AERB SAFETY GUIDE NO. AERB/NPP&RR/SG/G-10

REGULATORY REVIEW OF LEVEL-1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS AND RESEARCH REACTORS

Atomic Energy Regulatory Board
Mumbai - 400 094
India

August 2015

Price:

Order for this ‘Safety Guide’ should be addressed to:

The Chief Administrative Officer
Atomic Energy Regulatory Board
Niyamak Bhavan
Anushakti Nagar
Mumbai-400 094
India

FOREWORD

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

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

This safety guide outlines standard review methodology for Level-1 PSA. It also provides consistent technical approaches on aspects of PSA and guidance for preparation of the review report. Review aspects related to PSA Level-2 and PSA Level-3 are not addressed in this safety guide. In drafting this guide, extensive use has been made of the information contained in the relevant documents of the International Atomic Energy Agency (IAEA) and other PSA standards and good practices.

Consistent with the accepted practice, ‘shall’ and ‘should’ are used in the safety guide to distinguish between a recommendation and a desirable option respectively. An Annexure and bibliography are included to provide further information on the subject that might be helpful to the user(s).

The initial draft of the guide has been prepared in-house and subsequently reviewed and revised by the AERB committee on PSA for nuclear facilities. Experts have reviewed the Guide and the relevant Advisory Committee on preparation of Codes and Guides on Governmental Organisation for Regulation of Nuclear and Radiation Facilities vetted it before issue.

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

(S. S. Bajaj)
Chairman, AERB

DEFINITIONS

Acceptance Criteria
The standard or acceptable value against which the value of a functional or condition indicator is used to assess the ability of a system, structure or component to perform its design function or compliance with stipulated requirements.

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

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

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

Active Maintenance Time
That part of the maintenance time during which a maintenance action is performed on an entity, either automatically or manually, excluding logistic delays.

Ageing

General process in which characteristics of structures, systems or components gradually change with time or use although the term ‘ageing’ is defined in a neutral sense – the changes involved in ageing may have no effect on protection or safety, or could even have a beneficial effect - it is commonly used with a connotation of changes that are (or could be) detrimental to protection or safety, i.e. as a synonym of ‘ageing degradation’

Anomaly
Deviations from normal which could be due to equipment failure, human error or procedural inadequacies but do not pose a risk which may exceed authorised operational limits and conditions.

Anticipated Operational Occurrence (AOO)
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.

Availability
The fraction of time in which an entity is capable of performing its intended purpose.

Basic Event
An event in a logic model, which represents the state in which a component or a group of components is unavailable. Generally, basic events are component failures, operator errors, adverse environmental conditions, etc. However, they can also relate to operation, maintenance, etc.

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

Beyond Design Basis Events (BDBE)
Events of very low probability of occurrence, which can lead to severe accidents and are not considered as design basis events.

Catastrophic Event
Any event, which could potentially cause the loss of primary system function(s) resulting in significant damage to the system or its environment and/or cause the loss of life or limb.

Cause-Consequence Diagram (CCD)
A logic diagram showing the causes and consequences of an initiating event.

Common Cause Failure (CCF)
The failure of a number of devices or components to perform their functions, as a result of a single specific event or cause.

Common Mode Failure (CMF)
Failure of two or more structures, systems or components in the same manner or mode due to a single event or cause. It is a type of common cause failure.

Component
The smallest part of a system necessary and sufficient to consider for system analysis.

Computational Model
A simplified description of a complex entity or process in terms of a collection of procedures and data suitable for calculation.

Conceptual Model
A set of qualitative assumptions used to describe a system (or part thereof).

Consequence Tree
A logic diagram showing the consequences of an initiating event.

Core Damage
Reactor state brought about by the accident conditions with loss of core geometry or resulting in crossing of design basis limits or acceptance criteria limits for one or more parameters. (The parameters to be considered include: fuel clad strain, fuel clad temperature, primary and secondary systems pressures, fuel enthalpy, clad oxidation, % of fuel failure, H_2 generation from metal-water reaction, radiation dose, time required for operator to take emergency mitigatory action).

Corrective Maintenance
The maintenance carried out after fault recognition to put an entity into a state in which it can perform a required function.

Critical Component
Component, whose failure, in a given operating state of the system, results in the system failure.

Critical Event
Any event, which could potentially cause the loss of the primary system function(s) resulting in significant damage to the said system or its environment (and negligible hazard to life or limb).

Criticality Analysis
Analysis for evaluating the likelihood and severity of the failure.

Cut Set
A combination of basic events resulting in an undesirable event.

Deductive Approach
The approach, where the line of reasoning goes down from the most general to the most specific.

Defects
Any deviation from the pre-defined acceptable limits, or any non-conformance with the stated requirements.

Degraded State
The state in which an entity exhibits reduced performance but insufficient degradation to declare the entity unavailable, according to the specified success criterion. (Examples of degraded states are relief valves opening prematurely outside the technical specification limits with less than 100 % flow but within a safety margin).

Dependent Failures
Interdependent, simultaneous or concomitant failures of multiple entities.

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

Design Basis Events (DBEs)
The set of events, that serve as part of the basis for the establishment of design requirements for systems, structures and components within a facility. Design basis events (DBEs) include operational transients and certain accident conditions under postulated initiating events (PIEs) considered in the design of the facility (see also “Design Basis Accidents”).

Deterministic Analysis
Analysis using, for key parameters, single numerical values (taken to have probability of 1), leading to a single value of the result.

Direct Cause
The latent weakness, which allows or causes the observed cause of an initiating event to happen, including the reasons for the latent weakness.

Dual Failure
A normal operating system failure with simultaneous unavailability of a safety system or any other system.

Earthquake
Vibration of earth caused by the passage of seismic waves radiating from the source of elastic energy.

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

Entity

It refers to a structure, system or component and in specific case may include humans.

Error of Omission

An error that amounts to omitting a part or entire task.

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

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

Failure Mode
The effect by which a failure is observed.

Failure Modes and Effects Analysis (FMEA)
A qualitative method of system analysis, which involves the study of the failure modes that can exist in every component of the system and the determination of the causes and effects of each failure mode.

Failure Modes, Effects and Criticality Analysis (FMECA)
A qualitative method of system analysis, which involves a failure mode and effects analysis together with a criticality analysis.

Fault Tolerance
The attribute of an entity that makes it able to perform a required function in the presence of certain given sub-entity faults.

Frontline Systems
The systems that directly perform a safety function are termed frontline systems.

Hazard
Situation or source, which is potentially dangerous for human, society and/or the environment.

Human Behaviour
The performance, i.e. action or response of human operator to occurrence of event(s).

Human Reliability
The probability that an human operator will perform a required mission under given conditions in a given time interval.

Human Reliability Assessment/Analysis
Assessment concentrating on the human errors liable to be committed by the operator having a mission to fulfil on a system.

Incident
Events that are distinguished from accidents in terms of being less severe. The incident, although not directly or immediately affecting plant safety, has the potential of leading to accident conditions with further failure of safety system(s).

Incipient
The component is in a condition that, if left un-remedied, could manifest propagation of degradation or flaw, ultimately leading to a failure or unavailable state.

Inductive Approach
The approach in which the line of reasoning goes from the most specific to the following sequences resulting into condition or end state of concern.

Initiating Event/Initiator
An identified event that leads to anticipated operational occurrences or accident conditions and challenges safety functions.

In-service Inspection (ISI)
Inspection of structures, systems and components carried out at stipulated intervals during the service life of the plant.

Level 1 PSA (Nuclear Reactor)
It evaluates core damage frequency by developing and quantifying accident sequence (event trees) with postulated initiating events together with system unavailability values derived from fault tree analyses with inputs from failure data on components, common causes and human actions.

Level 2 PSA (Nuclear Reactor)
It takes inputs from Level 1 PSA results and quantifies the magnitude and frequency of radioactive release to the environment following core damage progression and containment failure.

Level 3 PSA (Nuclear Reactor)
Taking inputs from Level 2 analysis, it evaluates frequency and magnitude of radiological consequences to the public, environment and the society considering meteorological conditions, topography, demographic data, radiological release and dispersion models.

Living PSA
A PSA which is updated to reflect the current design and operational features, and is documented in such a way that each aspect of the PSA model can be directly related to existing plant information, plant documentation or the analysts' assumptions in the absence of such information.

Logistic Delay
The accumulated time during which a desired action cannot be performed due to the necessity to acquire required resources, excluding administrative delay. Logistic delays can be due to maintenance activity, travelling to unattended installations, pending arrival of spare parts, specialists, test equipment, information and suitable environmental conditions.

Man Machine Interface (MMI)
The abstract boundary between people and the hardware or software they interact with.

Maintenance
Organised activities covering all preventive and remedial measures, both administrative and technical, to ensure that all structures, systems and components are capable of performing as intended for safe operation of the plant.

Mathematical Model
A set of mathematical equations designed to represent a conceptual model.

Mean Down Time (MDT)
The expectation value of the down time.

Mean Time Between Failures (MTBF)
The expected operating time between two failures.

Mean Time to Failure (MTTF)
The expected operating time to first failure. The MTTF is also called MTTFF (mean time to first failure).

Mean Time to Repair (MTTR)
The expectation of the time to restoration (or to repair).

Minimal Cut Set
Combination of a minimum number of events such that, if one of the events in a minimal cut set does not occur, then the undesirable event will not happen.

Mission Time
Duration/period for which the operation of the system must be ensured.

Model
An analytical representation or quantification of a real system and the ways in which phenomena occur within that system, used to predict or assess the behaviour of the real system under specified (often hypothetical) conditions.

Observed Cause
The failure, action, omission or condition, which directly leads to an initiating event.

Operating State
The state when an entity performs a required function.

Partial Failure
A failure which results in the inability of an entity to perform some, but not all, required functions.

Passive Component
A component which has no moving part and only experiences a change in process parameters such as pressure, temperature, or fluid flow in performing its functions. In addition, certain components, which function with very high reliability, based on irreversible action or change, may be assigned to this category (examples of passive components are heat exchangers, pipes, vessels, electrical cables, and structures. Certain components, such as rupture discs, check valves, injectors and some solid-state electronic devices have characteristics, which require special consideration before designation as an active or passive component).

