes

4.5.1 General

Complex computer codes are used for the analysis of the performance of NPPs. Computers codes for safety analysis broadly cover [15] the following areas.

-Reactor Physics
-Fuel behaviour
-thermal hydraulic
-Computational fluid dynamics
-Containment Analysis
-Atmospheric dispersion and Radiological Impact Assessment (RIA)
-Structural analysis
-Thermo-mechanical behaviour

All the important phenomena identified should be represented in the models embedded in the computer code used for calculation. The models and computer code applicability to the analyzed event should be demonstrated. Model of the plant systems shall be verified to reflect as built plant condition. User of the computer codes should make sure that codes are appropriate for their end use.

4.5.2 Analysis Approaches

Safety analyses are carried out by using computer code, initial and boundary conditions, taking credit for availability of the system in the analysis. Various approaches [16] to carry out safety analysis are given in Table 4.1.
The key words used in the Table 4.1 are defined based on [15, 16] and given below. Conservative code: A combination of all the models necessary to provide a pessimistic estimate for a physical process relating to specified acceptance criteria.

Best estimate code: A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. Best estimate model provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of the phenomena concerned. The term 'best estimate code' means that the code is free of deliberate pessimism, and contains sufficiently detailed models and correlations to describe the relevant processes for the transients that the code is designed to model.

Conservative assumptions on system availability: This includes applicable single failure criterion over and above the systems and component which can be taken on maintenance as per design intent. Applicability of single failure criterion is defined in section 4.8.6.

Best estimate assumptions on system availability: Except system taken under maintenance as per design intent, application of single failure criterion may not be required.

Table 4.1. Approaches for Safety Analysis

Option Number	Computer Code Type	Assumptions on systems availability	Type of initial and boundary conditions	Applicable Plant States
1	Conservative	Conservative	Conservative	DBA
2	Best Estimate	Conservative	Conservative	DBA
3	Best Estimate	Conservative	Best estimate; partly most unfavourable conditions	DBA
4	Best Estimate	Best Estimate	Best Estimate	AOO and DEC without and with Core melt

Conservative type of initial and boundary conditions: Plant parameters, initial and boundary conditions chosen to give a pessimistic result, when used in a safety analysis code, in relation to specified acceptance criteria. This includes the error in measurement/prediction of parameter by experiment or suitable models.The complete analysis requires use of sensitivity studies to justify conservative selection of input data.

Best estimate type of initial and boundary conditions: Plant parameters, initial and boundary conditions plant conditions corresponds to nominal value corresponding to operating condition.

Best estimate; partly most unfavourable conditions: few parameters on initial and boundary condition are selected as nominal value and few parameters still may have conservative value.

Option 3 can be termed as “Best Estimate Plus Uncertainty”. The difference between Options 2 and 3 is that in Option 3, whenever extensive data are available, the best estimate input data is used, and whenever data are scarce, use is made of the conservative input data. The use of “best estimate” requires that the uncertainties be accounted for by a statistical combination of uncertainties. This approach is defined in 4.8.12.

Deterministic safety analysis performed according to options 1, 2 and 3 is considered conservative analysis, with a decreasing level of conservatism from options 1 to 3.

Any option out of Option Number 1 or 2 or 3 can be selected for licensing analysis for design basis accident, to demonstrate that the safety system alone in short term and with operator action in long term are capable of fulfilling fundamental safety functions and meeting the acceptance criteria of DBAs, as given in Section 3.2.3.

The main objective of the realistic analysis of AOOs (option 4) is to check that control systems can prevent a wide range of AOOs from evolving into accident conditions and that the plant can return to normal operation following an AOO. Therefore, analysis of AOOs, using Option 4, should aim at providing the most possible realistic response of the plant to the initiating event [11, 16]. Analysis for AOOs should also check that as far as possible, for such events, reactor trip and safety systems are not actuated, and acceptance criteria for AOOs as given in Section 3.2.2 are met.

However, to prove robustness of control systems, limited number of governing AOOs from each functional category should be analysed using Option 4 with conservative initial and boundary conditions [11, 16]. The initial and boundary conditions can be selected at their limit of Limiting Conditions of Operation (LCOs) specified in Station Technical Specification in such a way that they maximise the effect of the AOO in the corresponding functional category. Initial and boundary conditions of plant parameters, which are expected to influence the effect of AOOs, should be considered in the conservative direction [17] in order to maximize the effect of the AOO with respect to the functional class in which the event is categorized. This would be done so that the analysis can confirm that the selection of an LCO value is effective. Alternatively, the analysis results may be employed to derive a suitable value for use as an operating limit. Measurement error and accuracy of the instrumentation should be taken into account to decide conservative bound of these parameters. To ensure conservatism in boundary conditions, errors considering instrument accuracy for set point of different automated actuation logic (e.g. setback, reactor trip) should be accounted. In case of lack of clarity of conservative side of any input parameter due to counteracting effects of different phenomena, nominal value may be used. For such analyses also, acceptance criteria for AOOs, as given in Section 3.2.2 should be met. More guidance for such type of analyses is given in Appendix -II.

If AOOs are analysed with failure of control systems, then such event combination should be considered as DBA and should be analysed using any option out of Option Number 1, 2 or 3. For analysis of such event combinations, acceptance criteria of DBAs, as given in Section 3.2.3 should be met [11, 16].

For the analysis of design extension condition without core melt option 4 should be used to meet the acceptance criteria of design extension condition (without core melt) as per section 3.2.4. In addition, a systematic process involving expert engineering judgment should be used to identify potential cliff edge effects [11,16], such as fuel dryout, pressure boundary failure and inventory depletion and identify the dominant parameters by assessing their influence on analysis results for each acceptance criterion. Where the likelihood is considered to be high and the potential impact is large, sensitivity analyses should be used to demonstrate to the extent practicable that, when more conservative assumptions are considered for dominant parameters, there are still margins with respect to cliff edge.

As mentioned above, Option 3 (more conservative) is used for Deterministic Safety Analysis (DSA) for Design Basis Accidents (DBAs) and Option 4 (Best estimate – less conservative approach) is used for Design Extension Conditions (DECs). It is recognized that this approach could result in dose estimates more for DBAs than that from DECs (resulting from the event sequence escalated from same DBA). This would require proper explanation in analysis reports to avoid misunderstanding/confusion. To justify this kind of results, in addition, DSA for DBAs for governing cases should be repeated with Option 4 also.

For design extension condition with core melt, Option 4 can be used and for these analyses acceptance criteria as given in Section 3.2.5 should be used [11, 16].

4.6 Computer Code Verification and Validation

4.6.1 Verification

It is recommended that utility shall have mechanisms for verification of computer codes to ensure that the code correctly performs all the intended functions and does not perform any unintended function. In general, the verification of the code design should ensure that the numerical methods, the transformation of the numerical equations into a numerical scheme to provide solutions, and user options and their restrictions are appropriately implemented in accordance with the design requirements [15, 16]. The verification of the code design should be performed by means of review, inspection and audit. Independent verification process by independent group other than the group involved in the development of the code should be carried out. The verification of the code design should include a review of the design concept, basic logic, flow diagrams, numerical methods, algorithms and computational environment. The results of the all verification activities should be documented and preserved as a part of the system for quality management. If the code is run on a hardware or software platform other than that on which the verification process was carried out, the continued validity of the code verification should be assessed. The code design may contain the integration or coupling of codes. In such cases, verification of the code design should ensure that the links and/or interfaces between the codes are correctly designed and implemented to meet the design requirements. Comparisons with independent calculations should be carried out where practicable to verify that the mathematical operations are performed correctly. The tracking of errors and reporting of their correction status should be a continuous process and should be a part of code maintenance. The impacts of such errors on the results of analyses that have been completed and used as part of the safety assessment for a plant should be assessed.

4.6.2 Validation

4.6.2.1 Computer code validation shall be performed and documented for all computer codes that are used for the deterministic safety analysis of nuclear power plants. The purpose of validation is to provide confidence in the ability of a code to realistically predict the safety parameter(s) of interest. If code is upgraded by improving changing the models of the code, appropriate required validation should be carried out. Adequate documentation should be maintained for change in the version of code.