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

Predictive Maintenance
Form of preventive maintenance performed continuously or at intervals governed by observed condition to monitor, diagnose or trend a structure, system or component's condition indicators; results indicate current and future functional ability or the nature of and schedule for planned maintenance. It is also known as condition based maintenance.

Preliminary Hazard Analysis
Analysis for identifying and assessing the (economic, human, etc.) hazards inherent in using a system and which is carried out before using other more precise methods of analysis.

Preventive Maintenance
Maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of an entity.

Probabilistic Risk Assessment (PRA)/ Probabilistic Safety Assessment (PSA)
Study aimed at evaluating the risks of a system using a probabilistic method. A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual

and a mathematical tool for deriving numerical estimates of risk . The term PRA and PSA are interchangeably used.

Plant Damage States
Accident sequences, obtained from Level 1 PSA analysis, that have similar effects on containment response and fission product source terms are grouped into one state, called plant damage state, for further analysis.

Quality
The totality of features and characteristics of an item or service that have the ability to satisfy stated or implied needs.

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

Random Process
Set of time-dependent random variables whose values are governed by a given set of multidimensional distributions, which correspond to all the combinations of the random variables.

Random Variable
Variable which can take any one of a given set of values, each with an associated distribution.

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

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

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

Risk Based Approach
Approach in which the decision making is solely based on the numerical result of the risk assessment judging against the probabilistic safety criteria set or established.

Risk Informed Approach

An approach to decision making that represents a philosophy whereby risk insights derived from risk assessment, by comparison of the results with the probabilistic safety goals, are considered together with other information obtained from deterministic safety analysis, engineering judgment and experience.

Risk Monitor
A plant specific real-time tool used to determine the instantaneous risk based on the actual states of the systems and components. At any given time, the risk monitor reflects the current plant configuration in terms of status of various systems and/or components, e.g. whether a component is out of service for maintenance or tests. The model used by the risk monitor is based on and is consistent with living PSA for the facility.

Root Cause
The fundamental cause of an event, which, if corrected, will prevent its recurrence, i.e. the failure to detect and correct the relevant latent weakness(es) (undetected degradation of an element of a safety layer) and the reasons for the failure.

Safety (Nuclear)
The achievement of proper operating conditions, prevention of accident or mitigation of accident consequences, reliability in protection of site personnel, the public and the environment from undue radiation hazards.

Safety Systems
System 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).

Scheduled Maintenance
The preventive maintenance carried out in accordance with an established time schedule.

Seismic Hazard
Any physical phenomenon (e.g. ground vibration, ground failure) associated with an earthquake that may produce adverse effects.

Sensitivity Analysis
A quantitative examination of how the behaviour of a system varies with change, usually in the values of governing parameters.

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

Significant Event
Any event, which degrades system performance function(s) without appreciable damage to either the system or life or limb.

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.

Station Blackout (SBO)
The complete loss of both off-site and on-site AC power supplies.

Stochastic Analysis
Often taken to be synonymous with probabilistic analysis. Strictly speaking, stochastic conveys directly the idea of randomness, whereas probabilistic is directly related to probabilities and hence, only indirectly concerned with randomness. Therefore, a natural event or process might more correctly be described as stochastic, whereas probabilistic would be more appropriate for describing a mathematical analysis of stochastic events or processes and their consequences (such an analysis, would strictly be stochastic if the analytical method itself included an element of randomness, e.g. Monte Carlo analysis).

Support Systems
The systems those are required for proper functioning of the frontline systems.

System Logic Model
A model that identifies the combinations of component states that lead to undesired system states.

Test
An experiment carried out in order to measure, quantify or classify a characteristic or a property of an entity.

Unavailability
The inability of an entity to be in a state to perform a required function under given conditions at a given point of time. It is measured as the probability (relative frequency) that the entity is in an unavailable state at a point of time.

Uncertainty Analysis
An analysis to estimate the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem.

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 software development process to ensure compliance with the user requirements. Validation is therefore ‘end-to-end verification’.

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

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

SPECIAL DEFINITIONS

(Specific for the Present 'Safety Guide')

Accident Sequence
Sequence of events leading to an accident.

Down Time
The time interval during which structures, systems and components (SSC) are not available for performing intended function.

Gradual Failure
A failure due to gradual change of a given characteristics of structures, systems and components (SSC) with respect to time.

Human Error
The departure of a human performance from what it should, and which may affect, structures, systems and components (SSC) availability, causes an initiating event or inadequate response to an initiating event.

Hypothetical Accident
It is generally a beyond design basis accident condition, categorized by probability of occurrence less than 1.0E-07 per reactor year.

Maintenance Time
The time interval during which a maintenance action is performed on structures, systems and components (SSC) including technical delays and logistic delays.

System
Given set of discrete elements (or components) which are interconnected or are interacting.

CONTENTS

1. INTRODUCTION

1.1 General

Atomic Energy Regulatory Board (AERB) has licensed nuclear facilities with traditional deterministic methods by applying criteria such as compliance with single failure, defense in depth, adequate safety margin etc. However, recognising the benefits of the Probabilistic Safety Assessment (PSA), AERB in its revised safety code titled 'Nuclear Power Plant Operation' AERB/SC/O (Rev. 1) made the performance of Level-1 PSA (internal events, full power) for all nuclear power plants as a mandatory requirement. The safety code on 'Design of Pressurised Heavy Water Reactor based Nuclear Power Plants' AERB/NPP-PHWR/SC/D (Rev.1) also specifies the requirement.

A probabilistic safety assessment (PSA) of a nuclear power plant (NPP) provides a comprehensive and structured approach for identifying failure scenarios and deriving numerical estimates of the risks to workers and members of the public. PSA are normally performed at three levels as follows:

(a) Level 1 PSA, which identifies the sequences of events that can lead to core damage, estimates core damage frequency and provides insights into the strengths and weaknesses of the safety systems and procedures provided to prevent core damage.
(b) Level 2 PSA, which identifies the ways in which radioactive releases from plants can occur and estimates their magnitudes and frequencies. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures such as reactor containment.
(c) Level 3 PSA, which estimates public health and other societal risks such as contamination of land or food.

PSA provides a systematic approach to determine whether safety systems are adequate, the plant design balanced, and the defense in depth requirement have been realised. These are characteristics of the probabilistic approach.

Despite benefits of PSA, there are certain limitations of PSA which are arising from:

(a) difficulty in ensuring completeness of initiating event identification,
(b) unavailability of adequate plant component failure data,
(c) difficulties in modeling and quantification of human errors,
(d) difficulties in modeling and quantification of common mode/cause failures and uncertainties associated with models and analysis steps. The regulatory decision-making should be based on the understanding of these uncertainties.

In view of these, a regulatory review of PSA became a necessary step before the PSA results are used in the decision-making. The AERB safety manual titled 'Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors', AERB/NPP&RR/SM/O-1, was issued in March 2008. This document covers the PSA review aspects, which were based on erstwhile IAEA guidelines and other PSA related literature. PSA studies are performed by different organisations and there exists wide variation in methods, models and assumptions used in the PSA. This

safety document for is prepared for standard review approach, timely and efficient review. The formats for PSA report are elaborated in AERB/NPP/SG/G-9 titled 'Standard Format and Contents of Safety Analysis Report for Nuclear Power Plants'.

1.2 Objectives

The objectives of this document are:

(i) To provide guidance for review of Level-1 PSA
(ii) To develop consistent approach and technical guidance on certain aspects of PSA
(iii) To provide guidance on the preparation of the review report.

1.3 Scope

This document is applicable for review of Level-1 PSA for nuclear power plants and research reactors and covers both internal and external events. The guidance for regulatory review of PSA applications such as optimization of Technical Specifications, design modifications etc. is beyond the scope of this document.

2. REGULATORY REVIEW

2.1 General

The decision making process uses Level 1 PSA to assess the level of safety of nuclear power plants and research reactors. For this purpose the PSA methodology should be well developed for results to be used in the regulatory decision making process.

The review process provides a degree of assurance of the objective, scope, validity and limitations of the PSA, as well as better understanding of the plant itself in risk informed decision making. The review approach is expected to differ depending on the purpose of the review. For example, the review carried out on the PSA for a new reactor design may differ from that for an existing reactor, carried out as a part of a periodic safety review.

2.2 PSA Review Team

The review team should be comprised of specialists in the fields such as PSA, system analysis, safety review, nuclear power plant and research reactor operation, severe accident phenomena, external events and structural engineering. The team may invite experts to support the review, if the need arises.

2.3 Review process

The objective of the regulatory review of the PSA is to assess whether important technological and methodological issues in PSA are treated adequately. The detailed review should focus on the models and the data used in PSA and it should be ensured that they are representations of the actual design and operation of the nuclear power plant and research reactors. It provides confidence in the PSA and reduces effort required for reviewing the PSA applications. The adequacy of the information in PSA submittal is checked during the review. Appropriate methods, models, assumptions and data used in PSA should be checked in the review process in order to have confidence in the PSA results. Independent peer review of PSA should be carried out and comments of the peer review, responses and action taken reports should be submitted by utility. AERB may decide to optimise the extent of the review based on peer review report and relevant documents.

It is considered a good practice that the reviewers obtain and use the electronic version of the PSA model rather than rely on paper copies of the fault trees and event trees for efficient and effective review. This would enable the reviewers to:

(i) search for specific information in the model,
(ii) perform spot checks on the model and its quantification, and
(iii) carry out independent sensitivity studies to determine how changes in assumptions can affect the results of the PSA

During the review of PSA, methods used for similar plants should be compared. The reworking of particular parts of PSA or carrying out independent calculations to aid in the understanding of PSA can also be considered during review. The findings of the

review should be documented in PSA review report. The contents of the review report are described in Section 4.0

The review is intended to verify that the modeling approach is correct and that the methodology reflects the current state-of-the-art in the PSA. A detailed review of specific areas should be undertaken. One of the important aspects of this review is to check the adequacy of the PSA models against the technical requirements of PSA standards. The guidance for review is provided in Section 3.0. In addition to all information sources, PSA software, in which the model was developed, should also be made available, to the extent possible/feasible for the review of PSA reports.

The review of PSA reports follows a systematic flow. Normally utility submits PSA reports to relevant AERB committees. AERB committees forward the reports to PSA committee for review. PSA committee should review the documents and give recommendations. All these recommendations should be complied by utility and compliance report should be submitted to PSA committee. The PSA committee should review the compliance and gives final report to AERB committee. The flow chart for review of PSA level-1 reports is elaborated in Annexure-1.

3. TECHNICAL ELEMENTS AND ADEQUACY THEREOF FOR REVIEW

3.1 General

The important elements of review of Level-1 PSA analysis comprise the following:

(a) Review of Level-1 PSA (internal events, full power)
(b) Review of Level-1 PSA (Low power and shutdown conditions)
(c) Review of Level-1 PSA (External events)
(d) Quantification of the analysis
(e) Quality assurance in PSA

Each element of Level-1 PSA should be reviewed in detail. The review should demonstrate that the modeling approach is correct and that the methodology reflects the current state-of-the-art in the PSA. A detailed review of specific areas needs to be undertaken. Compliance with requirements of AERB safety codes mainly 'AERB/NPP/SC/O (Rev.1)' and 'AERB/NPP-PHWR/SC/D (Rev.1)', 'AERB/NPP-LWR/SC/D' with respect to Level-1 PSA should be checked during the review.

In order to standardize the review, guidance needs to developed, which can be readily used during the review. Keeping this in view, the following review guidance is given based on the survey of available literature, good practices, PSA standards and review guidelines prepared for IAEA International peer review services (IPERS).

3.2 Review of Level-1 PSA (Internal Events, Full Power)

The following important technical elements should be considered while carrying out the review.

(i) Initiating Event (IE) analysis
(ii) Success criteria (SC)
(iii) Accident sequence (AS) analysis
(iv) System analysis (SY)
(v) Human reliability analysis (HRA)
(vi) Data analysis (DA)
(vii) Analysis of passive systems, components and structures
(viii) Uncertainty, sensitivity and importance analysis
(ix) Audit of utilities PSA procedure.

3.2.1 Initiating Event Analysis

(a) Selection and identification of Initiating Events (IE)

(i) The review should verify that a systematic procedure has been used to identify the set of IE. The reviewers should verify that the set of IE (e.g. list of IE given in safety guide on design basis events for pressurised heavy water reactor, AERB/SG/D-5(PHWR)) identified is as complete as possible, within the scope decided for the PSA. It is recognized that it is not possible to demonstrate completeness,

however, by using a combination of the methods for identifying IE, it is possible to gain confidence that the contribution to the risk from IE, which have not been identified would be small.

(ii) The review should check for any design features which are novel or plant specific and whether they are potential sources of new IE.

(iii) In the case of twin or multiple unit sites where some safety systems may be shared or cross-tied, the review should verify that those IE that can affect both units (for example, loss of grid and most external events) have been identified and the PSA takes account of the shared systems that are required by both/all of the units (instead of being fully available for one unit).

(iv) Review of the operating experience of the nuclear power plant and research reactor (if it is already operating) and of similar nuclear power plants and research reactors to ensure that any IE that have actually occurred are included in the set of IE addressed in the PSA. The review should consider previous PSA if any and operational experience feedback/significant event reports etc. while reviewing PSA.

(v) Review should verify the criteria that were used to screen out very low frequency events.

(vi) The set of initiating events identified should include partial failures of equipment since it is possible that they could make a significant contribution to the risk.

(b) Grouping of IE

(i) The review should verify that only IE resulting in similar accident progression and with similar success criteria for the mitigating systems have been grouped together. The success criteria used for that specific group should be the most stringent criteria of all the individual events within the group. The loss of coolant accidents (LOCA) identified are usually categorized and grouped according to the success criteria of the safety systems that must be operated to prevent or limit core damage. For LOCA in the reactor coolant system piping, the reviewers should pay particular attention to the locations of the break, since this can influence the success criteria for the required safety systems.

(ii) The success criteria for the LOCA groups should be supported by analysis and take account of equipment failures that could occur as a consequence of the break or the harsh environment generated by the LOCA.

(iii) Interfacing systems, LOCA and steam generator tube ruptures are usually grouped separately since the primary coolant leakage from the SG tube rupture bypasses the containment and hence is not available for re-circulation from the containment sump.

(iv) PSA studies have shown that station blackout has made a significant contribution to risk for a number of plants. Loss of grid/external AC power is an important IE and it is necessary for the review to pay particular attention to this event when it is followed by loss of all on-site AC power in the event sequence.

(v) The frequency of loss of grid should be specified as a (usually stepwise) function of the duration of the loss. The review should verify

that the derivation of this frequency/duration function is clearly documented, based on records of grid loss in the area and taking account of any site specific factors such as redundancy of grid lines or susceptibility to storm damage.

(vi) The review should make a comparison of the finalized initiator groups and frequencies with other similar studies.

(c) Estimation of IE frequencies

(i) The review should verify whether the adequate plant-specific data are available to characterize the parameter value and its uncertainty. If it is found that 'adequate' data are not available, the reviewers should verify that the IE frequencies are estimated accounting for relevant generic and plant-specific data.

(ii) The review should also verify that while using the plant-specific data, the most recent applicable data are considered in frequency estimation. The justifications provided for excluding certain data points also should be reviewed.

(iii) The review should verify that while combining evidence from generic and plant-specific data, Bayesian update process or equivalent statistical process is used.

(iv) There are many systems in nuclear power plants wherein parts, trains or components of the system are in on-line mode and redundant parts, trains or components are in standby mode. For example, a three train compressed air system is usually operated with one train in operation, a second train as a first backup and the third train as a second backup. The order of the trains is rotated after one month of operation in this mode. The first train is stopped and replaced by the second train. Thus the former second train becomes now the train in operation and the former third train first backup. Usually some preventive maintenance is made at the formerly operating train, now in second backup. The review should confirm whether a reasonable reliability model is used to depict such system including consideration of specific operation modes, scheduled and unscheduled maintenance. If system fault trees from the sequence analysis are used to estimate IE frequencies, it should be checked whether the necessary modifications and extensions have been made in a correct and consistent way.

(v) The review should verify that the IE analysis is documented in a manner that facilitates PSA applications, upgrades, and peer review. The documentation typically includes:

- Initial IE list
- Basis for screening out the IE from further considerations
- IE grouping criteria
- Final IE list
- Procedure for estimation of IE frequencies
- Key modeling assumptions.

3.2.2 Accident Sequence Analysis

(a) The plant response to the initiating events identifies the event sequences that could occur leading either to a safe state, where the reactor is shut down and the residual heat is being removed, or to core damage. The important safety functions and associated safety systems should be identified along with important human actions, if any. The dependencies among the front line systems and support system should also be identified in this task. The review should verify that the event tree analysis for each of the initiating event groups addresses all the safety functions that need to be performed and the operation of the safety systems required as identified by the success criteria. Event tree analyses cover all possible combinations of success or failure of the safety systems in responding to an initiating event and identify all the sequences leading either to a successful outcome, where a sufficient number of the safety systems have operated correctly, or to core damage.

(b) If one event tree is used to model several initiating event groups, the review should verify that this event tree does indeed envelope all sequences which can evolve from the different initiating event groups and that this grouping does not introduce excessive conservatism.

(c) Where operator actions are modelled in the event tree analysis, the review should make certain that the procedures for the initiating event have been produced (or will be produced for a plant being designed) and cover the event sequence being addressed. In addition, the timing required for operator actions should be determined based on plant specific best estimate thermal-hydraulic analyses and this should be reflected in the event trees.

(d) The review should verify that the personnel who prepared the event trees have communicated with the personnel who participated in the systems analyses, human reliability analyses and sequence quantifications in the development of the event trees.

(e) In the case, different system success requirements in the event trees are modelled by means of house events in the system fault trees, the house event descriptions should be reviewed and the interfaces with the respective event trees checked.

(f) If the time frames are derived from thermal hydraulic analyses, then the details should be available for review. If expert judgment is used to estimate available time frames, the basis for the judgment should be checked. The review should verify that personnel from the operation section of the plant have taken part in the estimation process.

(g) The review should verify that the way the end states have been defined and grouped is consistent with what has been done in previous PSA for similar plants.

(h) The review should verify that the AS analysis is documented in a manner that facilitates PSA applications, upgrades, and peer review. The documentation should typically include:

– Event trees

- Description of the accident scenarios
- Important human actions
- Front-line system and support system dependency matrix
- List of house events with event description
- Key modeling assumptions

3.2.3 Success Criteria (SC)

(a) The review should verify that core damage criteria have been developed. This is often done by adopting indirect criteria where core damage is assumed to occur following prolonged core exposure to the top of the core or over pressurization and these should be differentiated for comprehensive analysis. Core exposure is an acceptable surrogate for core damage if only limited possibilities exist to mitigate core damage after core exposure starts. This is often assumed for light water reactors (LWR) but is not necessarily applicable for all reactor types. If a significantly long time interval is required to cause core damage after core exposure, then this should be taken into account in framing a realistic definition of core damage.

(b) The safety functions for prevention of 'core damage' should be identified for each of the initiating event groups. The safety functions required typically include detection of the initiating event, reactor shutdown, residual heat removal, etc. depending on the reactor type and the nature of the initiating event.

(c) The safety systems available to perform each of the safety functions should be identified. The success criterion for each system can then be determined as the minimum level of performance required from the system and expressed, typically, in terms of the number of trains of a redundant system which are required to operate, or the number of relief valves which are required to open and close. The success criteria also specify the requirements for the support systems based on the success criteria for front line systems.

(d) It is important to verify the success criteria of the safety systems to determine whether they depend on the prior success or failure of other safety systems and ensure that this is taken into account in the definition of the success criteria.

(e) Wherever possible, success criteria should be defined and used in the PSA based on best estimate transient analysis. However, if conservative success criteria have been used in the PSA for some of the systems in any accident sequence, this should be clearly indicated and justified. In addition, the results should be reviewed carefully to ensure that such conservatism do not dominate the risk and hence obscure insights from the PSA. If plant specific accident and transient analyses have been performed as part of the PSA in order to determine safety systems success criteria, the review should verify the quality of these analyses.