4.6.2.2 For validation of computer codes, combination of the following approaches as applicable are acceptable:

(a) computational checks: checking of individual model against analytical solutions or with existing correlations derived from experimental data wherever possible.
(b) separate effect test: Separate effect tests addresses specific phenomena that may occur on a nuclear power plant but the test does not address the other phenomena that may occur at the same time.
(c) integral test: Integral test are directly related to a nuclear power plant. All or most of the relevant physical process are represented. However these tests are may be at reduced scale, use substitute material or be performed at low pressure.
(d) operational transients: Operational transients occur either in an actual nuclear power plant or an experimental rig which represents the plant at full scale and in realistic conditions. Validation through operational transients together with NPP tests is crucial to qualify the plant model. Though it is noted that data from actual operational transients are subject to measurement as available at the time of incident.
(e) inter code comparisons.
(f) Solving the standard/benchmark problem.
(g) Commissioning data and Operational data

4.6.3 Computer code validation should be properly documented and validation report should be referenced in utility submissions for licensing. Regulatory body may ask for submission of computer code validation report for review. Once reviewed, such validation reports can be referenced in future submissions (unless there is a major modification in the computer code.

4.6.4 Computer Code Documentation
Responsible organization should maintain documentation for each computer code used for safety analysis. Information from the code documentation may be used for facilitating review of the models and correlations employed, and to ensure that the models for important phenomena are appropriate. The code documentation should also include user manual and input descriptions to ensure that user can use the software properly.

4.7 Input Data Preparation for Safety Analysis

4.7.1 Authentic input data should be used for safety Analysis. Appropriate reference of the source of the input data should be provided in the safety analysis report. The input data should be collected from plant design documents, technical specifications of equipment, documentation gathered during the commissioning and startup of NPP, operation documents for the plant (limit and conditions, operating instructions, and record of operational regime, ‘As built’ plant information). It is preferred that all data necessary for the preparation of a particular computer code input deck (input file) is compiled and formalized into a single document, which can be referred in deterministic safety analysis reports. This source of information needs to contain all necessary information, such as information on geometry, thermal hydraulic parameters, material properties, characteristics of control system and set points, and the range of uncertainties in plant instrumentation devices, including references to drawings and other permanent documents. Physical properties used in the analysis/input should be well documented and referenced and its range of applicability and dependencies on pressure, temperature, etc. should also be mentioned.

4.7.2 Nodalization Schemes should be selected with sufficient details for all the important phenomena of the scenario and design characteristics of NPP under investigation to be represented. For example, considerations should be given to modelling of the channels at different elevations when such modelling is expected to influence results significantly. Important geometrical parameters, boundary conditions and initial conditions of achieved steady state should be compared with design values and reported. In case of reactor power of 103% for conservative analysis, steady state should be achieved by keeping the flow constant (at Design Rated Power). It should be ensured that effect of change of spatial size of node in final nodalization on the results of analysis is not significant. Important phenomena to be observed during different event should be verified and reported. It should be ensured that the effect of time step on the result of analysis is negligible.

4.7.3 User Effect

The user has to make many input decisions for typical system code calculations, including: the level of system nodalization; input parameters for code models and specific system characteristics and components; initial and boundary condition for system; state transport properties.

User effect could be reduced in the following ways:

-by using a code which has capabilities to identify probable input errors.
-by reducing the number of code options to be selected by code users by making sophisticated modeling of the process,
-by enhancing qualification and training of users.
-by mutual discussions among users.

4.7.4 If more than one code are used for the analysis of a initiating event or event sequence then methodology used for coupling of codes should be addressed in detail, in particular information exchange among codes and numerical convergence in each code.

4.8 Safety Analysis Rules

Assumptions and other considerations for the safety analysis should depend on the plant state for which analysis is being carried out. These are given below taking into consideration objectives of safety demonstrations of plant states [15, 16].

4.8.1 Initial and Boundary Conditions

As deliberated in sub-section. 4.5.2.

4.8.2 Neutronics Considerations

Deterministic safety analysis for events associated with reactivity changes require the solution of reactor kinetics equations (either point kinetics or space time kinetics equation in 1-2 or 3 dimensions). Use of point kinetics instead of coupled 3-D neutron kinetics should be justified on event basis for all plant states. The applicability of solution method, its accuracy and conservatism, should be ensured.

4.8.3 Thermal Hydraulic considerations:

Consideration should be given to simulation of different phenomena/aspects like critical discharge rate, stored energy in fuel and structural components, sources of heat in fuel, heat losses from structural components, phenomena related to fuel and channel behaviour under different condition, thermal and flow stratification, flow reversal, swell level, thermo-syphoning, equilibrium and non-equilibrium among phases, different modes of heat transfer, re-flooding, Counter Current Flow Limitation(CCFL), simulation of different components like pump, pressuriser, steam generators, accumulators, valves etc., depending upon scenario. Multidimensional phenomena should be adequately simulated and Computational Fluid Dynamics (CFD) simulation should be made whenever needed. Coupling between other codes like neutronics, structural, source term and codes for specific application should be appropriately accounted. Typical representative list of phenomena [18, 19] experienced during some of the important accident scenarios is given in Table I.1 phenomena matrix of Appendix I.

4.8.4 Reactor Trip Parameters

For analysis of design basis accidents, reactor trip function should be assumed to be actuated on reaching set point of the second trip parameter; ignoring the trip parameter reached first [20]. These first and second trip parameters could be on same or different shutdown system. However, first trip signal may be credited for AOOs and DEC.

4.8.5 Delay in Reactor Trip

For reactor trip, first the sensor should sense that the trip set point is reached. Thereafter there are delays in processing the information. For reactor trip the total instrumentation delays should be accounted, till the shutoff rods begin to fall or poison injection valves begin to open. This time delay in reactor trip should be considered for analysis of anticipated operational occurrences, design basis accidents and design extension conditions.

4.8.6 Single Failure Criterion

The single failure criterion shall be applied to each safety group or the assembly of equipment designated to perform all actions required for a particular event, to ensure that the limits specified in the design basis for design basis accidents are not exceeded. For AOO and DEC single failure criteria may not be considered.

4.8.7 Control System

For analysis of design basis accidents, no credit should be taken for the control system provided for normal plant control, unless such a control action could aggravate the accident or delay the actuation of the protection features. For analysis of anticipated operational occurrences credit of plant controls may be taken unless the initiating event leads to unavailability of a particular control system.

4.8.8 Offsite Power

For design basis accidents, in addition to a single failure and any consequential failures, a loss of off-site power should be assumed if it has unfavourable results. The loss of offsite power should be assumed at the initiation of the event or at the initiation of shutoff rod movement/poison injection, whichever is conservative. Additional consideration of Loss of offsite power along with events may not be required for the analysis of AOO and DEC.

4.8.9 Consideration of Systems

(a) For analysis of anticipated operational occurrences and design basis accidents, credit for equipment and systems for mitigation can be taken only if such equipment and systems are designed for the environmental conditions expected to be prevailing during the event.

(b) For analysis of anticipated operational occurrences and design basis accidents credit of systems provided for prevention and mitigation of DEC should not be taken.

(c) For analysis of design extension conditions, credit can be taken for both safety and non-safety systems provided their survivability is demonstrated.

(d) Assumptions on credit of availability of the system should be as per table 4.1. Minimum allowed configuration of equipment and system as per limiting condition of operation of Technical Specifications should be considered. This consideration is over and above the single failure criterion.

(e) For analyses of all plant states, any process equipment that is operating prior to the event is assumed to continue operating, if it is not affected by the initiating event.

4.8.10 Decay Heat

Decay heat should be estimated using computer code ORIGEN2. For design basis accidents decay heat enveloping all fuel burnups should be considered; whereas for analysis of other plant states, decay heat corresponding to channel average burnup (selected channel for lumping for representative) can be considered.