(f) Regarding the computer codes used to define the success criteria, the review should verify following but not limited to the same:

- The calculation methods used are well qualified to model the transients and accidents being analysed and to obtain a best estimate prediction of the results.
- Both the computer codes and the code users have been subject to quality assurance procedures. The analyses have been performed only by qualified code users. A record documenting the qualification is available.
- The origin and the version of the computer codes used is clearly documented and must be referenced. Computer codes are verified and validated for the relevant area of their application. Verification, validation and benchmarking (if done) are well documented.
- All sources of primary plant data are clearly mentioned. Best estimate input data and assumptions are used whenever possible. Derivation of the input data for computer codes from primary information is documented in such a way that it allows adequate control, review, check and verification.
- For each case analysed, a sufficient description of input data, basic assumptions, safety system set points and capabilities are provided.
- All calculations are well documented and the analysis results which are to be used further in the PSA study are well identified.

3.2.4 System Analysis (SY)

(a) Fault Tree Analysis

(i) The review should verify that fault trees have been developed for each of the safety system failure states identified in the event tree analysis. (For example, NUREG-0492 provides the detailed guidelines for development of the fault trees).

(ii) The review group should carry out plant walk downs and conduct interviews with the system engineers and plant operators to confirm that the systems analysis correctly reflects the as-built and as-operated plant.

(iii) In some cases, more than one model may be needed for the same system to address the success criteria defined for different initiating event groups or in different branches of the event tree, depending upon the sequence of events prior to the demand for the system. Alternatively, one fault tree may be used incorporating house events to switch in the appropriate success criteria. The review should verify that list of all house events, adding the description of how they are to be used is included in the PSA report and fault trees are developed accordingly.

(iv) The modeling of all the individual basic events, in fault trees, which could lead either directly or in combination with other basic events to the top event should be checked.

(v) The basic events modelled in the fault trees should be consistent with the available component reliability data. The component boundaries and component failure modes should be consistent with those defined in the component failure database.

(vi) The modelling of maintenance unavailability must be consistent with the way the system is actually taken out of service for maintenance and with the maintenance unavailability data that are available to quantify these fault events. Where operation of the plant outside its technical specifications has been excluded from the scope of the PSA, maintenance configurations that are prohibited by the technical specifications or operating procedures are not to be modelled in the fault trees.

(vii) The reviewer should be satisfied that there is a proper system of uniquely coding/labeling for each of the basic events in the fault trees, and that this is used consistently throughout all the fault trees in the PSA.

(viii) The failure modes of each of the components grouped together into super components should have the same effect on the system. All the super components must be functionally independent in such a way that no component appears in more than one super component or elsewhere as a basic event.

(b) Dependency Analysis:

(i) The reviewers should verify that a systematic analysis has been carried out to identify all the potential dependencies which could reduce the reliability of safety systems and components in providing protection against initiating events. This will ensure that the selection of common component groups and the screening for inclusion in the PSA has been carried out correctly to ascertain that important common cause failure groups have not been omitted. The different types of dependencies that can occur include the following:

(a) Functional dependencies - Functional dependencies between safety systems or components can arise when the functioning of one system or group of components depends on the functioning of another system or component. These dependencies can arise for a number of reasons including the following:

- Shared components
- Common actuation systems
- Common isolation requirements
- Common support systems — power, cooling, instrumentation and control, ventilation.

(b) Physical dependencies – They can arise in two ways. Firstly, an initiating event can cause the failure of a safety system or component which leads to the failure of some of the safety systems or components required to provide protection. One example of this is where loss of all or part of the electrical distribution system, instrument ventilation system or service water system can lead to a transient and also degrade, or cause the failure of, one or more of the required safety systems. Another example is for an interfacing system LOCA, where high pressure primary coolant flows through low pressure

piping following a failure. Because of the location of the LOCA, the discharge of the primary circuit fluid can lead to the failure of components in the ECCS due to harsh environmental conditions or flooding. Secondly, an internal hazard (such as a fire or a flood) or an external hazard (such as extreme environmental conditions, a seismic event or an aircraft crash) can cause an initiating event (a transient or a LOCA) and failure of some of the safety systems or components required to provide protection. For internal hazards, the safety system failures can arise as, for example, a consequence of pipe whip, missile impact, jet impingement and environmental effects.

(c) Human interaction dependencies – They arise when the operators make errors during repair, maintenance, testing or calibration tasks which lead to the unavailability or failure of safety systems or components such that they will not operate when required following an initiating event. Human interaction dependencies include:

- Test or maintenance activities that require multiple components to be reconfigured
- Multiple calibrations performed by the same personnel
- Post-accident manual initiation (or backup initiation) of components that requires the operator to interact with multiple components.

(d) Component failure dependencies – They cover those failures of usually identical components which are otherwise not analysed. Such failures may be caused by errors in design, manufacture, installation and calibration or by operational deficiencies and are treated quantitatively by common cause failure methods or other dependence quantification approaches. Common cause failure probabilities are usually quantified by using the alpha factor approach, the beta factor approach, the Multiple Greek Letter (MGL) approach or the binomial failure rate model to assess the probabilities of common cause failures on similar (redundant) components.

(ii) The review should verify that the hardware dependencies, including the functional dependencies which could arise within systems, have been identified and modelled explicitly in the fault tree analysis. The inter-system dependencies which could arise due to shared components should be identified and modelled explicitly in the fault tree analysis.

(iii) The common cause failures which can affect groups of redundant components should be identified and modelled in the fault trees. The analysis should identify all the relevant component groups and the important failure modes. The basic events representing common cause failure should be modelled in the fault trees.

(iv) Adequate justification should be provided for the common cause failure probabilities used in the PSA. Where possible, they should be

based on plant specific data. Where this is not possible, use of data from the operation of similar plants or generic data is acceptable. (For example NUREG/CR-5801 and NUREG/CR-5485 provide necessary guidelines for CCF modeling in PSA). The review should verify that the necessary details (i.e. common cause components in group, CCF parameters etc.) are documented in PSA report.

3.2.5 Human Reliability Analysis

(a) The review should verify that human reliability analysis (HRA) is performed in a structured and logical manner and that all steps of the analysis are documented in a traceable way. This is due to the fact that there is a wide variation in available methods for performing HRA and the state-of-the-art in this area is still evolving. Consistent application of the selected HRA methods is critical for a successful HRA.

(b) The review should verify that qualitative descriptions have been given in the PSA report for each of the key human interactions which identify all the significant aspects associated with the action of the plant personnel. This would include:

(i) the timing of the action including supporting information on ergonomics and layout,
(ii) the information available, and
(iii) the influence of prior actions.

(c) It is important to verify that the screening of the human interactions identified has been carried out correctly so that human errors which could be significant to the core damage frequency have not been screened out from detailed consideration.

(d) Type A human interactions take place during normal plant operation before a plant trip occurs. They have a potential to cause the unavailability or failure of a component or system when called upon. Errors may occur during repair, maintenance, testing, or calibration tasks. The review need to verify that important Type A interactions have been identified and included in the assessment in a thorough and consistent manner. This usually involves a review of the plant's maintenance, testing, and calibration procedures to identify these actions for the systems modelled in the PSA. The review should also verify that the quantification process has been done correctly.

(e) Type B human interactions are those actions that cause an initiating event. HRA analysis of these actions is rarely done within the scope of the PSA analysis. The review should verify that the human errors causing initiating events are accounted for in the occurrence frequencies of the initiating events analysed.

(f) Type C human interactions take place following plant trip when the operator is following the procedures and trying to bring the plant to a safe state. These actions are usually the most important human interactions to be considered in

the PSA. There are a number of available methods to analyse these actions, such as the Human Cognitive Reliability (HCR), Technique for Human Error Rate Prediction (THERP), Accident Sequence Evaluation Program (ASEP), Success Likelihood Index Method (SLIM) and others. However, the-state-of-the-art in this area is still evolving. Regardless of the method chosen for analysing Type C human actions, the same review process as for Type A actions should be performed. The review should verify whether the estimation approach for Type C human interactions addresses human failure in cognition as well as failure to execute.

(g) A detailed HRA should be performed for all the human actions that appear in important cut sets using the initial screening values. It should also be ensured that combinations of human actions are not truncated out of the screening quantification because human action dependencies have usually not been considered at this point. Often in screening, the dependency between human interactions is set to 1 to ensure that the related human action dependency is not eliminated in the process. The review should verify that the screening values used initially represent an upper bound for the human error probability.

(h) The review should verify that the specific rules used for excluding or including recovery actions are identified and justified. The rules should cover the feasibility of the recovery actions. Modelling of the human interactions is to be thoroughly documented. The PSA should identify clearly and document all the minimal cut sets that have recovery actions and include the recovery actions. If more than one recovery action is applied to the same cut set, then it should be verified that if their probabilities are independent/dependent.

(i) For the recovery actions that have been included, the review should verify that the time to diagnose and correct the failures (this may mean that co-ordination is required between the main control room (MCR) staff and auxiliary operators), the location in which the recovery can be performed (MCR or locally), the environment in the location, the access to the location, and the stress levels are all identified, justified and documented.

(j) If expert judgment methods, such as the direct estimation approach, are used, the review should examine the process carefully as to how the process was carried out. The review should cover the detailed description of human interactions, the situation influences with regard to the event sequences or scenario, the selection and number of experts and the elicitation process itself.

3.2.6 Data Analysis

(a) One of the main issues with data is their applicability to the NPP in consideration. It is not often that there is much data available which are entirely applicable, and the reviewers should recognize that the analysts will have had to use their judgment in selecting the best sources for each case. Clearly, plant specific data are always to be preferred to generic data but, even for a plant which has been operating for a number of years, the plant specific data are often rather sparse and have to be combined in some way with generic data. A balance has to be struck between the use of a small amount of more

applicable (plant specific) data and the larger amount of less applicable data. For example, a Bayesian approach or other equivalent statistical approach can be used, which combines the available plant data with the generic data. Care should be taken that the generic data/Bayesian priors are not inconsistent with the plant specific data, in terms of both component definitions and numerical values, or that any discrepancies have been adequately explained and accounted for in the combination process.

(b) For a new plant, the designers may have supplied them with data for a similar plant which they have designed and which has been in operation for a number of years, but the analysts may still have had to rely largely on generic data. In any case, the reviewers should verify that the data have been sufficiently justified in the PSA documentation and shown to be relevant, item by item.

(c) For initiating events with a low frequency or for equipment with a low failure probability, the data will be sparse or non-existent, even on a generic basis, and the values to be used in the PSA will then have to be assigned by informed judgment. The review group should be satisfied that the bases for the judgments on these numerical estimates have been given and are acceptable.

(d) The review may audit how the plant records have been used to make plant specific estimates of the number of events or failures. The review should verify the consistency between the definitions of failure modes and component boundaries used in the PSA and the definitions used in the data records.

(e) The estimation of the number of demands, operating hours or standby hours are important in the analysis of specific plant records. The review should verify this estimation for selected components.

(f) The mission times for components, such as pumps which are required to run for some time post reactor trip, should be justified taking into account the definitions of the long term safe states used in the event tree analysis. For some accident sequences, following a large LOCA for example, the time required for recovery of the plant to safe state may be a matter of weeks or months. In such cases, the reliability model has to allow for replacement/repair of components which have failed during the mission time, if this is within the scope of the PSA. This will require estimates of the times required for access and replacement/repair of the components. Times for access should include considerations of the radioactive environment of the component during the particular accident sequence. For many accident sequences, however, the mission time will only be a matter of a few hours and replacement/repair may not be practicable. In these cases, while it is still preferable to determine the appropriate mission time for each component in each sequence, it is often the practice for a blanket mission time, such as 24 hours, to be adopted as a conservative approximation. This may be acceptable provided that it has been justified and does not introduce an excessive conservatism.

(g) For the calculations of system and component unavailability due to maintenance, testing, or calibration, the use of plant specific data, where possible, is preferable to the use of generic data. If a plant specific analysis has

been performed, the review should verify that the calculations have been performed correctly. If generic data have been used, the review should verify that the source is recent and is recognized as acceptable.

3.2.7 Uncertainty, Sensitivity and Importance Analysis

(a) Uncertainty Analysis

(i) Review should be performed in order to gain confidence that the uncertainty introduced by incompleteness is reasonably small. The review should verify that studies have been carried out to determine the extent to which the results of the analysis are sensitive to:

- Assumptions made in various parts of the analysis
- Analytical models selected (or the parameters that influence them) for severe accident phenomena
- Data/parameters used in quantitative analysis.

In particular, the review should verify to ensure that the scope and level of detail of such studies are consistent with the objectives of the PSA. In all cases, the review should verify that the sensitivity/uncertainty analyses address the topics in which there is significant uncertainty and those that are dominant contributors to severe accident progression. The calculation of the core damage frequency should be complemented by sensitivity studies to explore the major uncertainties separately.

(ii) For those scenarios that have been identified in PSA analyses, there are uncertainties introduced by the relative inadequacy of the conceptual models, the mathematical models, the numerical approximations, the coding errors, and the computational limits. For the time being, quantification of model uncertainties is still a very difficult task, and there is no generally accepted method available yet. The review should assess the relative importance of model uncertainties by reviewing the results of sensitivity analysis.

(iii) Data/parameter uncertainty, at present, is the most readily quantifiable one among the three types of uncertainties. Considering the fact that there exists wide variation in values of parameters used in PSA due to scarcity or lack of data, variability within the population of plants and/or components, and assumptions made by experts, uncertainty analysis should be carried out in PSA.

(iv) The review may consider to focus on the method(s) used for uncertainty analysis, the basis of selected distributions and input values for different parameters (including error factors or standard deviations), and whether dependencies have been properly treated in the uncertainty quantification (for example, correlation of variables) to ensure that the uncertainty analysis process is technically accurate, and that the uncertainties have been propagated through the models correctly.

(b) Sensitivity Analysis

(i) The aim of carrying out sensitivity analysis is to address those issues such as the modelling assumptions and data which are suspected of having a potentially significant impact on the results. These assumptions or data are generally in the areas where information is lacking and heavy reliance must be placed on the analyst's judgment. Sensitivity analysis can be performed by substituting alternative assumptions or data and evaluating their individual impacts on the results.

(ii) Modelling assumptions should be addressed case by case, since they do not appear as such in the PSA results, but it may be possible to use simple bounding calculations rather than re-running the PSA evaluation. The reviewers should verify that sensitivity studies have been performed on all the appropriate assumptions and data.

(c) Importance Analysis

(i) Importance analysis determines the importance of contributors to core damage frequency, accident sequence frequencies and system unavailability. The various importance factors typically include the Fussell-Vesely and Birnbaum importance factors and the risk reduction and risk achievement worth. The review should verify that the importance analysis results are in general agreement with the sensitivity analysis qualitatively, and make logical sense.

3.2.8 Analysis of Passive Systems, Components and Structures

In modern reactor designs there is a tendency to incorporate passive safety systems to carry out safety functions such as decay heat removal and emergency core cooling. The PSA should take account of the reliability of these systems just as it does for the active systems. A separate issue is that of the treatment in the PSA of failures of passive structures and components, particularly of high energy pipework and vessels.

a) Passive Safety Systems

These have been introduced into modern designs to provide higher reliability than can be obtained from active systems since they do not depend on support systems such as electric power, and often not on active initiation by the protection system. They are thus particularly valuable during station blackouts. Although the novelty of these passive systems has sometimes been viewed as presenting difficulties in PSA, their treatment is in principle the same as that of the systems, such as accumulators, and of inherent passive safety features, such as natural circulation of reactor coolant when the pumps are not available, which have always been incorporated into PSA.

There are, however, some aspects of novel designs of passive safety systems which warrant the attention of the reviewers. They must, as with active systems, have been shown to be effective by thermal hydraulic analysis and by

extensive tests. This deterministic demonstration of effectiveness should cover the full range of accident conditions for which they are claimed.

Passive systems tend to work at much lower pressures than do active systems so that thermal hydraulic performance predictions may be more difficult. The successful performance of passive systems will have been demonstrated within a set of boundary conditions (e.g. for coolant temperature, pressure and inventory) which can only be ensured by the correct system set-up, including the correct configuration of the relevant valves (not necessarily within the passive system itself).

Given the correct boundary conditions, and a satisfactory demonstration of effectiveness, it may be assumed that the system will work. The failure probability of the passive system is then the probability that the boundary conditions are not realized, i.e. that the system set-up is incorrect. This can be found by standard fault tree analysis, but the reviewers should verify that full account is taken of the potential for human error in leaving the system in the proper condition, as well as of all necessary valves (e.g. check valves) which are required to act and any active initiation signals.

b) Passive Structures and Components

These items may include structures, such as walls, floors and supports, and high energy pipework and vessels.

(i) Structures- Failure of structures as a consequence of certain high energy events, for example seismic events and the impact from missiles generated by failures of pressurized or rotating components, are taken into account in the analysis of internal and external hazards and the detailed review of conditional failure probabilities (fragilities) requires assessment by specialists in these areas. Otherwise, the failure of a properly engineered structure is generally taken to have such a low probability that it need not be considered in the PSA. The reviewers may accept this approach, provided that the regulatory body has accepted the deterministic safety case for the structures, and that there is nothing in the operating history of the plant which casts doubt on particular items.

(ii) Pipework and Vessels- The significance of these in PSA is twofold. First, a spontaneous failure will constitute an initiating event, and an estimate of its frequency will be required. Secondly, the pipework associated with a standby safety system may fail when it is brought into action, contributing to the system failure probability. As regards initiating events, the main interest is in breaches of the primary circuit (LOCA) and of the secondary circuit (steam line breaks and feed line breaks). For some plants, the utility may claim that certain components in the primary and secondary circuits (e.g. the reactor pressure vessel, the steam generator shells and critical lengths of pipework) have been engineered and inspected to such a high standard that the possibility of their failure may be ignored, i.e. that it is outside the design basis of

the plant, and no specific protection should be provided. If the regulatory body accepts this claim in its deterministic engineering assessment, then the PSA reviewers may accept that these failures need not be included in the PSA model, or may be included with a correspondingly low estimated failure rate. Reviewers should check the overall sensitivity of the PSA results to the frequencies adopted. If the sensitivity is low, and the values used are reasonably consistent with those found in other peer reviewed PSA, this approach may be regarded as acceptable. Where a probabilistic fracture mechanics code has been used in the PSA, the reviewers should verify that it is a state-of-the-art code which has had adequate QA, and that the code users are sufficiently qualified and experienced to be aware of its capabilities and limitations.

3.3 Review of Level-1 PSA (Low Power and Shutdown Conditions)

3.3.1 General

The initiating events occurred during low power and shutdown modes usually make a significant contribution to the core damage frequency. It could be due to the wide range of activities taking place during these modes, the simultaneous unavailability of safety system equipment, the blocking of automatic actuation of safety systems and the high reliance on operator actions to restore safety functions. Much of the guidance given in Section 3.2 for the full power PSA is also relevant to the low power and shutdown PSA. This section gives specific guidance applicable to the low power and shutdown modes.

3.3.2 Identification and Grouping of Plant Operating States

(a) The review team should be familiarized with the design, operation and maintenance of the plant during outages. It includes the Technical Specifications applicable to shutdown conditions, maintenance schedules, operating procedures for startup and shutdown, and relevant emergency procedures. In addition, it is prudent to study the available shutdown PSA which have been performed for similar plant designs. In addition, the reviewers should confirm that the refuelling operations are considered in the applicable plant operating states (POS).

(b) The review should be carried out to satisfy that the PSA analysts have carried out a systematic review to identify all the different POS that could occur during low power and shutdown conditions. It should be consistent with the way that the plant is being operated during low power and shutdown as specified in the plant Technical Specifications, operating procedures, maintenance procedures, etc. The initiating events occurring during low power and shutdown modes can also make a substantial contribution to core damage frequency. This could arise due to the wide range of activities taking place during these modes, the simultaneous unavailability of safety system equipment, the blocking of automatic actuation of safety systems and varying plant configurations.