4.8.11 Operator Action Time

Safety analysis of the plant should take proper account of potential human errors in operational states and accident conditions. The time available for operator actions should be considered from the first clear and unambiguous indication of the necessity for operator actions Operator actions should be as follows:-
-Credit for operator action should not be considered earlier than 20 min. [21] (if actions are taken from main control room)
-Credit for operator action should not be considered earlier than 30 min. (if actions are taken from the field)
In both the above cases sufficiently detailed procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. Safety analysis should take into account that the credit for such operator intervention is acceptable only if the:
(a) design can demonstrate that the operator has sufficient time to decide and to act,
(b) necessary information on which the operator must base a decision to act is simply and unambiguously presented,
(c) physical environment following the event is acceptable in the control room or in the supplementary control room/backup control points, and
(d) access route to that supplementary control room/backup control points, is available.

Action from supplementary control room shall be counted as field action.

For existing NPPs (220 and 540 MWe PHWR), in certain circumstances, which must be justified, an operator action shorter than 20 minutes for main control room action might be assumed, provided that:

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

4.8.12 Best Estimate Plus Uncertainty Analysis

Uncertainties in deterministic safety analysis, in particular for design basis accidents, need to be addressed when Option 3 is adopted (best estimate computer codes are used in combination with best estimate initial and boundary conditions and availability of systems is assumed in a conservative way) [Table 4.1]. To achieve conservative safety analysis, uncertainties [11, 16 and 22] should be identified and assessed to confirm that the actual plant parameters will be bounded by the results of calculation plus uncertainty with an adequate confidence.

There are three potential sources of uncertainties:

(a) Plant uncertainty:

Uncertainty in the parameters used in measuring or monitoring or representing a real plant which has significant effect on the acceptance criteria should be accounted, such as reference plant parameters, instrument error, set points, instrument response. Typical examples are the pressurizer level at the start of the transient, the conductivity of the fuel, and the gap between the pellets and the cladding/gap conductance, decay heat, primary pressure, secondary pressure, etc.

For the uncertainties associated with input parameters, the preferred means is the collection of nuclear power plant data of initial and boundary conditions that are relevant to the events being considered and based on these data obtain a probabilistic distribution.

Uncertainties associated with input parameter is obtained by performing a sufficient number of calculations varying these input uncertain parameters and monitoring the output parameters of relevance. Because there are thousands of plant parameters, one must first identify the sensitive ones (those which affect in a major way the analysis outputs used for comparison with the acceptance criteria) and the uncertain input parameters should include the most significant ones. The selected input parameters should be ranged and their probability distribution specified using relevant experiments, measurements of parameters, records of plant operational parameters, etc. If this is not feasible, the approach of "partly most unfavourable" [Table 4.1] may be followed. Conservative values from the given range should be used. Selected input parameters have to be independent or dependencies between uncertain input parameters should be identified and quantified and a specific processing should be applied.

The selection of uncertain input parameters, their ranges and probability distributions is crucial for the reliability of results, since it strongly affects the width of the uncertainty bands of the results that is essential for engineering applications.

Overall quantification of uncertainties should be based on statistically combined uncertainties in plant conditions and code models to ensure with a specified probability, that a sufficiently large number of calculated results meet the acceptance criteria.

(b) Representation or simulation uncertainty:

Uncertainty in representing or idealizing the real plant, such as that due to the inability to model a complex geometry accurately, three dimensional effects, scaling, control and system simplifications (e.g. modelling few channels instead of all the channels, radial and axial subdivision in the nodalization scheme etc.).

The amount of uncertainty introduced by the necessary simplifications in modelling a real plant can be estimated by performing a sensitivity study in which the simplification introduced in the model is reduced in a stepped manner. Measure of the uncertainty in the results introduced by the simplification should be quantified.

Results produced by computer codes are sensitive to decisions that are made by the user, such as the number and structure of nodes that are used. Such user effects could be particularly large for a specific analysis. The procedures, code documentation and user guidelines should be carefully followed to limit such user effects.

(c) Code or model uncertainty:

Uncertainty associated with the models and correlations, the solution scheme, model options, unmodelled processes and data libraries.
Validation of the code should be performed to assess the uncertainty of values predicted by the code. Outputs of the code are compared with relevant experimental data and with operational transients, if possible, for the important phenomena expected to occur. The code accuracy obtained as the result of validation work should be used as a source for uncertainties of relevant modelling parameters. It is important to focus the end point of the uncertainty analysis on parameters which, are used directly in comparison with acceptance criteria, for example, the clad temperature, the radiological dose to the public and the peak containment pressure. The purpose of uncertainty analysis is not to quantify the uncertainty in every prediction, but only in the parameters used directly in the comparison with acceptance criteria.

Uncertainties are deemed to be accounted for a code intended to be conservative regarding certain acceptance criterion. In that case, it should be demonstrated that the code prediction is conservative when compared against the experimental data.

4.9 Presentation and Evaluation of Results

The results of safety analysis should be structured and presented in an appropriate format in such a way as to provide a good understanding and interpretation of the course of the accident. A standard format is suggested for this type of analysis. The presentation of the results should be sufficiently complete to allow the entire process to be displayed, starting from the initial steady state up to the long term safe stable condition. The presentation of accident analysis results should contain those parameters reflecting the key phenomena expected to occur in the course of the transient or accident. The format of the results needs to be such as to allow an inter comparison with the results obtained from the same or different codes.

4.9.4 For presenting deterministic safety analysis in preliminary/final safety report, format given in AERB Safety Guide on Format and Contents of Safety Analysis Reports should be followed (AERB/SG/G-9) [6, 23].

4.10. Review of Deterministic Safety Analysis Results

4.10.1 Before any use of the results, their correctness needs to be carefully checked. This could be done on the basis of user experiences and logical judgment, comparison with similar calculations, sensitivity analysis and consistency with general findings. The results derived should be reviewed and evaluated in relation to the initial goal and purpose of the analysis, such as licensing, improvement of operational documentation or plant upgrading.

4.10.2 The prime objective of reviewing the results is to check by comparison of calculated values with criteria whether the acceptance criteria have or have not been satisfied. If the analysis is used for evaluation of the system safety performance, the review and discussion of the results needs to be focused on the safety functions and the status of the physical barriers.

4.10.3 A certain amount of attention should be devoted in the discussion of the results to their sensitivity to the key input parameters as well as to expected uncertainties and the tolerances band of the parameters, if analysis is not considered conservative and analysis results are very close to the acceptance criteria. The review of the results may lead to a specification of the additional analysis and the resolution of the relevant safety issues (if necessary).

4.10.4 The review and discussion of the results should address the correctness of the calculations.

4.11 Update of Safety Analysis

4.11.1 The objective of the update of safety analysis is to check the extent of validity of existing safety analysis taking into account the actual plant status, expected degradation till the next update of safety analysis or the end of predicted life and current analytical methods, safety standards and knowledge.

4.11.2 Overall Safety analysis of the plant should be reviewed and updated as required for all design basis events to ensure that the plant does not pose any undue hazard to the surrounding. During review, it should be ensured that the actual state of the plant including modifications is considered. In addition the completeness of the list of postulated initiating event should be checked. Current analytical methods including computer code should be used wherever re-analysis is required [2].

4.11.3 Accepted rules for analysis, operator action, common cause failures, redundancy, diversity, separation, etc. should be used. Required modification in any input data should be incorporated based on plant operation and operational feedback.

4.11.4 A revision of the safety analysis should be made on the basis of

-feedback from operational experience, the findings of periodic safety reviews, regulatory requirements,
-changes to the applicable rules and regulations and regulatory requirements
-advances in knowledge and improvements in technology
-modernization of the plant
-changes in the described plant configuration as implemented
-changes in operating procedures due to operational experience

-up-rating of the reactor power, use of improved types of fuel and innovative principles for core reloads

4.12 Quality Assurance in Deterministic Safety Analysis

4.12.1 Accident analysis needs to be the subject of a comprehensive quality assurance programme applied to all activities affecting the quality of the final results.

4.12.2 Formal quality assurance procedures and/or instruction need to be developed and reviewed for the whole accident analysis process, including.

-Collection and verification of plant data,
-Verification of the computer input file/deck
-Validation of plant models

4.12.3 It is helpful to approve a document on the method of analysis prior to performing an analysis. Such a document lists the models to be used, system assumptions, acceptance criteria and system nodalization.

4.12.4 The responsibilities of all individuals in the organization involved in the analysis need to be clearly specified. Safety analysts need to be trained and qualified. All documents, including calculational notes and results, need to be recorded to allow them to be independently checked by qualified reviewers. Validated and accepted methods and tools need to be used, and their uses need to be referenced. All sources of data should be clearly referenced and documented.

4.12.5 The result should be checked using one or more of the following techniques depending on the importance of the analysis.

-Peer review
-Independent review by competent individuals
-Independent calculation of the same case under analysis by a competent Individual

4.12.6 All safety analyses used for plant licensing need to archived so that the code version, code documentation, input data and calculation results are recoverable.

Chapter 5 SOURCE TERM ESTIMATION AND DOSE EVALUATION

5.1 General

To evaluate the source term and dose from a nuclear power plant, it is necessary to know the sources of radiation, the inventories of radionuclides and the mechanisms by which these can be transported through different barriers and released to the environment.

An evaluation of the behaviour of fission products, radioactive corrosion products, activation products in coolant and impurities, and actinides following possible accidents of each type at the NPP shall be carried out early in the design stage [6, 24]. This is required to identify all important phenomena that affect source term behaviour and to identify the possible design features that could increase their retention in the plant. For all plant states, source term should include all radionuclides (liquid or gas) which have significant contribution to dose [3].

5.2 Source Term

The amount and isotopic composition of material released (or postulated to be released) from a facility is called a Source Term (ST).

The radio nuclides releases from various barrier and its treatment can be addressed in following ways depending on the requirements i.e. (a) radionuclides release to containment (b) radionuclides in containment (c) radionuclides release outside environment. Detailed guideline on the source term and its modelling are given in AERB safety design guidelines on Radiological Impact Assessment for NPPs [25]

Source terms should be evaluated for operational states and accident conditions for the following reasons:

(a) To ensure that the design is optimized so that the source term will be reduced to a level that is as low as reasonably achievable;
(b) To demonstrate that the design ensures that requirements for radiation protection, including restrictions on doses, are met;
(c) To provide a basis for the emergency planning arrangements that are required to protect the public and assess the impact on the environment in the vicinity of the NPP;
(d) To demonstrate that the qualification of equipment that is required to survive, including instruments and gas treatment systems, is adequate;
(e) To support software for use in emergency planning that employs theoretical source terms related to the damage to the plant to provide an early indication of what emergency measures are required. This allows decisions to be made early, before measurements of the activity levels of released radioactive material outside the plant can be made;

The source term should be evaluated for the bounding scenarios in each plant states including severe accident.

The evaluation of source terms shall also include a comprehensive analysis of event or event sequence in which the release of radioactive material would occur outside the containment. This exercise ensures that the design is optimised so that requirements for radiation protection, including restrictions on doses, are being met.

5.2.1 Radionuclides Release to Containment

Release to containment should consider the magnitude, composition, physical and chemical form and timing of the release of fission products and other aerosols from core as a result of a reactor accident. Total release phenomena should be broadly divided into five phases;

a) Gap release on sheath failure,
b) Diffusional release on heating,
c) Grain boundary sweeping on oxidation in presence of steam,
d) Melt Release and
e) Vaporization Release.

A methodology to be adopted to calculate source term release from the fuel or to containment should consider the effects of operating conditions, nuclide properties, thermo-mechanical behaviour of the fuel and distribution of the fission products within the core at equilibrium core conditions.

Appropriate consideration should be given to account the retention of radionuclide in primary and moderator circuit as applicable before its release to primary containment.

5.2.2 Radionuclides in Containment

Source term in the containment should consider the magnitude, composition, physical and chemical form of the radionuclides and aerosols which are airborne in the primary containment environment with time.

All relevant attenuation processes inside containment should be modeled.

5.2.3 Radionuclides Release to Outside Containment

Source term to outside environment should consider the magnitude, composition, physical and chemical form of radionuclides and aerosols which is leaked out of containment to outside environment.

The evaluation of source terms should also include a comprehensive analysis of postulated accidents in which the release of radioactive material would occur directly outside the containment. For example, a loss of reactor coolant might involve a break in a system such as the secondary circuit that is outside the containment, and there would be a potential for the containment to be bypassed if there were a leakage path between the primary and secondary circuits. Accidents in which the release of radioactive material could bypass the containment form a very important category, because a bypass accident with a relatively small release of radioactive material from the fuel may have the same radiological consequences as an accident with a large release into the intact containment.

5.3 Dose Evaluation

Dose evaluation should be carried out by using either conservative or realistic analysis. The applicant should summarize the assumptions (stability class, metrological data, atmospheric dispersion model, ground deposition, etc.), parameters, and calculation methods used to determine the doses that result from accidents should be provided. The annual release of radioactive material to the environment can be evaluated by using an average value for the activity of the primary coolant. Values for the effect of spiking on the activity of the primary coolant due to applicable operational transient should be considered based on relevant operational data. The parameters and assumptions used for these analyses, as well as the results should be presented in tabular form. Sufficient information should be provided for an independent analysis to be performed. The following modelling aspects should be provided.

(a) the containment modelling,
(b) the leakage or transport of radioactivity from one compartment to another or to the environment, and
(c) the presence of ESFs such as filters or sprays that are relied upon to mitigate the consequences of a Loss Of Coolant Accident (LOCA).

All radionuclides which have considerable contribution on dose should be accounted. For the dose calculation all path ways (ingestion, inhalation, plume and ground shine) should be considered

In presenting the assumptions and methodology used in determining the radiological consequences, it should be ensured that analyses are adequately supported with backup information, either by reporting the information where appropriate or by referencing other sections. Detailed guideline on the source term and its modelling are given in AERB safety design guidelines on Radiological Impact Assessment for NPPs [25]

6. APPLICATION OF DETERMINSITIC SAFETY ANALYSIS

6.1 General

6.1.1 Deterministic safety analyses should be carried [15,16] for
- (a) design of nuclear power plants
- (b) licensing of nuclear power plants
- (c) providing inputs for probabilistic safety analysis
- (d) development of emergency operating procedures and accident management guidelines
- (e) analysis of events occurred at nuclear power plants
- (f) review and refinement of safety analysis as part of periodic safety review, and
- (g) review and assessment of modifications in NPPs

6.1.2 Before submitting safety analysis report to the regulatory body, the responsible organization should ensure that an independent verification of the safety analysis is performed by individuals or groups separate from those carrying out the original analysis.

6.1.3 Additional independent analyses of selected aspects may also be carried out by regulatory body itself or on behalf of the regulatory body by technical support organization. The responsible organization should provide the necessary inputs and details for such analyses to the regulatory body as per agreed terms and conditions.

6.2 Design of Nuclear Power Plants

Deterministic safety analysis should be used iteratively with NPP design process. The design basis for items that are important to safety should be established and confirmed by means of comprehensive safety assessment through both deterministic and probabilistic safety analyses. With reference to the deterministic safety analysis, applicability of the assumptions, methods and degree of conservatism used should be verified. The design requirements for structures, systems and components important to safety must be met for safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardize safety.

6.3 Licensing of Nuclear Power Plants

6.3.1 Deterministic safety analysis carried out for a NPP should be used for showing compliance with applicable regulations and standards and other relevant safety requirements. This should be presented to the regulatory body through Preliminary Safety Analysis Report (PSAR) for initial licensing of the NPP, and after regulatory review, it should be converted into Final Safety Analysis Report (FSAR) as per AERB/SG/G-9 [23] for format and contents of safety analysis report). The final safety analysis report should be consistent with the current or ‘as built’ state of NPP.

6.3.2 The safety analysis for licensing purpose should examine
- (i) All planned modes of the plant in normal operation;

(ii) Plant performance in anticipated operational occurrences;
(iii) Design basis accidents ;
(iv) Event sequences that may lead to Design Extension Conditions.