(c) A systematic review of the activities carried out during low power and shutdown conditions should identify a large number of POS. POS have similar

characteristics with respect to the plant conditions, the initiating events that could occur and the availability of safety system equipment, all may be grouped.

(i) Where the set of POS has been condensed, the review should ensure that the POS included in the same group have similar characteristics.

(ii) Where POS have not been addressed explicitly, the reason for not including them should be justified and documented. The review should conform to the set of POS identified for analysis which includes all the different modes of operation of the plant which are not covered in the PSA for full power operation.

3.3.3 Success Criteria

(i) The review should verify that the PSA analysts have defined the consequences that are addressed in the event sequence analysis. Similar to full power PSA, the safety functions that should be performed to prevent these adverse consequences occurring after an initiating event should be identified, the safety systems which are available to perform these safety functions should be identified and the minimum level of performance required from the safety systems (success criteria) should be defined. The safety functions required for an intact core are the same as identified for the full power PSA although the success criteria might be different depending on the decay heat level.

(ii) The review should verify that for any of the POS which have a long duration, the decay heat level may change and this in turn might change the safety system success criteria and provide a longer time scale for operator actions to be carried out. If a POS has been subdivided to take account of the reducing decay heat level, additional event sequence analysis and the appropriate transient analysis should be carried out to provide justification for the different success criteria used.

3.3.4 Accident Sequence Analysis

The review should verify whether the methods used for the event sequence analysis are acceptable. These are usually based on the full power PSA models with appropriate revisions to reflect the different system availabilities and success criteria for example, the headings related to reactor trip can be removed if the reactor is already shutdown and those related to the operation of particular safety systems can be removed if they are not available during the POS. As in full power PSA, for shutdown PSA initiating events may be categorized as internal and external. The review process should ensure that identification of the potential sources, effectiveness of barriers and the probability of mitigating operator response for shutdown PSA model are developed and quantified. The review should verify that success criteria are supported by appropriate analysis. Plant response modeling may be reviewed considering the low power and shutdown configuration of the plant systems as well as activities in each POS. It has to be ensured that the model is capable of reflecting this.

3.3.5 End State Categorisation

(i) The review should verify that the end states identified for the full power PSA should be supplemented by additional ones which represent the conditions which are unique to shut down and refueling (for vessel type reactors). It includes states where the reactor vessel head has been removed or the reactor coolant system is open for inspection. For channel types of reactors, these can be categorised as 'hot shutdown' and 'cold shutdown' states.

(ii) The review should verify that an adequate set of additional end states have been defined and that they are consistent with those already identified.

3.3.6 System Analysis

(i) The review should verify that the systems analysis which is carried out using fault trees and the technical guidance provided in section 3.2.4 for full power PSA, is applicable to shut down and low power PSA. However, there are a number of differences such as:

- safety system success criteria may be different,
- safety systems may be in operation rather than on standby — for example, the residual heat removal (RHR) system (for light water reactors),
- safety systems may be manually initiated rather than initiated automatically,
- the level of redundancy may be lower since some of the trains of the safety systems may have been removed from service, (as allowed by Technical specifications), and
- the required mission time may be significantly different.

The possible modes of operation of the safety systems may be different, for example, some of the modes of the system involving cross-connections may not be available during maintenance activities.

(ii) If the fault trees used in the Shutdown PSA have been developed from those used in the full power PSA, the review should verify that a systematic approach has been used to identify all the features of the POS that would affect the reliability of the safety system and the necessary changes have been reflected in the fault trees.

3.3.7 Common Cause Failure (CCF) Analysis

The review should verify the adequacy and appropriateness of common cause failure probabilities used in the shutdown and low power PSA. The numerical values are likely to be different from those used in the full power PSA since maintenance, test and other activities could introduce additional mechanisms which would affect the potential for a common cause failure to occur.

3.3.8 Human Reliability Analysis

(i) The guidance given for reviewing the HRA and the associated Human Error Probabilities (HEP) as included in the full power PSA in Section 3.2.5 are also applicable to the shutdown and low power PSA. However, there are some differences given below.

(ii) Review should verify whether following factors are considered while estimating the HEP included in the shutdown and low power PSA:

- ongoing multiple activities in plant ,
- higher levels of activity in the plant,
- difficulty in diagnosing initiating events that have occurred and carrying out the appropriate recovery actions,
- the change from automatic to manual actuation for some of the safety systems,
- the use of external contractors to carry out the maintenance work,
- there are a large number of POS that could occur during shutdown and level of detailing of procedures may be different than the level for full power operation,
- the levels of training of operators to deal with accidents occurring during shutdown may be different than the level for full power operation,
- due to the lower decay heat level, the time scale available for operator actions to be carried out is longer than that for the equivalent accident sequence occurring during full power operation.

(iii) Review should verify that HRA methods used in full power PSA are applicable to shut down and low power PSA. Review should also carefully ensure that where there are long time scales available for operator actions to be carried out, caution should be exercised in applying the time reliability correlations used in a full power PSA since the time scales available during shutdown conditions are often well outside the range in which they are applicable.

(iv) Review should verify that the HRA model has taken account of the dependencies which occur between operator actions. It is common practice to assume that there is a high degree of dependence between successive operator actions unless they are carried out by different individuals, or they are well separated in time and location.

3.3.9 Data Assessment

(i) Review should verify that the initiating event frequencies used in shut down and low power PSA are either derived from operating experience from similar plants, derived from the initiating event frequencies used in the full power PSA with factors applied to take account of the different conditions during shutdown or calculated using a logical model which includes all the ways that the initiating event can occur due to configuration, maintenance and other issues. In each case, justification should be provided that the initiating frequency is applicable.

(ii) Where the initiating event frequencies from the full power PSA are modified for use in the shutdown and low power PSA, the review should satisfy the following:

- differences in physical conditions - for example, the lower pressures and temperatures in the reactor coolant system during shutdown which may affect the frequency of pipe break LOCA
- operator errors during maintenance which may affect the frequency of fluid systems being inadvertently drained due to incorrect valve line-ups

(iii) Review should verify that the component failure rate data used in the shutdown and low power PSA are applicable to shutdown conditions and if the same is not available, the component failure rates as those in the full power PSA may be accepted if justification is made available.

3.4 Review of Level-1 PSA (External Events)

3.4.1 General

This section provides guidance for the review of the PSA for internal and external hazards, sometimes referred to as external events, even when internal hazards are included. It addresses the identification of internal and external hazards and the screening carried out to eliminate those which are unimportant contributors to the core damage frequency. It then gives guidance on three specific hazards — earthquakes, fires and floods (internal and external) which have typically been among those found to give significant contributions to the risk. A methodology similar to that for internal flood assessment may be used for analysis of external floods and all other similar associated phenomenon. Guidance available in the AERB regulatory documents should be referred for extreme values for the external events. This illustrates the general approach, which can be adapted to the review of the analysis of other hazards.

3.4.2 Seismic Events

(i) Major elements of a Seismic PSA are:

(a) Probabilistic seismic hazard analysis (PSHA)
(b) Seismic fragility analysis
(c) Seismic plant response analysis

Review should verify whether the above elements are addressed adequately, covering the aspects mentioned below. The review should also verify that each of these steps is clearly identified in the PSA and bases are given for data and models used.

(ii) Probabilistic Seismic Hazard Analysis:

Review should verify whether a site-specific seismic hazard analysis has been performed and the following aspects are appropriately addressed:

a) The frequency of earthquakes at the site reflects the current understanding of seismic experts.

b) A comprehensive up-to-date database of geological, seismological, and geophysical data; historical, instrumental, and paleoseismicity; local site topography; geological and geotechnical site properties, is available.

c) All credible sources of earthquakes are considered in the assessment and the uncertainties in characterizing the seismic sources are included.

d) Sufficient number of attenuation relations, appropriate for the region including the site have been used and adequate technical basis is available for weightage provided for different attenuation relations in the logic tree. Local site response is also appropriately considered.

e) Uncertainties (aleatory and epistemic) associated with all relevant input parameters/models are appropriately captured.

f) Logic tree approach has been adopted for propagating the uncertainties in each step of the hazard analysis. Weightages used for different parameters are justified.

g) Fractal hazard curves, median and mean hazard curves are included. Seismic source de-aggregation and magnitude-distance de-aggregation are performed and results available.

h) Uniform hazard spectra have been developed and the spectral shape is based on a site-specific evaluation.

i) The basic data and interpretations are still valid in light of current information, when an existing study is adopted in lieu of a fresh PSHA.

j) Possibility of other seismic hazards like fault displacement, landslide, soil liquefaction and soil settlement, have been addressed.

(iii) Seismic Fragility Analysis:

Review should verify whether:

a) Methodology for seismic fragility evaluation of structures, systems and components (SSC) is documented and acceptable. The methodology covers components qualified by analysis, testing and experience based approaches including walk down.

b) The seismic-fragility analysis is plant-specific and provides an estimate of seismic fragilities of SSC whose failure may contribute to CDF. Sources for the fragility parameters and their uncertainties should be documented.

c) The basis for screening is described and acceptable, if screening of seismically rugged components has been performed.

d) Seismic analysis has been performed to evaluate the behaviour of SSC and the results are appropriately used for seismic fragility analysis.

e) The seismic-fragility analysis considers critical failure modes of SSC and these critical failure modes are identified through plant walk down and review of appropriate plant documents.

f) Plant walk down has been undertaken with focus on component dependencies, equipment anchorage, spatial interactions and equipment capacity. The findings of a plant walk down are documented.

g) The seismic-fragility evaluation appropriately addresses the findings of plant walk down.

h) The calculation of seismic-fragility parameters is based on plant-specific data supplemented as needed by generic data (from earthquake experience) and test data. When test data or generic data is used, uniformity in basic seismic parameter used for representing the seismic capacity has been ensured. Use of such data is technically justified.

i) Uncertainties in fragility curves should be documented.

(iv) Seismic Plant Response Analysis:

Review should verify whether:

a) A full scope level-1 PSA at full power exists and that is the basis for the system model used in seismic PSA.

b) The system model for seismic-PSA includes seismic-induced initiating events and other failures including seismically induced SSC failures, non-seismically induced unavailability, and human errors.

c) The systems model for seismic-PSA incorporates the seismic-analysis aspects that are different from corresponding aspects found in the at-power internal-events PSA systems model.

d) The systems model for seismic-PSA reflects the as-built and as-operated state of the plant.

e) The sum of the component fragility and its unavailability due to internal plant causes is used as the component unavailability in the calculations.

f) The approach for selection of SSC considers the basic safety functions viz. shutdown, decay heat removal and confinement of radioactivity. The list of SSC selected for seismic-fragility analysis includes all SSC that participate in accident sequences included in the systems model for seismic-PSA.

g) Physical and systematic (functional) dependencies between components due to the seismic event are appropriately addressed.

h) The analysis to quantify core damage frequency appropriately combines the seismic hazard, the seismic fragilities, and the systems-analysis aspects.

i) Assigned human error probabilities appropriately accounts for psychological factors, like increased stress etc.

j) Detailed and specific HRA for seismic events is carried out. The effects of the seismic event on the probability of human error and the corresponding increase due to the seismic event are appropriately accounted for. The recovery actions should be reviewed to identify changes in any conditions due to the seismic event that result in higher non-recovery probabilities (such as room access concerns or hazardous room environments).

3.4.3 Fire Events

(i) The review should verify analysis of internal fire events which includes the following steps:
- Initial screening to eliminate fire scenarios in rooms that are small contributors to plant risk
- Estimation of the frequency of fires of different size starting in different rooms of the plant
- Assessment of the type of plant disturbance potentially caused by a fire
- Identification of other possible sources of fire
- Calculation of the propagation of the initiated fire and propagation of fire effects to affected components and operators
- Estimation of non-detection and non-suppression probabilities for the initiated, propagating fire
- Evaluation of component dependencies and component failure probabilities due to fire effects
- Estimation of the effects of the fire on human actions and possibilities for increasing the probabilities of identified human errors
- Calculation of the core damage frequency due to fires by combining the fire initiation frequency with the component failure probabilities and failure of operator recovery actions.

(ii) The review should verify that if a screening process is carried out, for example to identify the critical locations or compartments, the screening technique, including the basis for any screening of fire initiation frequencies used, should be assessed for its validity.

(iii) The review should verify plant specific data or data from similar plants to determine whether plant specific fire initiating frequencies can be estimated. If plant specific data exist, fire initiating frequencies are to be estimated by means of accepted Poisson approaches describing the likelihood and Bayesian approaches describing the uncertainties in the parameters.

(iv) The review should verify databases used for the fire initiation frequencies and it should be referenced so that during review it can be checked for consistency between the databases and the data for the plant being analysed.

(v) The review should verify the effects of the fire propagation and it should be calculated by means of one of the accepted fire propagation approaches. Input parameters to the calculations warrant review to determine whether they represent the actual plant. The review should verify the parameters to be reviewed which include the amount of permanent or transient combustible material available in each zone. The transmission of smoke through ventilation ducts, fire dampers and the heating of instrument and component compartments should be included in the propagation analyses.

(vi) The review should verify the probabilities of non-detection and non-suppression which are incorporated into the fire propagation analysis to determine the probability that the fire propagates to critical equipment without detection or suppression. The physical layout and manual as well as automatic actions in determining non-detection and non-suppression probabilities should be considered during review.

(vii) The review should verify whether the fire barrier effectiveness is established and documented. The review should verify whether penetrations in the barriers, such as doors and windows that may have been left open, have been taken into account in probability assignments.

(viii) The review should verify about scenarios of fires in MCR which may require MCR evacuation and transfer of control to back up control room/ supplementary control room. The review should consider the procedures for operator actions which may suffer from diagnostic difficulties and limited instrumentation on back up panel.

(ix) The review should verify that if fault trees are developed for fire suppression systems, the treatment of dependencies caused by the fire are adequately addressed.

(x) The shutdown and low power PSA for internal fire should take account of the fact that the initiating events frequencies may be increased (for example, due to welding operations being carried out), there may be additional inventories of combustible materials introduced into some areas of the plant, automatic fire suppression systems may not be available and some of the fire barriers may not be fully effective (for example, fire barriers may have been removed, fire doors left open or penetration seals removed). Where possible, review should consider a plant walk down to determine the status of the fire protection systems during a representative subset of the POS to ensure that this is accurately reflected in the shutdown and low power PSA.

3.4.4 Flood Events

(i) The review should verify analysis for internal floods which includes the following steps:

- initial screening to eliminate flooding scenarios in rooms that are small contributors to plant risk,
- identification of the possible water and steam sources,
- assessment of the type of plant disturbance potentially caused by the flooding,

- evaluation of the frequency of occurrence of an initiating event caused by these sources,
- estimation of the likelihood that the operator does not detect and control the flood,
- identification of the components that are affected by the flooding, and
- calculation of the frequency of core damage due to internal flooding by combining the initiating event frequencies with the probability of occurrence of the accident sequence.

(ii) The review should verify that the frequencies of initiating events are first screened for their potential contribution to the core damage frequency. Initiating event frequencies that are significantly lower than the frequencies of internal event core damage sequence frequencies can be screened out.

(iii) The review should verify that consideration of components affected by flooding takes into account elevations, barriers, doors and drains. Drain blockage should be considered. The review should verify that a conservative approach is considered to assume that all components fail in the compartment that is affected. If this assumption does not cause a significant contribution to the core damage frequency, the initiating event can be screened out. It is necessary to assess the possibility of flooding from one room to another.

(iv) The review should verify that all potentially contributing initiating events are evaluated in terms of the means of detecting and controlling the event. The means then should be considered in estimating the non-detection probability.

(v) The review should verify that additional human actions that may be needed to mitigate the flooding consequences are identified and assessed for their probability of success/failure. These include, for example, isolation and subsequent restoration of the electrical power supplies. It is important that the HRA takes into account the loss of I&C equipment and spurious indications that may be generated due to the flood.

(vi) The review should verify the following and it should be considered while reviewing flood analysis for shutdown and low power PSA:

- sources of the internal flood may be different from those during full power operation - for example, water systems which are pressurized during power operation may be depressurized during shutdown; temporary water systems and hose connections may be in use,
- initiating events frequencies may be increased — for example, due to incorrect valve alignments leading to flooding,
- flood protection features may be defeated — for example, there is an increased potential for drainage systems to become blocked due to debris which accumulated during maintenance activities, doors in segregation barriers may be left open, penetration seals may be removed.

3.5 Quantification of the Analysis

The review should verify the following:

(i) The next stage is to quantify the analysis to determine the core damage frequency and to identify the sequences which contribute to core damage. This requires that a Boolean reduction be carried out for the logical models

developed using event trees and fault trees for each of the initiating event groups.

(ii) The accident sequence frequencies are then calculated using the data, for example, for initiating event frequencies, component failure probabilities, durations and the corresponding frequencies, common cause failure probabilities and human error probabilities.

(iii) A number of computer codes are available that can be used to carry out this analysis. The reviewers should verify that the PSA quantification process is technically correct and thorough, and that key dependencies are correctly accounted for in the quantification process.

(iv) The quantification process should be carried out using a suitable computer code which has been fully validated and verified.

(v) In addition, the users of the codes should be adequately experienced, and understand the uses and limitations of the code.

(vi) Reviewers should verify that the accident sequences/cut sets identified do actually lead to core damage.

(vii) This is advisable for a sample of the sequences, focusing on those which make a significant contribution to the risk. Where cut-offs are used in the quantification process (either on cut set order or frequency), the reviewers should verify that they have been set at a sufficiently low level that they would not lead to a significant underestimate of the frequency of core damage.

3.6 Quality Assurance in PSA

The review process should consider review of the utility's PSA production process along with the technical issues in order to give confidence that those aspects which have not been reviewed in detail have been performed satisfactorily. The review should verify that the utility has procedures in place for the PSA production which set out the basic principles and methodologies to be adopted and they are adequate to produce state-of-the-art PSA.

The review should also verify that the relevant QA requirements specified in AERB/NPP/SC/QA are fulfilled by the utilities in PSA production process. Review may also take cognizance of other documents such as AERB/NPP&RR/SM/O-1 and IAEA-TECDOC-1101. It is a good practice to have arrangements in place for an independent peer review of the PSA.

The review should also verify that the utility has maintained the control of all the documents and workbooks used in the performance of the PSA as per QA requirements to allow for any audit or review by the AERB. All the documents and workbooks used in the review of the PSA as per QA requirements should be maintained.

4. CONTENT OF REVIEW REPORT

The regulatory review report of level-1 PSA for nuclear power plants and research reactors should include following:

4.1 Executive Summary

The executive summary of review report should address the objective and scope of the review, review team members, methods and approaches considered in the review, major review findings and recommendations.

4.2 Overview of the PSA Document

This section should provide an overview of the PSA submittal covering the general description of the nuclear power plant and research reactor for which the PSA is carried out, structure of the PSA report and PSA team members.

4.3 Review Bases

The bases of the review and the relevant references used during the PSA review should be documented. The outcome and observations of the plant walk-down and interview with the plant personnel if any may be documented.