On the basis of this analysis, the robustness of the engineering design in performing its safety functions during postulated initiating events and accidents should be established. In addition, the effectiveness of the safety systems and safety related systems should be demonstrated, and guidance for emergency response should be provided.

6.3.3 Analyses should be performed for transients that can occur in all planned modes of the plant in normal operation, including operations during shutdown. For this mode of operation, the main objectives of the analysis are to evaluate the ability of plant systems to perform safety functions and to determine the time available for the operators to establish safety functions, considering the likely configuration of systems and equipment in shutdown state.

6.3.4 The range of scenarios should be evaluated to determine whether abrupt changes in the results of the analysis occur for a realistic variation of inputs (usually termed cliff edge effects)

6.3.5 Safety analyses should be performed for development of LCOs in station technical specification for operation. Results of safety analysis should be used for operator training, training simulator etc.

6.4 Providing Inputs for Probabilistic Safety Analysis

Deterministic Safety Analysis (DSA) should use the best estimate methods, best estimate computer codes, assumptions and data for providing inputs to PSA wherever possible. It is recognized that it is very difficult and time consuming to use best estimate DSA for all accident scenarios. In cases, where conservative DSA is used for some accident scenarios and best estimate DSA is used for the other scenarios, it should be ensured that the relative contribution of both DSAs do not distort the PSA results.

6.5 Development of Emergency Operating Procedures and Accident Management Guidelines

6.5.1 Best estimate deterministic safety analyses should be performed to confirm the strategies that have been developed to restore normal operational conditions at the plant following transients due to anticipated operational occurrences and accident conditions. These strategies are reflected in the emergency operating procedures that define the actions that should be taken during such events.

6.5.2 Deterministic safety analyses are required to provide the input that is necessary to specify the operator actions including time available for operator action to be taken in response to some accidents, and the analyses should be an important element of the review of accident management strategies. In the development of the recovery strategies, to establish the available time period for the operator to take effective actions, sensitivity calculations should be carried out on the timing of the necessary operator actions, and these calculations may be used to optimize the procedures.

6.5.3 After the emergency operating procedures have been developed, a validation analysis should be performed. This analysis is usually performed by using a simulator. The validation should confirm that a trained operator can perform the specified actions within the time period allowed and that the reactor will reach a safe end state.

6.5.4 When the predictions of a computer code that has been used to support or to verify an emergency operating procedure do not agree with observed plant behaviour during an event, the code and the procedure should be reviewed. Any changes that are made to the emergency operating procedure should be consistent with the observed plant behaviour.

6.5.5 Deterministic safety analyses should also be performed to assist the development of the strategy that an operator should follow if the emergency operating procedures fail to prevent a severe accident from occurring. The analyses should be carried out by using one or more of the specialized computer codes that are available to model relevant physical phenomena. Applicable guidance on PHWR severe accident analysis given in IAEA TECDOC [26] can be used.

6.5.6 The analyses should be used to identify what challenges can be expected during the progression of accidents and which phenomena will occur. These should be used to provide the basis for developing a set of guidelines for managing accidents and mitigating their consequences.

6.5.7 The analysis should start with the selection of the accident sequences that, without intervention by the operator, would lead to core damage. A grouping of accident sequences with similar characteristics should be used to limit the number of sequences that need to be analysed. Such a categorization may be based on several indicators of the state of the plant: the postulated initiating event, the shutdown status, the status of the emergency core cooling systems, the coolant pressure boundary, the secondary heat sink, the system for the removal of containment heat and the containment boundary.

6.5.8 The measures can be broadly divided into preventive measures and mitigatory actions. Both categories should be subject to analysis.

6.5.9 Preventive measures are recovery strategies to prevent core damage. They should be analysed to investigate what actions are possible to inhibit or delay the onset of core damage. Conditions for the initiation of the actions should be specified, as should criteria for when to stop the actions or to change to another action.

6.5.10 Mitigatory measures are strategies for managing severe accidents to mitigate the consequences of significant core degradation. Possible adverse effects that may occur as a consequence of taking mitigatory measures should be taken into account, such as pressure spikes, hydrogen generation, return to criticality, steam explosions, thermal shock or hydrogen deflagration or detonation. Detailed guide lines for the same topic may be referred from a separate guide on Severe Accident Management Guidelines [27] being developed.

6.6 Analysis of Events Occurred at Nuclear Power Plants

6.6.1 Safety analysis may be used as a tool for obtaining a full understanding of events that occur during the operation of nuclear power plants and should form an integral part of the feedback from operating experience. Operational events may be analysed with the following objectives:

(i) To check the adequacy of the selection of postulated initiating events;
(ii) To determine whether the transients that have been analysed in the safety analysis report bound the event;
(iii) To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;
(iv) To check whether the plant operators and plant systems performed as intended;
(v) To check and review emergency operating procedures;
(vi) To identify any new safety issues and questions arising from the analyses;
(vii) To support the resolution of potential safety issues that are identified in the analysis of an event;
(viii) To assess the severity of possible consequences in the event of additional failures (such as severe accident precursors);
(ix) To validate and adjust the models in the computer codes that are used for analyses and in training simulators.

6.6.2 The analysis of operational events requires the use of a best estimate approach. Actual plant data should be used. If there is a lack of detailed information on the plant state, sensitivity studies, with the variation of certain parameters, should be performed.

6.6.3 The evaluation of safety significant events is a very important aspect of the feedback from operating experience. Modern best estimate computer codes make it possible to investigate and to gain a detailed understanding of plant behaviour. Conclusions from such analyses should be incorporated into the plant procedures that address the use of feedback from operating experience.

6.7 Review and Refinement of Safety Analysis as part of Periodic Safety Review

New deterministic analyses may be required to refine previous safety analyses in the context of a periodic safety review, to provide assurance that the original assessments and conclusions are still valid, considering the current status of NPP. The methodologies are defined in section 4.5.2 of this guide.

6.8 Review and Assessment of Modifications in Nuclear Power Plants

6.8.1 A nuclear power plant may be modified on the basis of feedback from operating experience (including a major event occurred at any NPP anywhere), the findings of periodic safety reviews, regulatory requirements, advances in knowledge or developments in technology. The modification of existing nuclear power plants may be undertaken to counteract the ageing of the plant, to justify the continued operation of the plant, to take advantage of developments in technology or to comply with changes to the applicable rules and regulations. A revision of the safety analysis of the plant design should be made when

(a) major modifications or modernization programmes are implemented
(b) advances in technical knowledge and understanding of physical phenomena are made
(c) changes in the described plant configuration are implemented
(d) changes in operating procedures are made owing to operating experience

6.8.2 Other important applications of deterministic safety analysis are aimed at the more optimum utilization of the reactor and the nuclear fuel. Such applications encompass uprating of the reactor power, the use of improved types of fuel and the use of innovative methods for core reloads. Deterministic safety analysis for such applications should be used for checking safety margins to operating limits, and it should be ensured that the limits are not exceeded.

APPENDIX I
Phenomena Matrix

Table I.1 Phenomena Matrix

Sr. No.	Phenomenon	Description	Safety significance	Indicative applicable events
1.	Change in power due feedback induced reactivity	Coolant-Density-Change (temperature and density changes in coolant and moderator, and changes in fuel temperature) Induced reactivity is the dominant influence on neutron kinetics, power and flux distributions in the reactor core.	Clad temperature increase and fuel failure. After reactor trip reactivity addition due shutdown device plays primary role in keeping reactor in safe shutdown state with adequate sub-criticality margin. After blowdown phase decay heat is importance source of heat.	Large Break (LB) LOCA, Small Break (SB) LOCA & Loss of Regulation Accident (LORA)
		Moderator-Density-Change Induced Reactivity Moderator system related failures	Changes in Reactor Power	Increase in Moderator Temperature
2	Xenon related phenomenon	This results in more increase in reactor power for slow LORA transient.	Changes in Reactor Power	Loss of Regulation Accident (LORA)
3.	Device-movement induced reactivity RRS s/d device	The device-movement induced reactivity is an important phenomenon during both the pre-shutdown and the post-shutdown phases. For the pre-shutdown phase, reactor-regulating-system response is significant.	For the post-shutdown phase, the effect of the shutdown system is dominant.	LBLOCA, SBLOCA & LORA
4.	Distribution (Prompt/decay heat) in space and time flux and power	The flux and power distributions during the early phase of LOCA characterize the reactor core configuration and have a strong influence on the subsequent transient. However, the decay heat characterizes the reactor physics behaviour during the blowdown phase of the transient	Rate of increase in fuel and clad temperature and subsequent fuel-clad failure and release of radioactivity.	LBLOCA, SBLOCA & LORA

System and Fuel Channel Thermal Hydraulics				
5.	Break flow, Critical flow in orifices in tail pipes	Single and two phase critical flow at the break	Determines the inventory of the system and its state and flow rate and depressurization rate of the system and core cooling, containment pressurization.	SBLOCA and LBLOCA with and without Emergency Core Cooling System (ECCS), Main Steam Line Break (MSLB), Steam Generator (SG) feed line break.
6.	Level swell and void holdup	Swelling of the level affecting the void holdup in SG due to depressurization of secondary side	Cooling rate of primary system to remove decay heat	MSLB and feed water line break to SG
7.	Single phase and two phase natural circulation	In the absence of RCPs, natural circulation (single-phase/two-phase) is established between the core and steam generators.	Decay heat removal from the core. And intermittent break of natural circulation and flow reversal	LBLOCA (intact loop), SBLOCA and Station Blackout (SBO)
8.	Phase separation	Vapour liquid separation/stratification in channel and, CCFL in feeder and headers. Phase separation is predominant at low flow and low pressure.	Spatial (asymmetric) heat up of coolant channel takes place and will lead to pressure tube straining. Delay in the ECCS injection.	LBLOCA, SBLOCA and SBO, Critical header size LB LOCA and stagnation channel break.
9.	Mixing and condensation during injection	As the ECCS water is injected, it mixes with the fluid in the headers causing rapid condensation of the vapour on the cold liquid. The efficiency of this process affects the depressurization of the system and causes system pressure oscillations. Also, this process	This process has an effect on core cooling because it affects the fluid flow through the core and therefore the cladding temperatures.	LBLOCA, SBLOCA and SBO.

		has direct feedback on other processes such as phase separation and CCFL		
10.	Core void and flow distribution	Flow distribution in the core during blowdown and refill.	The void distribution and coolant flow directly affects the fuel cladding temperatures.	LBLOCA, SBLOCA
11.	Core heat transfer including, DNB, Dryout	During low flow, Departure from nucleate boiling (DNB, dryout) and post-dryout heat transfer from clad to coolant dominates the fraction of void generation due to heat transfer from the clad to the coolant.	Determines fuel clad temperature and fuel failure.	LBLOCA, SBLOCA, SBO, LORA.
12.	Single and two-phase pump behavior	Two-phase behaviour of the pumps during large break LOCA leads to degradation or phase separation phenomena on the pump impellers affecting the timing and point of stagnation of the core flow.	Effect on the fuel cladding temperature excursion during blow-down.	LBLOCA
13.	Non-condensable gas effects	Nitrogen released from the accumulators has mechanical and thermal effects on the system behaviour. This will also affect condensation phenomena in various parts of the system. Hydrogen is released due metal water reaction.	Heat transfer deterioration due to plug formation at the top of SG tube and feeders. It plays important role in cooling the fuel.	LBLOCA, SBLOCA and SBO. LOCA along with failure of isolation of accumulator
14.	Reflux condenser mode and CCFL	The steam from the core is condensed in the steam generator tubes, and may flow to both tube ends.	Affects the heat removal process at low steam velocities.	SBLOCA, SBO
15.	Asymmetric loop/pass behaviour	Different heat removal capacity of loops (broken and intact loop and broken and unbroken pass of same loop), caused by asymmetric mass flow and distribution.	Will reduce the overall heat removal capacity.	SBLOCA & LBLOCA, MSLB, SBO with PDHR
16.	Pressurizer and surge line hydraulics	Affects the pressure control by the pressuriser during early stages of the accident. Potential for CCFL, and overall flow control.	Affects pressure and coolant inventory.	LBLOCA and SBLOCA and SBO
17.	Structural heat	Release of stored heat in the	affects the heat	SBLOCA

	and heat losses	metal structures of the primary system will affect pressure in slower SB LOCAs. Also the heat losses to the environment will contribute to the pressure transient.	removal and depressurization	and SBO, etc.
18.	Phase separation in T junctions and effects on break flow	Phase separation and flow partitioning at branches and T-connections.	Influences mass and energy loss from the system.	LBLOCA, SBLOCA and SBO
19.	Thermal-hydraulics on secondary side of SG	Tube bundle uncovery affects as partial loss of heat sink with primary pressure and temperature increase.	Affect the decay heat removal and depressurization rate of primary system	SBLOCA and SBO and MSLB.
20.	Modes of heat transfer. (conduction, convection, radiation and condensation, etc.)	During accident progression various modes of heat transfer occurs. For example radiation mode of heat transfer contribute significantly in heat removal from fuel/clad when coolant channel is totally voided.	Impact on fuel/clad temperature and accident progression.	LBLOCA plus ECCS failure, SBLOCA and SBO
21.	Fission gas release to gap and internal pressurization	At elevated temperature fuel cracks and lead to release of gas into gap, resulting in internal pressurization.	It has impact on clad strain and its failure behaviour.	LBLOCA, SBLOCA, LORA and SBO
22.	Zircaloy-steam reaction	Zirconium oxidation by steam is an exothermic reaction with significant heat and hydrogen generation at clad temperature more than 800 °C. When fuel clad temperatures rise above approximately 1200°C run away metal steam reaction leads to higher rate of hydrogen generation.	Potential to affect the clad heat up and hydrogen generation.	LBLOCA, SBLOCA, LORA and SBO
23.	Clad deformation and failure	It is a phenomenon which governs the release of fission products from the fuel. A potential clad failure /deformation mechanism is clad strain at high temperature driven by the pressure differential between the internal fission gas pressure and the channel coolant pressure, which reduces rapidly during blowdown.	Release of fission products into primary and containment. It also has impact on coolable geometry	LBLOCA plus LOECCS, SBLOCA, LORA and SBO

24.	The fuel-to-clad heat transfer	It reduces due to fuel clad strain driven by coolant depressurization and contraction of the fuel pellet after reactor trip.	The reduction in fuel-to-clad heat transfer increases the fuel heat-up, which has a corresponding effect on the potential for fuel deformation, clad failure and fission product release.	LBLOCA, SBLOCA, LORA and SBO
25.	Fuel/clad melting and relocation	During the later phase of the accident progression, moderator boil-off leads to uncover of channels and further progression to fuel/clad melting. Stagnation and/or complete flow blockage in channel may also lead to fuel melting	Fission product release and hydrogen.	LOCA plus ECCS failure plus moderator circulation failure, and unmitigated SBO, single channel events, stagnation channel SB LOCA
26	Hydrodynamic transients within the liquid moderator	For limiting single channel events reaction forces including moderator hydrodynamics from the failed channel have the potential to lead to failure of additional channels or to interfere with shutdown. High-temperature channel components (specifically fuel elements and fuel bundle components) can potentially be expelled into the moderator following channel rupture. Fuel-to-moderator interaction (FMI) between the hot (or possibly molten) channel components and the subcooled moderator could produce a significant volume of steam and generate hydrodynamic transients within the liquid moderator. The intensity of the hydrodynamic transient is primarily determined by the rate at which the channel	May lead to additional channel failure.	Pressure tube break, Simultaneous Pressure tube calandria tube break, Stagnation feeder break

		debris is delivered to the moderator water, and the rate of heat transfer from the debris to the moderator. Debris fragmentation influences the surface area available for interaction between the debris and moderator and is also a key factor in the amount of steam generation and the subsequent magnitude of the hydrodynamic transients Failure of both PT and CT as a consequence of initiating event, may lead to rise/oscillations in pressure in various parts of moderator system (adjacent channels, safety and shutdown devices, moderator vessel)		
27.	Hotspot formation	This phenomena is due to bundle mechanical deformation, heat transfer between the clad and the pressure tube, clad-to-coolant and coolant-to-pressure tube, etc.	Hot spot development on the pressure tube lead to, local strain and rupture.	LOCA plus ECCS failure, and SBO
28.	Fuel channel deformation	Fuel channel deformation leading to sagging and/or ballooning contact of PT-CT increases heat transfer from fuel to moderator. If the area of dryout is sufficiently large and the dryout is prolonged on the external surface of CT, the pressure-tube/calandria-tube combination can continue to strain radially and may challenge fuel-channel integrity.	It can affect heat transfer and/or failure of fuel channel.	LBLOCA, SBLOCA, LORA and SBO.