4.4 Review Findings

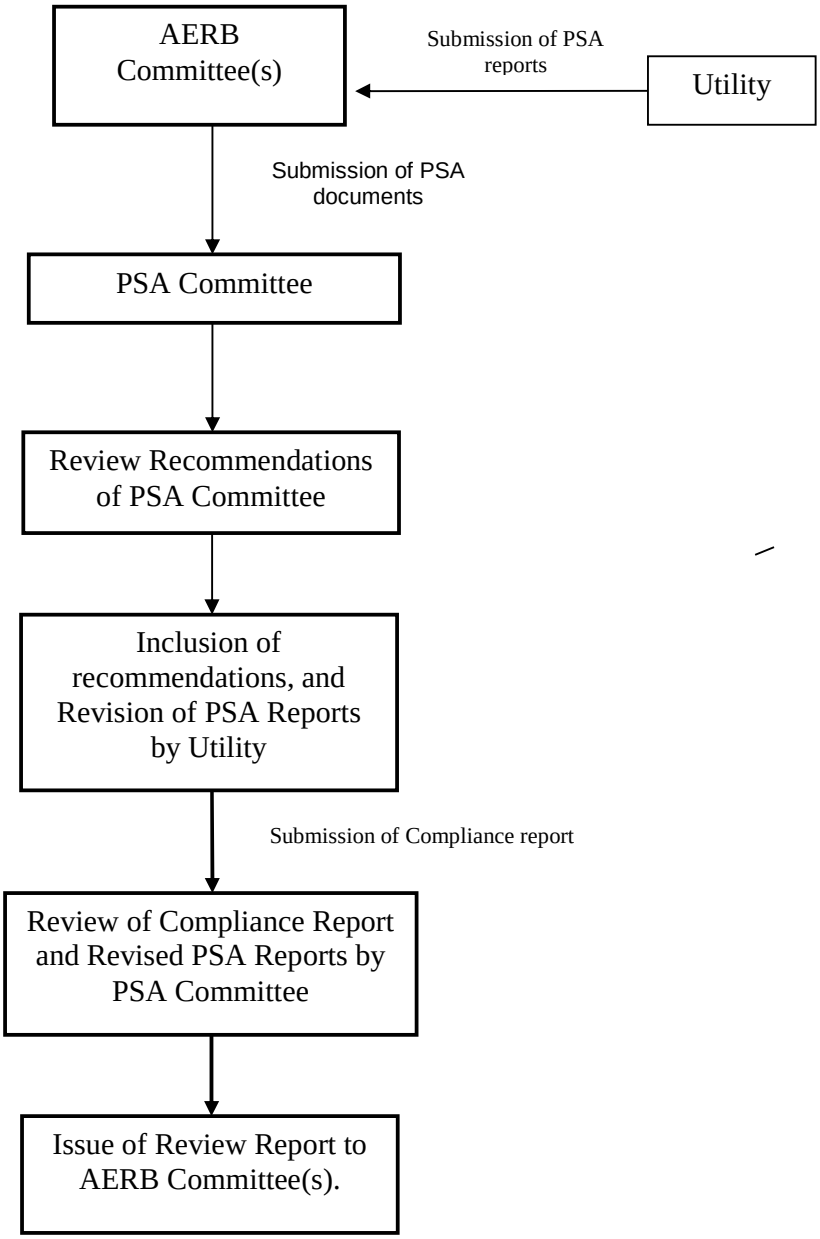
The review findings should be properly documented for future reference and follow up actions. The review process should verify and document that all the review findings are reported along with the final conclusions of the review. The review report should give the conclusion reached on the adequacy of the PSA including the PSA results with uncertainty and sensitivity analyses. The problem areas identified if any should be reported.

4.5 Recommendations

The review report should bring out the improvement areas in PSA where applicable, for future work. It should include recommendations where applicable, on the scope/methodology/quality of the PSA, changes to be made in PSA in order to apply it to particular application, or changes to be made in design or operation of the nuclear power plants. It may also include the recommendations regarding the revision of the PSA in order to keep it up to date and to ensure that it continues to meet the requirements originally agreed for PSA.

ANNEXURE-I

REVIEW PROCESS



BIBLIOGRAPHY

1. ATOMIC ENERGY REGULATORY BOARD, Site Evaluation of Nuclear Facilities, AERB Safety Code, AERB/NF/SC/S (Rev.1), Mumbai, March (2014).

2. ATOMIC ENERGY REGULATORY BOARD, Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors, AERB Safety Manual No. AERB/NPP&RR/SM/O-1, Mumbai, March (2008).

3. INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants IAEA-TECDOC-1511, Vienna, July (2006).

4. UNITED STATES NUCEAR REGULATORY COMMISSION, An Approach for Determining the Technical Adequacy of PRA Results for Risk Informed Activities, RG-1.200, Washington, DC, February (2004).

5. AMERICAN SOCIETY FOR MECHANICAL ENGINEERS, Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-Sb-2005, New York, (2005).

6. UNITED STATES NUCEAR REGULATORY COMMISSION, Issues and Recommendations for Advancement of PRA Technology in Risk-informed Decision-making, NUREG/CR-6813, Washington, DC, April (2003).

7. INTERNATIONAL ATOMIC ENERGY AGENCY, Review of Probabilistic Safety Assessment by Regulatory Bodies, IAEA Safety Report Series No.25, Vienna, December (2002).

8. INTERNATIONAL ATOMIC ENERGY AGENCY, IPERS Guidelines for the International Peer Review Service, IAEA-TECDOC-832, Vienna, October (1995).

9. UNITED STATES NUCEAR REGULATORY COMMISSION, Guidance on the Treatment of Uncertainties Associated PRA in Risk-informed Decision-making, NUREG-1855, Washington, DC, November (2007).

10. UNITED STATES NUCEAR REGULATORY COMMISSION, Estimating Loss of Coolant Accident (LOCA) Frequencies through the Elicitation Process, NUREG-1829, Washington, DC, April (2008).

11. INTERNATIONAL ATOMIC ENERGY AGENCY, External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Series No.50-P-7, Vienna, January (1995).

12. INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment of Nuclear Power Plants for Low Power and Shutdown Modes, IAEA-TECDOC-1144, Vienna, March (2000).

13. INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101, Vienna, August (1999).

14. UNITED STATES NUCEAR REGULATORY COMMISSION, Procedure for Analysis of Common-cause Failures in Probabilistic Safety Analysis NUREG/CR-5801, Washington, DC, April (1993).

15. UNITED STATES NUCEAR REGULATORY COMMISSION, Guidelines on Modeling Common-cause Failures in Probabilistic Risk Assessment NUREG/CR-5485, Washington, DC, November (1998).

16. UNITED STATES NUCEAR REGULATORY COMMISSION, Fault Tree Handbook, NUREG-0492, Washington, DC, January (1981).

LIST OF PARTICIPANTS

IN-HOUSE CONTRIBUTION FOR DRAFT DOCUMENT PREPARATION

Shri R. B. Solanki, AERB
Shri Mahendra Prasad, AERB
Shri Dhanesh B.Nagrale, AERB

AERB COMMITTEE ON PSA FOR NUCLEAR FACILITIES

Dates of meeting:

November 27, 2012
February 13, 2013
June 26, 2013
February 11, 2014
May 20, 2014
May 21, 2014.

Members and invitees of the PSA Committee:

Shri S.P.Dharne(Chairman)	:	NPCIL (Former)
Shri R.K.Saraf	:	BARC (Former)
Shri A. J. Gaikwad	:	AERB
Smt. Rajee Guptan	:	NPCIL
Dr. Gopika Vinod	:	BARC
Dr. Senthil Kumar	:	AERB
Shri John Arul	:	IGCAR
Smt. A.K.Vijaya	:	NPCIL
Shri R.B.Solanki	:	AERB
Dr. Hari Prasad	:	BARC
Shri Ravikant Karda	:	AERB (Former)
Shri V.R.Dhotre	:	AERB
Shri Mahendra Prasad (Member-Secretary)	:	AERB
Shri R.S.Rao (Permanent Invitee)	:	AERB
Shri Dhanesh B. Nagrale (Invitee)	:	AERB

ADVISORY COMMITTEE FOR PREPARATION OF CODES AND GUIDES ON GOVERNMENTAL ORGANIZATION FOR REGULATION OF NUCLEAR AND RADIATION FACILITIES (ACCGORN)

Dates of meeting:

August 21,2014
September 1, 2014
September 8, 2014
January 22, 2015
February 3, 2015

Members and Invitees of ACCGORN:

Shri S.C.Hiremath, (Chairman)	:	HWB (Former)
Shri Avinash J. Gaikwad	:	AERB
Shri L. R. Bishnoi	:	AERB
Shri K.J.Vakharwala	:	AERB (Former)
Dr. Avinash Sonawane	:	AERB
Shri R. Bhattacharya	:	AERB
Shri P. R. Krishanmurthy	:	AERB
Shri Jose Joseph	:	AERB
Dr. A. Nandakumar	:	AERB (Former)
ShriS.K.Pradhan (Permanent invitee)	:	AERB
Shri Y.K. Shah, (Member-Secretary)	:	AERB

LIST OF CODES, GUIDES AND MANUALS FOR REGULATION OF NUCLEAR AND RADIATION FACILITIES

Safety Series No.	Title
AERB/SC/G	Regulation of Nuclear and Radiation Facilities
AERB/SG/G-1	Consenting Process for Nuclear Power Plants and Research Reactors: Documents Submission, Regulatory Review and Assessment of Consent Applications
AERB/SG/G-2	Consenting Process for Nuclear Fuel Cycle and Related Industrial Facilities: Documents Submission, Regulatory Review and Assessment of Consent Applications
AERB/SG/G-3	Consenting Process for Radiation Facilities
AERB/SG/G-4	Regulatory Inspection and Enforcement in Nuclear and Radiation Facilities
AERB/SG/G-5	Role of Regulatory Body with respect to Emergency Response and Preparedness at Nuclear and Radiation Facilities
AERB/SG/G-6	Development of Regulatory Safety Documents for Nuclear and Radiation Facilities
AERB/SG/G-7	Regulatory Consents for Nuclear and Radiation Facilities: Contents and Formats
AERB/SG/G-8	Regulations and Criteria for Health and Safety of Nuclear Power Plant Personnel, the Public and the Environment
AERB/SG/G-9	Formats and Contents of Safety Analysis Reports for Nuclear Power Plants (Under preparation)
AERB/SG/G-10	Regulatory Review of Level-1 Probabilistic Safety Assessment for Nuclear Power Plants and Research Reactors
AERB/NPP&RR/SM/G-1	Regulatory Inspection and Enforcement in Nuclear Power Plants and Research Reactors
AERB/NF/SM/G-2	Regulatory Inspection and Enforcement in Nuclear Fuel Cycle and Related Industrial Facilities other than Nuclear Power Plants and Research Reactors
AERB/RF/SM/G-3	Regulatory Inspection and Enforcement in Radiation Facilities