29.	Channel and sub-channel flow effects	Increase in the exterior sub-channel area due to strain in PT would result in a substantial diversion of flow to the exterior of the fuel bundles. On the other hand, diametral straining of the outer element fuel clad would tend to divert some of the flow into the interior sub-channels.	Alter the subsequent thermal and mechanical response of the fuel channel.	NOs and AOOs
30.	Fuel cracking	When the fuel expands/contracts due to rapid heating/cooling, the core of the pellet expands more than the rim or rim contracts more than core. The fuel cracks due to the thermal stress and tend to go from the centre to the edge.	The cracking of the fuel has an effect on the release of radioactivity from fuel.	LBLOCA, and LORA
31.	Gap inventory	The fission gas release from the fuel is retained in the gap and is a function of initial gap inventory (due to power history and burn up) and fuel temperature.	Inventory in the gap is an important factor that limits the total fission product release into the containment	LBLOCA, unmitigated SBO and LORA
32.	Fission product deposition/settling and revaporization/re-suspension including its transport	Fission product compounds may deposit directly on surfaces from the vapour phase, once the appropriate condensation temperature is reached. Revaporization may occur if the surface temperature increases or the gas composition changes significantly. Aerosol deposition in the channel will be dominated by gravitational deposition, turbulent deposition and re-suspension in the turbulent flow	Release of fission product inventory into the containment and its radiological consequence.	LOCA plus LOECCS, unmitigated SBO
33.	Transport of deposits by water	Deposited fission products may be released if liquid water flows over the pipe surface. Liquid flow may occur during flow transients, or during a delayed triggering of the ECC injection. The dissolved or re-suspended fission products will be	Increase in fission product inventory release into the containment and its radiological consequence.	LOCA plus LOECCS

		transported out of the HTS in the break discharge flow.		
34.	Flashing discharge into containment	High enthalpy discharge into the low-pressure containment results in flashing.	This contributes to the pressurization of the containment	LOCA, unmitigated SBO, MSLB
35.	Buoyancy and momentum induced mixing (laminar/turbulent)	Substantial quantities of hydrogen may be released into containment and mixed with the air-steam atmosphere. Forced convection in the containment atmosphere is the dominant mixing mechanism, driven by the local air coolers. Natural convection circulation paths within containment also have a significant impact on mixing behaviour	Improper mixing may result in local flammable mixture in the containment	LOCA plus LOECCS plus LOMD Unmitigated SBO
36.	Hydrogen deflagration and detonation, and transition from deflagration to detonation	A deflagration is characterized by a subsonic flame propagation and relatively modest overpressures. Detonation is characterized by supersonic flame propagation and substantial over pressurization. A transition takes place from deflagration to detonation type for an ignitable mixtures of a flammable gas and oxygen.	Challenges the integrity of the containment	LOCA plus LOECCS plus LOMD Unmitigated SBO
37.	Hydrogen removal by re-combiners	Removal of hydrogen using catalytic oxidation by reacting hydrogen with oxygen at below flammable concentrations	Reduction of hydrogen concentration	LOCA plus LOECCS plus LOMD, Unmitigated SBO
38.	Iodine chemistry in containment	This includes liquid iodine chemistry, species transfer between liquid phase and gas phase, gaseous iodine chemistry and iodine-surfaces interaction, spray interactions, etc.	Total Iodine release from the containment	LOCA plus LOECCS Unmitigated SBO

39.	Fuel clad interactions	Melting of clad and formation of eutectic mixture of uranium oxide and Zircaloy results in a low melting point alloy.	Leads to early melting of fuel and early release of radionuclides.	LOCA plus LOECCS Unmitigated SBO
40.	Cooling by containment structures	Structures absorbs the heat released from discharge to the containment.	Containment depressurization	LOCA, MSLB and Unmitigated SBO
41.	Quenching and rewetting of hot fuel	It involves condensation of steam in the channel and subsequent fuel cooling.	Clad failure and enhanced oxidation.	
42	Vapour pull through and liquid entrainment from stratified header	When Header is stratified during small break LOCA, phenomena of liquid entrainment or vapour pull through occurs through connected feeder depending upon its location with respect to header level.	It affects thermal hydraulic conditions in channel and clad surface temperature.	Small break LOCA.
43	Radiative heat transfer	Radiative heat transfer occurs between fuel elements, fuel element and pressure tube, pressure tube and calandria tube, between fuel element and PT CT contact, calandria tube and moderator depending upon range of temperatures during scenario.	It affects clad surface temperatures, fuel failure and fission product release.	Different limited core damage and severe core damage scenerios.

APPENDIX II

Guidance for AOOs Analysis with Conservative Initial and Boundary Conditions

A limited number of AOOs should be analysed using conservative initial and boundary conditions. For deciding events for such analysis, governing event from each functional category should be selected and this event should be analysed using Option 4, but with conservative input conditions. For arriving at initial conditions, they may be taken as their limiting LCO value given in Station Technical Specifications; in such a way that the selected input maximizes the effect of AOO with respect to the function class in which the event is categorized. Initial conditions of plant parameters, which are also expected to influence the effect of AOOs, should be considered in the conservative direction in order to maximize the functional effect of the AOO. Measurement error and accuracy of the instrumentation should be taken into account to decide conservative boundaries of the parameter. Conservatism in boundary conditions is ensured by taking into account the error band of actuation set-point of the control system. In case of lack of clarity of conservative side of any input parameter, due to counteracting effects, nominal value may be used. To ensure conservatism in boundary conditions, errors considering instrument accuracy for set point of different automated actuation logic (e.g. setback, reactor trip) should be accounted. A typical list of Category-2 events analysed as AOOs, indicating the event functional category, governing PIE, Rationale for conservative direction of initial and boundary conditions are given below in Table II.1

Table II.1 Rationale for Conservative Direction of Initial and Boundary Conditions

S. N.	Event category	PIEs analysed and Governing Event	Rationale for Conservative Direction of Initial and Boundary	Examples of Initial Conditions and their Conservative Directions
1	Reactivity and Power Distribution Anomalies	-Single ZCC draining -Slow Loss of regulation transient (LORT)	To maximise rate of power rise	-Reactor thermal power 103%-higher enthalpy coolant -Core flow lower bound-higher enthalpy coolant
2	Decrease in PHT System Inventory	-One IRV stuck open -Both bleed CVs suck open and feed CVs stuck closed -Both PSBVs stuck open	To minimise initial system inventory and higher discharge rate	-Reactor thermal power 103%- higher enthalpy coolant -Pressuriser level lower bound-lesser inventory -Core flow lower bound-higher enthalpy coolant
3	Increase in PHT System Inventory	-Both feed CVs suck open and bleed CVs stuck closed	To maximise system inventory	-Reactor thermal power 103%- higher enthalpy coolant -PHT pressure upper

				bound- higher peak pressure -Pressuriser level upper bound- Higher inventory
4	Increase in Heat Removal by Secondary System	-All SG large feed water CVs stuck open -Feed water HP heater bypass	To maximise heat removal from primary system	-Reactor thermal power 103%- higher enthalpy coolant -Core flow lower bound- higher enthalpy coolant -SG pressure lower bound- higher heat removal
5	Decrease in Heat Removal by Secondary System	-Turbine trip -Gross load rejection -Net load rejection	To maximise decrease in heat removal.	-Reactor thermal power 103%- higher heat generation -PHT pressure higher bound- higher peak pressure -Pressuriser level higher bound-higher inventory -SG pressure higher bound- higher peak pressure
6	Decrease in PHT System Flow Rate	-All PCPs trip -PPP trip and standby PPP fails to resume -Credible flow blockage in any reactor coolant channel assembly -Class-IV power supply failure	To maximise power to flow ratio	-Reactor thermal power 103%- higher enthalpy coolant -Core flow lower bound- higher enthalpy coolant

REFERENCES

[1] AERB Code of Practice on Nuclear Power Plant Design, AERB Safety Code No. AERB/SC/D, Rev.1, 2009.

[2] AERB Safety Code on Nuclear Power Plant Operation, AERB/NPP/SC-O, Rev.1, 2008.

[3] AERB Code of Practice on Nuclear Power Plant, Design of Light Water Reactor Based Nuclear Power Plants, AERB Safety Code AERB/NPP-LWR/SC/D, 2015.

[4] IAEA Safety Standards on Safety of Nuclear Power Plants: Design Nuclear Power Plants: Design, Specific Safety Requirements, IAEA, SSR-2/1 (Rev. 1), 2016.

[5] AERB Design Safety Guide, Design Basis Events for Pressurized Heavy Water Reactors AERB/SG/D-5, 2000 and Rev.1 (at final stage).

[6] USNRC, Transient and Accident Analyses, Combined License Applications for Nuclear Power Plant (LWR edition), Regulatory Guide 1.206, 2007.

[7] AERB Safety Code on Site Evaluation of Nuclear Facilities, No. AERB/NF/SC/S, Rev.1, 2014.

[8] AERB Design Safety Guide, on Fuel Design for Pressurised Heavy Water Reactors, AERB/SG/D-6, 2003.

[9] AERB Design Safety Guide, Primary Heat Transport System for Pressurised Heavy Water Reactors, AERB/NPP-PHWR/SG/D-8, 2003.

[10] AERB Design Safety Guide, Loss of Coolant Accident Analysis for Pressurised Heavy Water Reactor, AERB/DG/D-18, 2001

[11] Canadian Regulatory Document, Safety Analysis, Deterministic Safety Analysis, REGDOC 2.4.1, 2014.

[12] AERB Safety Manual on Hydrogen Release and Mitigation Measures Under Accident Conditions in Pressurised Heavy Water Reactors, AERB/NPP-PHWR/SM/D-2, 2017

[13] IAEA Safety Standard Series on Format and Content of the Safety Analysis Report for Nuclear Power Plants, Safety Guide, IAEA-GS-G-4.1, 2004.

[14] IAEA Safety Standard Series on Safety Assessment and Verification of Nuclear Power Plants, IAEA Safety Guide, NS-G-1.2, 2001.

[15] IAEA Safety Report Series on Accident Analysis for NPPs, IAEA SRS-23, 2002.

[16] IAEA Safety Standards, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide, SSG-2, Rev.1 (Draft), 2016.

[17] IAEA Safety Report Series on Accident Analysis for Nuclear Power Plants with Pressurized Heavy Water Reactors, IAEA SRS-29, 2003.

[18] NEA CSNI Report on Validation Matrix for the Assessment of Thermal-Hydraulic Codes for VVER LOCA and Transients, Nuclear Energy Agency Committee on the Safety of Nuclear Installations, Organisation for Economic Co-operation and Development, NEA/CSNI/R(2001)4, 2001.

[19] E.O. Moeck, J.C. Luxat, M.A. Petrilli and P.D. Thompson, Status of Validation Matrixes for CANDU Power Plants, 18th Annual Conferences of Canadian Nuclear Society, Toronto, Ontario, Canada, June 08-11, 1997.

[20] AERB Design Safety Guide, Safety Systems for Pressurised Heavy Water Reactors, AERB/SG/D-10, 2005

[21] ASNI/ANS-58.8, American Nuclear Society, Time Response Design Criteria for Safety Related Operator Actions, 1994.

[22] IAEA Safety Report Series on Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation, IAEA SRS-52, 2008.
[23] AERB Regulatory Guide, Format and Content of the Safety Analysis Report, AERB/SG/G-9, 2018
[24] AERB Design Safety Guide, Radiation Protection Aspects in Design for Pressurised Heavy Water Reactor Based Nuclear Power Plants, AERB/SG/D-12, 2005.
[25] AERB Design Safety Manual on Methodology Radiological Impact Assessment for NPPs, AERB/SM
[26] IAEA TECDOC on Analysis of Severe Accidents in Pressurized Heavy Water Reactors, IAEA TECDOC-1594, 2008.
[27] AERB Design Safety Guide, Accident Management Programme for Water Cooled Nuclear Power Plants, AERB/SG/D-26

LIST OF PARTICIPANTS
WORKING GROUP

Dates of meeting: June 8, 2008
November 10, 2009
December 15, 2009
September 20, 2011
September 24, 2012
October 21, 2014
October 28, 2014
November 3, 2014
November 19, 2014
November 27, 2014
December 04, 2014
January 05, 2016
March 11, 2016
May 11, 2016
July 01, 2016
August 04, 2016
February 03, 2017
May 23, 2017
April 24, 2018
May 07, 2018

Members of the Working Group:

Shri H.G. Lele (Convener) (partly)	Ex. Head, CSSS, RSD, BARC
Shri S.G. Ghadge, (Convener) (partly)	Director (Technical), NPCIL
Shri S.S. Bajaj (Convener) (partly)	Ex. Sr. Executive Director, Safety, NPCIL
Dr. H.P. Gupta	Th.PD, BARC
Dr. A.K. Nayak	RED, BARC
Shri Ashok Chauhan	NPCIL
Shri H.P. Rammohan	RSA, NPCIL
Dr. K. Velusamy	THS, IGCAR
Shri J. Koley	OPSD, AERB
Shri S. C. Utkarsh	NPSD, BARC
Dr. R.S. Rao	NSAD, AERB
Dr. S.K. Dubey (Member-Secretary)	DRP&E, AERB
Shri Manoj Kansal (invitee)	RSA, NPCIL
Shri S.Hajela (invitee)	RSA, NPCIL
Shri T.A.Khan (invitee)	RSA, NPCIL
Shri S.Pahari (invitee)	RSA, NPCIL
Dr. S.P. Lakshmanan (invitee)	NSAD, AERB
Shri Pranav Paliwal (invitee)	NSAD, AERB)

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

Dates of meeting: June 04, 2015
June 25, 2015
July 01, 2015
August 18, 2015

Shri K.K. Vaze	…	Chairman
Dr. P.K. Vijayan	…	Member
Shri S.G. Ghadge	…	Member
Dr. P. Chellapandi	…	Member
Shri Y.S. Mayya	…	Member
Shri A.J. Gaikwad	…	Member
Shri K. Srivasista	…	Member
Shri S.K. Ghosh	…	Member
Shri P. Bansal	…	Member
Shri G.M. Behra	…	Member-Secretary

ADVISORY COMMITTEE FOR NUCLEAR AND RADIATION SAFETY (ACNRS)

Dates of meeting: February 04, 2017
March 04, 2017
June 03, 2017

Shri S.S.Bajaj	Chairman
Dr. M.R.Iyer	Member
Prof. C.V.R.Murty	Member
Shri H.S.Kushwaha	Member
Shri S.C.Chetal	Member
Shri A.R.Sundararajan	Member
Shri S.K.Ghosh	Member
Shri K.K.Vaze	Member
Dr. N.Ramamoorthy	Member
Shri V.Rajan Babu	Member
Shri K.Srivasista	Permanent-Invitee (Partly)
Shri R.B.Solanki	Permanent-Invitee
Shri Parikshat Bansal	Permanent-Invitee
Shri S.T.Swamy	Member-Secretary